RECHERCHES

ARITHMÉTIQUES.

Carl Friedrich GAUSS

RECHERCHES ARITHMÉTIQUES

Traduction française des *Disquisitiones Arithmeticae*



ÉDITIONS
JACQUES GABAY

© 1989, Éditions Jacques Gabay
25, rue du Dr Roux 92330 Sceaux

Tous droits réservés. Aucun extrait de ce livre ne peut-être reproduit, sous quelque forme ou quelque procédé que ce soit, sans le consentement préalable de l'Éditeur

ISBN 2-87647-054-3

RECHERCHES ARITHMÉTIQUES,

Par M. Ch.-Fr. GAUSS (de Brunswick);

Traduites par A.-C.-M. POULLET-DELISLE,

Professeur de Mathématiques au Lycée d'Orléans.

A PARIS,

Chez Courcier, Imprimeur-Libraire pour les Mathématiques, quai des Augustins, n° 57.

1807.

Je n'ai eu d'autre but, en traduisant cet Ouvrage, que de contribuer à répandre les excellentes Recherches de M. Gauss, sur la *Théorie des nombres*. Je m'abstiendrai d'en faire ici l'éloge; déjà sa place a été assignée par le jugement des plus illustres Géomètres, et il y aurait de la présomption de ma part à joindre ma voix à la leur.

Je ne me suis permis aucune altération du texte, parceque j'ai voulu donner au Public l'ouvrage de M. Gauss, et non me l'approprier. C'est par cette raison, et d'après des conseils que j'aurais dû respecter, quand même ils auraient été contraires à mon opinion, que j'ai conservé rigoureusement les dénominations et la notation, qui peuvent étonner au premier abord. Mon intention était même de ne mettre aucune note; le très-petit nombre de celles que l'on rencontrera signées du traducteur, fait voir avec quelle réserve j'ai cru devoir user de cette faculté; leur nature indique assez le motif qui m'a déterminé, et le lecteur jugera si c'est avec raison.

Il m'aurait été possible de remplacer quelques-unes des démonstrations que l'auteur a supprimées, dans l'intention d'abréger; mais par-là je serais tombé dans l'inconvénient qu'il a voulu éviter. Enfin, conduit naturellement par mon travail même, à quelques considérations nouvelles, j'avais été tenté de les placer à la fin des Recherches arithmétiques; mais j'ai préféré attendre que le temps et

la méditation me missent dans le cas de les présenter aux Géomètres d'une manière plus complète et plus digne de leurs regards.

Je prie le lecteur de corriger d'avance, d'après l'*Errata*, les fautes d'impression qui n'ont pu manquer de se glisser dans un ouvrage de ce genre.

A MONSIEUR LAPLACE,

Chancelier du Sénat-Conservateur; Grand-Officier de la Légion d'Honneur; Membre de l'Institut et du Bureau des Longitudes; des Sociétés Royales de Londres et de Gottingue; des Académies des Sciences de Danemarck, de Suède, d'Espagne, d'Italie, etc.

MONSIEUR,

LE mérite de l'Ouvrage dont j'ai l'honneur de vous offrir la traduction, et l'intérêt que vous avez daigné accorder à mon entreprise, sont les seuls titres qui la rendent digne de vous être présentée; mais quoique je sente combien cet intérêt doit influer sur l'accueil

que mon travail pourra recevoir, ce n'est pas pour m'appuyer de votre illustre nom que j'ai desiré vous en faire hommage. Cet hommage était dû à l'homme de génie qui, pénétré d'un noble amour pour la science, non content d'en reculer chaque jour les limites, accueille tous les travaux utiles, encourage les talens, applaudit à leurs efforts et n'aspire qu'à répandre le feu qui l'anime. C'est à celui qui aime la science pour elle-même, que doivent s'adresser ceux qui les cultivent; et si l'on recherche avec orgueil à mériter son approbation, on s'estime heureux d'être en quelque sorte, auprès de lui, l'interprète de la reconnaissance et de l'admiration publique. Tel est, MONSIEUR, le double motif qui m'a fait ambitionner l'honneur que je reçois aujourd'hui; mais je sens aussi toute l'étendue des engagemens qui en résultent pour moi: en consacrant ma vie entière à cette science sublime, mon seul desir est de prouver un jour que je n'étais pas tout-à-fait indigne d'une aussi grande faveur.

Je suis avec le plus profond respect,

MONSIEUR,

Votre très-humble et
très-obéissant serviteur,

POULLET-DELISLE.

ÉPITRE

ÉPITRE DÉDICATOIRE DE L'AUTEUR.

A SON ALTESSE SÉRÉNISSIME, MONSEIGNEUR CHARLES-GUILLAUME-FERDINAND, DUC DE BRUNSWICK ET DE LUNEBOURG.

PRINCE SÉRÉNISSIME,

LORSQUE la reconnaissance m'impose le devoir sacré de vous offrir cet Ouvrage, vous mettez le comble à ma félicité, en me permettant de placer à la tête votre nom illustre et respectable. En effet, PRINCE SÉRÉNISSIME, eussé-je pu me dévouer tout entier aux sciences mathématiques, vers lesquelles une ardeur irrésistible m'a toujours emporté, si votre faveur ne m'en eût ouvert l'entrée, si vos bienfaits continuels n'eussent incessamment soutenu mes travaux. Par vos seules bontés, libre des soins étrangers, et maître de consacrer mon temps à l'étude, j'ai pu entreprendre les recherches dont cet Ouvrage renferme une partie, et m'y livrer pendant plusieurs années. Lorsque j'ai desiré de le mettre au jour, votre munificence a écarté tous les obstacles qui en retardaient la publication. Il m'est plus facile de conserver au fond de mon cœur et d'admirer en silence,

que de célébrer dignement cet intérêt si grand et si généreux que vous avez bien voulu accorder à mes efforts : non-seulement je me sens au-dessous d'une telle entreprise, mais je pense que personne n'ignore quelle est l'étendue de votre libéralité à l'égard de ceux qui semblent portés vers l'étude des sciences, et que votre protection est également accordée à celles qui paraissent les plus abstraites et d'une application moins directe aux usages ordinaires de la vie, parceque dans la profondeur de votre sagesse, habile à profiter de tout ce qui tend au bonheur et à la prospérité de la société, vous avez senti la liaison intime et nécessaire qui unit entre elles toutes les sciences.

Si cet Ouvrage, PRINCE SÉRÉNISSIME, témoignage de ma reconnaissance pour vous, et des travaux que j'ai consacrés à la plus noble des sciences, ne vous semble pas indigne de la faveur dont vous m'avez si long-temps environné, je me féliciterai de n'avoir pas perdu ma peine et d'avoir mérité cet honneur, celui de tous qu'ambitionnait le plus,

PRINCE SÉRÉNISSIME,

De votre Altesse, le
très-dévoué serviteur,
CH.-F. GAUSS.

Brunswick, juillet 1801

PRÉFACE DE L'AUTEUR.

Les Recherches contenues dans cet Ouvrage appartiennent à cette partie des Mathématiques où l'on considère particulièrement les nombres entiers, quelquefois les fractions, mais où l'on exclut toujours les nombres irrationnels. L'Analyse *indéterminée*, ou de *Diophante*, qui apprend à distinguer, parmi les solutions d'un problème indéterminé, celles qui sont entières, ou du moins rationnelles et le plus souvent positives, ne constitue pas cette doctrine, mais elle en est une partie très-distincte; elle a avec elle à-peu-près le même rapport que l'Algèbre, c'est-à-dire, l'art de réduire ou de résoudre les équations, avec l'Analyse universelle. En effet, de même que l'on rapporte à l'Analyse toutes les recherches que l'on peut faire sur les affections générales des quantités, la considération des nombres entiers et des fractions, quand ces dernières s'expriment au moyen de nombres entiers, constituent proprement l'objet de l'*Arithmétique;* mais on ne donne ordinairement sous ce nom que l'art de former les nombres et de les calculer, c'est-à-dire, l'art de représenter les nombres par des signes convenables (par exemple, suivant le système décimal), et d'exécuter les opérations arithmétiques, en y ajoutant quelques points, dont les uns n'appartiennent pas à l'Arithmétique, comme la théorie des logarithmes et les autres ne sont pas particuliers aux nombres entiers, et ont lieu pour toutes les quantités. On voit par là que l'on doit distinguer deux parties dans l'Arithmétique, et que les considérations dont nous venons de parler se rapportent à l'Arithmétique élémentaire, tandis

que les recherches générales sur les affections particulières aux nombres entiers sont revendiquées par l'*Arithmétique transcendante.*

Ce qu'*Euclide* a présenté dans le *Livre VII de ses Élémens*, avec l'élégance et la rigueur ordinaires aux anciens, appartient à l'Arithmétique transcendante, mais se borne aux premiers élémens. Le célèbre Ouvrage de *Diophante*, qui est consacré tout entier aux problèmes indéterminés, contient un grand nombre de questions qui, par leur difficulté et la subtilité des artifices, donnent une grande idée du génie et de la pénétration de l'auteur, surtout quand on considère le peu de ressources qu'il pouvait employer; mais comme ces problèmes demandent plutôt de l'adresse et des procédés ingénieux que des principes difficiles, et qu'en outre ils sont trop particuliers et conduisent rarement à des conclusions générales, cet Ouvrage semble plutôt avoir fait époque dans l'histoire des Mathématiques, parcequ'il fixe les premiers vestiges de l'Algèbre, qu'avoir enrichi l'Arithmétique transcendante par de nouvelles découvertes. La Science est bien plus redevable aux modernes, parmi lesquels peu d'hommes à la vérité, mais tous dignes d'une gloire immortelle, FERMAT, EULER, LAGRANGE, LEGENDRE (et un petit nombre d'autres), ont ouvert l'entrée de cette science divine, et ont découvert la mine inépuisable de richesses qu'elle renferme. Je n'entre pas ici dans l'énumération des découvertes de ces géomètres, d'autant qu'on peut les connaître par la Préface des Additions dont *Lagrange* a enrichi l'*Algèbre d'Euler*, et par celle de l'Ouvrage de *Legendre*, dont nous parlerons bientôt. D'ailleurs nous rendrons hommage à ces différentes découvertes, lorsque l'occasion s'en présentera dans nos Recherches.

Mon but en publiant cet Ouvrage, annoncé depuis cinq

ans, a été de faire connaître les recherches dont je m'étais occupé avant cette époque, et celles que j'ai faites depuis. Mais afin que l'on ne s'étonne pas de voir ici la Science prise presque dès son principe, et que je sois revenu sur des recherches faites déjà par plusieurs autres, j'ai cru qu'il n'était pas inutile d'avertir que, lorsqu'en 1795, j'ai commencé à m'appliquer à ce genre de considérations, je n'avais absolument aucune idée de tout ce qui avait été fait sur ce sujet, même par les modernes, et que j'étais privé de tous les secours que j'aurais pu tirer de leurs travaux. Occupé dans ce temps d'une autre matière, je tombai par hasard sur une vérité importante de l'Arithmétique (c'était, si je ne me trompe, le théorème du n° 108); comme elle me sembla très-belle par elle-même, et que je la soupçonnais liée à d'autres plus importantes, j'employai toute la contention d'esprit dont j'étais susceptible, à découvrir les principes sur lesquels elle s'appuyait, et à en trouver une démonstration rigoureuse; le succès ayant répondu à mes vœux, je me sentis tellement entraîné par l'attrait de ces questions, qu'il me fut impossible de les abandonner, et comme une vérité me conduisait à une autre, la plus grande partie des quatre premières Sections était déjà terminée avant que j'eusse rien vu des travaux des autres géomètres sur ce sujet. M'étant ensuite trouvé à même de lire les ouvrages de ces hommes de génie, je ne tardai pas à reconnaître que j'avais employé la plus grande partie de mes méditations à des choses faites depuis long-temps; mais animé d'une nouvelle ardeur, je m'efforçai, en suivant leurs pas, de cultiver plus avant le champ de l'Arithmétique, et telle a été l'origine des Sections V, VI et VII. Quelque temps après, je demandai des conseils sur le projet que j'avais de publier le fruit de mes veilles, et d'après le desir de plusieurs personnes, je me

laissai d'autant plus facilement persuader de ne rien supprimer de mes premières recherches, qu'à cette époque il n'existait aucun ouvrage dans lequel on pût trouver les travaux des autres géomètres, épars dans les Mémoires des Académies; que d'ailleurs elles renfermaient un grand nombre de choses nouvelles, et d'autres présentées d'une manière qui m'appartenait; qu'enfin toutes ces recherches étaient tellement liées entre elles, et avec celles qui leur étaient postérieures, qu'il aurait été très-difficile d'expliquer les choses nouvelles sans reprendre les autres dès leur principe.

Dans cet intervalle, il a paru un excellent ouvrage d'un homme qui avait déjà rendu de très-grands services à l'Arithmétique transcendante (*Essai sur la Théorie des nombres*, *Legendre*, *an VI*), dans lequel il a non-seulement rassemblé et mis en ordre tout ce qui a paru jusqu'à présent sur cette science, mais ajouté beaucoup de choses nouvelles qui lui sont propres. Comme cet ouvrage m'est parvenu trop tard, et lorsque la plus grande partie de mes *Recherches* était imprimée, je n'ai pu en faire mention dans les endroits où l'analogie des matières m'en aurait donné l'occasion. Les Additions renferment seulement quelques observations qu'il m'a paru nécessaire d'y placer, et j'espère que son indulgence et sa franchise les lui feront interpréter avec bienveillance.

Pendant l'impression, que différens obstacles ont plusieurs fois interrompue, et qui s'est prolongée pendant quatre années entières, non-seulement j'ai continué les recherches entreprises auparavant, et dont je m'étais décidé à retarder la publication, dans la crainte que l'ouvrage ne devînt trop volumineux, mais j'en ai entrepris de nouvelles. Plusieurs points que je n'ai fait, par la même raison, que toucher légérement (par exemple, aux n°s 37, 82 et sui-

vans, et en d'autres endroits), ont été repris ensuite, et m'ont donné lieu de faire des recherches plus générales, qui me semblent mériter d'être connues. (*Voyez* encore ce qui est dit dans les Additions, par rapport au n° 306.) Enfin, comme le volume devenait plus considérable que je ne m'y étais attendu, surtout à cause de la Section V, j'ai été forcé de retrancher beaucoup de choses que je me proposais d'y faire entrer, et particulièrement la Section VIII toute entière, qui traite en général des congruences algébriques de tous les degrés, et qui se trouve souvent citée. Tout cela formera facilement un volume égal à celui-ci, que je publierai lorsque les circonstances me le permettront.

Si, dans plusieurs questions difficiles, j'ai employé des démonstrations synthétiques, et supprimé l'analyse qui m'y avait conduit, je m'y suis déterminé par le desir d'abréger, auquel je devais me conformer autant qu'il était possible.

La théorie de la division du cercle, ou des polygones réguliers, qui compose la Section VII, n'appartient pas *par elle-même* à l'Arithmétique, mais ses *principes* ne peuvent être puisés que dans l'Arithmétique transcendante. Ce résultat pourra sembler aux géomètres, aussi inattendu que les vérités nouvelles qui en dérivent, et qu'ils verront, j'espère, avec plaisir.

Telles sont les choses dont j'ai cru devoir prévenir le lecteur. Quant à l'Ouvrage lui-même, il ne m'appartient pas de le juger; ce que je desire surtout, c'est qu'il plaise à ceux qui s'intéressent aux progrès des sciences, soit en ne laissant plus rien à desirer sur quelques points qui manquaient jusqu'à présent, soit en frayant la route pour d'autres découvertes.

TABLE

DES MATIÈRES.

SECTION PREMIÈRE. *Des Nombres congrus en général.*

Nombres *congrus*, *modules*, *résidus* et *non-résidus* . . . . . n° 1 — 3
Résidus *minima* 4
Propositions élémentaires sur les nombres congrus . . . . . 5 — 11
Applications. . . . . 11 et 12

SECTION SECONDE. *Des Congruences du premier degré.*

Théorèmes préliminaires sur les nombres premiers, les diviseurs, etc. n° 13 — 23
Résolution des congruences du premier degré . . . . . 24 — 31
De la recherche d'un nombre congru à des nombres donnés suivant des modules donnés . . . . . 32 — 36
Congruences du premier degré à plusieurs inconnues 37
Différens théorèmes . . . . . 38 et suiv.

SECTION TROISIÈME. *Des résidus des puissances.*

Les résidus des termes d'une progression géométrique qui commence par l'unité, forment une suite périodique . . . . . n° 45 — 48

Des modules qui sont des nombres premiers.

Si le module est un nombre premier p, le nombre des termes de la période divise nécessairement $p-1$ 49
Théorème de *Fermat*. 50, 51
A combien de nombres répondent les périodes dont le nombre des termes est un diviseur donné de $p-1$ . . . . . 52 — 56
Racines primitives, *bases*, *indices* 57
Algorithme des indices 58, 59
Des racines de la congruence $x^n \equiv A$. . . . . 60 — 68
Relation entre les indices pour différens systèmes. . . . . 69 — 71
Bases choisies pour des usages particuliers 72
Méthode pour trouver les racines primitives 73, 74
Divers théorèmes sur les périodes et les racines primitives. . . . . 75 — 81

Théorème

Théorème de *Wilson*. . . . . n° 76
Des modules qui sont des puissances de nombres premiers . . . . . 82 — 89
Des modules qui sont des puissances de 2. . . . . 90 , 91
Des modules composés . . . . . 92 , 93

SECTION QUATRIÈME. *Des congruences du second degré.*

Résidus et non-résidus quadratiques. . . . . n° 94 , 95
Toutes les fois que le module est un nombre premier, le nombre des résidus moindres que lui est égal au nombre des non-résidus. . 96 , 97
La question de savoir si un nombre composé est résidu d'un nombre premier donné, dépend de la nature de ses facteurs. . . . . 98 , 99
Des modules composés. . . . . 100 — 105
Caractère général auquel on peut reconnaître si un nombre donné est résidu ou non-résidu d'un nombre premier donné 106
Recherches sur les nombres premiers qui ont pour résidus ou non-résidus des nombres premiers donnés . . . . . 107 et suiv.
Résidu — 1 . . . . . 108 — 111
Résidu + 2 et — 2 . . . . . 112 — 116
Résidu + 3 et — 3 . . . . . 117 — 120
Résidu + 5 et — 5 . . . . . 121 — 123
Résidu + 7 et — 7 124
Préparation à une recherche générale . . . . . 125 — 129
Le théorème général (*fondamental*) s'établit par induction; conclusions qu'on en déduit. . . . . 130 — 134
Démonstration rigoureuse de ce théorème . . . . . 135 — 144
Méthode analogue de démontrer le théorème du n° 114 145
Solution du problème général 146
Des formes linéaires qui contiennent tous les nombres premiers dont un nombre quelconque donné est résidu ou non-résidu. . . . . 147 — 150
Travaux des autres géomètres sur ce sujet. 151
Des congruences complètes du second degré 152

SECTION CINQUIÈME. *Des formes et des équations du second degré.*

Objet de la recherche; définition et notation des *formes*. . . . n° 153
Représentation des nombres; *déterminans*. 154
Valeurs de l'expression $\sqrt{(b^2 - ac)}$ (mod. M), auxquelles *appartient* la représentation du nombre M par la forme (a, b, c). . . . . 155 , 156
Forme qui en *contient* une autre, ou qui y est contenue; transformation *propre* ou impropre. 157
Équivalence propre et impropre 158
Formes *opposées* 159
Contiguës 160

Diviseurs communs des coefficiens des formes. . . . . n° 161
Relation entre les transformations semblables d'une forme donnée en une autre forme donnée. 162
Formes *ambiguës*. 163
Théorème relatif au cas où une forme est contenue à-la-fois dans une autre proprement et improprement 164, 165
Considérations générales sur les représentations des nombres par les formes et leur liaison avec les transformations . . . . . 166 — 170
Des formes de déterminant négatif . . . . . 171 — 182
Applications particulières à la décomposition des nombres en deux quarrés, en un quarré et le double d'un autre, en un quarré et le triple d'un autre 182
Des formes de déterminant positif non quarré . . . . . 183 — 205
Des formes de déterminant quarré. . . . . 206 — 212
Des formes qui sont contenues dans d'autres, auxquelles elles ne sont cependant pas équivalentes. 213, 214
Des formes de déterminant $= 0$ 215
Solution générale en nombres entiers de toutes les équations indéterminées du second dégré à deux inconnues. . . . . 216 — 221
Remarques historiques 222

RECHERCHES ULTÉRIEURES SUR LES FORMES.

Distribution par *classes* des formes de déterminant donné . . . n° 223 — 225
———— Des classes en *ordres* 226, 227
Division des ordres en *genres*. . . . . 228 — 237
De la composition des formes . . . . . 238 — 244
Comparaison des ordres 245
———— des genres . . . . . 246 — 248
———— des classes . . . . . 249 — 251
Pour un déterminant donné, chaque genre d'un même ordre contient le même nombre de classes. 252
Composition des nombres de classes contenues dans deux genres d'ordres différens . . . . . 253 — 256
Du nombre de classes ambiguës . . . . . 257 — 260
Il y a toujours une moitié des caractères assignables pour un déterminant donné, à laquelle ne répond aucun genre proprement primitif (positif quand le déterminant est négatif). 261
Seconde démonstration du théorème fondamental, et des théorèmes relatifs aux résidus -1, $+2$ et -2. 262
On déterminera plus exactement cette moitié des caractères assignables auxquels ne répond aucun genre. . . . . 263 — 264
Méthode particulière pour décomposer un nombre premier donné en deux quarrés. 265

DIGRESSION CONTENANT UN TRAITÉ DES FORMES TERNAIRES, n° 266 — 285

Quelques applications à la théorie des formes binaires.

Trouver une forme de la duplication de laquelle résulte une forme binaire donnée 286

Il répond effectivement des genres à tous les caractères, excepté à ceux qui (n°s 262, 263) ont été démontrés impossibles. . . . . 287 (3°)

Théorie de la décomposition des nombres et des formes binaires en trois quarrés . . . . . 288 — 292

Démonstration des théorèmes de *Fermat*, que tout nombre entier est décomposable en trois nombres triangulaires ou en quatre quarrés 293

Résolution de l'équation $ax^2 + by^2 + cz^2 = 0$ . . . . . 294 — 295

Sur la méthode par laquelle *Legendre* a traité le théorème fondamental. . . . . 296 — 298

Représentation de zéro par des formes ternaires quelconques. 299

Résolution générale en nombres rationnels des équations indéterminées du second degré à deux inconnues 300

Du nombre *moyen* de genres. 301

——— de classes. . . . . 302 — 304

Algorithme particulier des classes proprement primitives; déterminans réguliers et irréguliers. . . . . 305 — 308

SÉCTION SIXIÈME. *Application des recherches précédentes.*

Décomposition des fractions en fractions plus simples . . . . . 309 — 311

Réduction des fractions ordinaires en fractions décimales. . . . . 312 — 318

Résolution de la congruence $x^2 \equiv A$ par une méthode d'exclusion . 319 — 322

Résolution de l'équation indéterminée $mx^2 + ny^2 = A$ par exclusions, 323 — 326

Autre méthode pour résoudre la congruence $x^2 \equiv A$, quand A est négatif. 327, 328

Deux méthodes pour distinguer les nombres composés des nombres premiers, et pour chercher leurs facteurs . . . . . 329 et suiv.

SECTION SEPTIÈME. *Des équations qui déterminent les divisions du cercle.*

On réduit la recherche au cas le plus simple, où le nombre des parties en lesquelles on doit diviser le cercle, est un nombre premier... n° 336

Équations pour les fonctions trigonométriques des arcs qui sont une ou plusieurs parties aliquotes de la circonférence. Réduction des fonctions trigonométriques aux racines de l'équation $x^n - 1 = 0$.. 337

Théorie des racines de cette équation, en supposant n un nombre premier; si l'on omet la racine 1, les autres (Ω) seront données par l'équation $X = x^{n-1} + x^{n-2} + \text{etc.} + x + 1 = 0$ 339, 340

La fonction X ne peut être décomposée en facteurs de degré moindre dans lesquels les coefficiens soient rationnels..... 341

Objet des recherches suivantes . . . . . n° 342
Toutes les racines Ω sont distribuées par périodes. 343
Divers théorèmes sur ces périodes. . . . . 344 — 351
Solution de l'équation $X = 0$, établie sur ces recherches. 352
Exemples pour $n = 19$, où la difficulté est réduite à deux équations du troisième degré et une du second, et pour $n = 17$, où elle est réduite à quatre équations du second degré. . . . . 353 , 354
Recherches ultérieures sur ce sujet. Les valeurs des périodes dans lesquelles le nombre de termes est pair, sont toujours réelles. . . 356
De l'équation qui détermine la distribution en deux, ou en trois périodes . . . . . 357 , 358
Les équations qui donnent les racines Ω peuvent toujours être ramenées à des équations à deux termes. . . . . 359 , 360
Application des recherches précédentes aux fonctions trigonométriques; Méthode pour distinguer les angles qui répondent aux différentes racines Ω. 361
On tire des sinus et cosinus les valeurs des tangentes, cotangentes, sécantes, cosécantes, sans se servir de la division. 362
Méthode pour abaisser successivement les équations qui donnent les fonctions trignométriques. . . . . 363 , 364
Divisions du cercle qui peuvent s'effectuer par de seules équations du second degré, c'est-à-dire, par des constructions géométriques, 365 , 366

ADDITIONS DE L'AUTEUR.

NOTES (*du Traducteur*) sur les n°s 162 et 164.

TABLES.

FIN DE LA TABLE DES MATIÈRES.

ERRATA.

Pages.	Lignes.	Fautes.	Corrections.
16	16	et le sera.	et le problème le sera.
21	3	$-15x \equiv 26$	$-15x \equiv -26$.
	4	$x \equiv 2$	$x \equiv -2$.
23	20	$\frac{1}{2}.\frac{2}{3}.\frac{3}{4}.\frac{4}{5}$.	$\frac{1}{2}.\frac{2}{3}.\frac{4}{5}$.
37	20	son correspondant	leurs correspondans.
39	7.	les exposans auxquels ils appartiennent b^{β}, c^{γ}, etc.	les exposans b^{β}, c^{γ}, etc. auxquels ils appartiennent.
43	19	on voit aussi.	on voit.
51	1	$a^{\beta x}$	$a^{\alpha\beta}$.
53	19	dans	parmi.
55	12	19.	10.
59	8(en rem.) (note)	$< a$	$< a^{a}$.
71	16	section première	section précédente.
75	12(en rem.)	ce qui supposerait	et supposerait.
81	7(en rem.)	dont le module est + 2	dont + 2 est résidu.
89	11 et 12 (en rem.)	$b^{\frac{p-1}{2}}$.	$b^{\frac{p-1}{2}}$.
98	2 et 3 (en rem.)	$1+A$ et $+A'$, $2+A$ et $-A'$, etc.	1...$+A$ et $+A'$, 2...$+A$ et $-A'$, etc.
102	21	et $+(T+1)Np$	et $+(T+1)Np$).
104	6	n'est pas.	n'est.
115	3 (note)	in	is.
116	15	fondamental. Il nous.	fondamental, il nous.
117	2(en rem.)	la	les.
120	14	v.	V.
122	20	forme.	transformation.
140	14(en rem.)	m', n', m, n	μ', ν', μ, ν.
141	7(en rem.)	$ut = -D$	et $= -D$.
154	12(en rem.)	de ces.	des.
162	21	réduites de (2°).	réduites, et de (2°).
178	6(en rem.)	$kq - kl = 1$	$kq - pl = 1$.
	7(en rem.)	$kq + kp$.	$kq + pl$.
182	3(en rem.) [(note)	$\mp\gamma A'$	$\mp rA'$.
186	10	44.	42.
193	11	ce nombre.	le nombre.
	12	B	D.
206	6(en rem.)	parconséquent qu'à prendre.	qu'à prendre.
207	11(en rem.)	$(m'; m-1)$.	$(m'; m'-1)$.
212	12	étant.	est.
214	8(en rem.)	$\alpha X + \beta\gamma$	$\alpha X + \beta Y$.
	10 (*idem.*)	$BG - \alpha H$.	$\beta G - \alpha H$.

Pages.	Lignes.	Fautes.	Corrections.
220	17	par la solution se trouver . . .	se trouver par la solution.
221	15	x pair.	n pair.
	22	entières.	fractionnaires.
223	12(en rem.)	représentatives.	représentantes.
224	6(en rem.)	membre.	terme.
234	5(en rem.)	forme	classe.
239	dernière	$\pm A^{\alpha}, B^{\beta}, C^{\gamma}$	$\pm A^{\alpha}.B^{\beta}.C^{\gamma}$.
240	7	Respectivement	respectivement.
	20 et 22	ordre.	genre.
244	5 (note)	$pq' - p'q = 0$.	$pq' - p'q = P$.
257	1	des formes ff'.	des formes f, f'.
	12	f'', F par.	f'', F; par
263	1 et 2	$\pi + \delta$, $\pi' + \delta'$, etc.	$\varpi + \delta$, $\varpi' + \delta'$, etc.
268	dernière	m étant $= 1$.	m' étant $= 1$.
269	10	trouveront.	trouvera.
274	9	proprement	improprement.
277	7	F et f'.	F et f.
295	2	K, K', K''.	k, k', k''.
307	9	γ	g.
321	9(en rem.)	binaires.	ternaires.
	10 (*idem*)	représenter	présenter.
	16 (*idem*)	$2x^2 + yz$	$2x^2 + 2yz$.
322	20	a, b', b''	b, b', b''.
334	12	φ par f.	Φ par f.
344	4(en rem.)	donnant.	donnent.
365	13	$ab = b'b'' = B$.	$ab - b'b'' = B$.
375	19	prétention.	pénétration.
378	12	Ainsi il est clair que de la composition de tant de classes qu'on voudra d'une même période, il résulte une classe contenue dans la période $C^{\varepsilon}, C^{\varepsilon'}, C^{\varepsilon''}$, etc. $= C^{\varepsilon+\varepsilon'+\varepsilon''+\text{etc.}}$	Ainsi il est clair que de la composition de tant de classes $C^{\varepsilon}, C^{\varepsilon'}, C^{\varepsilon''}$, etc. qu'on voudra, il résulte une classe $C^{\varepsilon+\varepsilon'+\varepsilon''+\text{etc.}}$, contenue dans la même période.
385	18	forme.	classe.
399	9	résidus	non-résidus.
401	12 et 13	$=$.	$\equiv$.
438	19	que n.	que λ.
439	19	$[\lambda h^2]$, $[\lambda h]$.	$[h\lambda]$, $[\lambda h^2]$
441	8(en rem.)	des.	de.
453	12	indéterminée.	déterminée.
457	4	$(2, 9) =$ 0,80, etc.	$(2, 9) = -$ 0,80, etc.

RECHERCHES

ARITHMÉTIQUES.

SECTION PREMIÈRE.

Des Nombres congrus en général.

1. Si un nombre a divise la différence des nombres b et c, b et c sont dits *congrus* suivant a, sinon *incongrus*. a s'appellera le module ; chacun des nombres b et c, *résidus* de l'autre dans le premier cas, et *non résidus* dans le second.

Les nombres peuvent être positifs ou négatifs, mais entiers. Quant au module il doit évidemment être pris absolument, c'est-à-dire, sans aucun signe.

Ainsi -9 et $+16$ sont *congrus* par rapport au module 5; -7 est *résidu* de 15 par rapport au module 11, et *non résidu* par rapport au module 3.

Au reste 0 étant divisible par tous les nombres, il s'ensuit qu'on peut regarder tout nombre comme congru avec lui-même par rapport à un module quelconque.

2. Tous les résidus d'un nombre donné a suivant le module m, sont compris dans la formule $a + km$, k étant un entier indéterminé. Les plus faciles des propositions que nous allons exposer

peuvent sans peine se démontrer par-là; mais chacun en sentira la vérité au premier aspect.

Nous désignerons dorénavant la congruence de deux nombres par ce signe $\equiv$, en y joignant, lorsqu'il sera nécessaire, le module renfermé entre parenthèses; ainsi $-16\equiv 9 \pmod 5$, $-7\equiv 15 \pmod{11}$ (*).

3. THÉORÈME. Soient m *nombres entiers successifs* a, $a+1$, $a+2$, ... $a+m-1$ *et un autre* A, *un des premiers sera congru avec* A, *suivant le module* m, *et il n'y en aura qu'un.*

En effet, si $\frac{a-A}{m}$ est entier, on aura $a\equiv A$; s'il est fractionnaire, soit k le nombre entier, immédiatement plus grand ou plus petit, suivant que $\frac{a-A}{m}$ sera positif ou négatif, en ne faisant point d'attention au signe; $A+km$ tombera nécessairement entre a et $a+m$; ce sera donc le nombre cherché. Or il est évident que les quotiens $\frac{a-A}{m}$, $\frac{a+1-A}{m}$, etc., sont compris entre $k-1$ et $k+1$, donc un seul d'entr'eux peut être entier.

4. Il suit de là que chaque nombre aura un résidu, tant dans la suite $0, 1, 2, \ldots (m-1)$, que dans celle-ci $0, -1, -2, \ldots -(m-1)$; nous les appellerons résidus *minima*; et il est clair qu'à moins que 0 ne soit résidu, il y en aura toujours deux, l'un positif, l'autre négatif. S'ils sont inégaux, l'un d'eux sera $<\frac{m}{2}$; s'ils sont égaux, chacun d'eux $=\frac{m}{2}$ sans avoir égard au signe; d'où il suit qu'un nombre quelconque a un résidu qui ne surpasse pas la moitié du module, et que nous appellerons résidu *minimum absolu.*

Par exemple -13 suivant le module 5, a pour résidu *minimum*

(*) Nous avons adopté ce signe à cause de la grande analogie qui existe entre l'égalité et la congruence. C'est pour la même raison que Legendre, dans des mémoires que nous aurons souvent occasion de citer, a employé le signe même de l'égalité, pour désigner la congruence; nous en avons préféré un autre, pour prévenir toute ambiguité.

positif 2, qui est en même temps *minimum absolu*, et -3 pour résidu *minimum* négatif; $+5$, suivant le module 7, est lui-même son résidu *minimum* positif; -2 est le résidu *minimum* négatif et en même temps le *minimum absolu*.

5. Des notions que nous venons d'établir, nous tirerons d'abord les conséquences suivantes :

Les nombres qui sont congrus suivant un module composé, le sont également suivant un quelconque de ses diviseurs.

Si plusieurs nombres sont congrus à un même suivant le même module, ils seront congrus entre eux (toujours suivant le même module).

On doit supposer la même identité de module dans ce qui suit.

Les nombres congrus ont les mêmes résidus minima; *les nombres incongrus les ont différens.*

6. *Si les nombres* A, B, C, *etc.*; a, b, c, *etc. sont congrus chacun à chacun, c'est-à-dire, si* $A \equiv a$, $B \equiv b$, *etc. on aura...*

$$A + B + C + \text{etc.} \equiv a + b + c + \text{etc.}$$

Si $A \equiv a$, $B \equiv b$, on a aussi $A - B \equiv a - b$.

7. *Si* $A \equiv a$, *on a aussi* $kA \equiv ka$.

Si k est positif, ce n'est qu'un cas particulier de l'article précédent, en posant $A = B = C$, etc., $a = b = c$, etc.

Si k est négatif, $-k$ sera positif; donc $-kA \equiv -ka$, et partant $kA \equiv ka$.

Si $A \equiv a$, $B \equiv b$, $AB \equiv ab$; car $AB \equiv Ab \equiv ba$.

8. Si les nombres A, B, C, etc., a, b, c, etc. sont congrus chacun à chacun, les produits ABC, etc., et abc, etc. seront congrus.

Par l'article précédent, $AB \equiv ab$; par la même raison $ABC \equiv abc$, et ainsi de suite.

En prenant tous les nombres A, B, C, etc., égaux entr'eux, ainsi que les correspondans a, b, c, etc., on déduit ce théorème :

Si $A \equiv a$ *et que* k *soit entier positif, on aura* $A^k \equiv a^k$.

9. *Soit* X *une fonction de l'indéterminée* x, *de cette forme....* $Ax^a + Bx^b + Cx^c$, *etc.*, A, B, C, *etc, étant des nombres entiers quelconques*, a, b, c, *etc. des nombres entiers positifs. Si l'on*

donne à x des valeurs congrues, suivant un certain module, les valeurs résultantes pour X, *le seront aussi.*

Soient f et g les valeurs congrues de x; par les articles précédens $f^a \equiv g^a$ et $Af^a \equiv Ag^a$; de même $Bf^b \equiv Bg^b$, etc. : donc

$$Af^a + Bf^b + Cf^c + \text{etc.} \equiv Ag^a + Bg^b + Cg^c + \text{etc.}$$

Au reste on conçoit aisément que ce théorème peut s'étendre à des fonctions de plusieurs indéterminées.

10. Si donc on substitue à la place de x tous les nombres entiers consécutifs, et que l'on cherche les résidus *minima* des valeurs de X, ils formeront une suite dans laquelle, après un intervalle de m termes (m étant le module), les mêmes termes se représenteront; c'est-à-dire que cette suite sera formée d'une période de m termes répétée indéfiniment.

Soit par exemple : $X = x^3 - 8x + 6$ et $m = 5$, pour $x = 0, 1, 2, 3$, etc. les valeurs de X donnent pour résidus *minima* positifs : 1, 4, 3, 4, 3, 1, 4, etc., où les cinq premiers 1, 4, 3, 4, 3 se répètent indéfiniment; et si l'on continue la série en sens contraire, c'est-à-dire, si l'on donne à x des valeurs négatives, la même période reparaît en sens inverse; d'où il suit que la série ne renferme pas d'autres termes que ceux qui composent la période.

11, Donc dans cet exemple, X ne peut devenir $\equiv 0$, ni $\equiv 2$, (mod. 5), et encore moins $= 0$ ou $= 2$, d'où il suit que les équations $x^3 - 8x + 6 = 0$ et $x^3 - 8x + 4 = 0$ n'ont point de racines entières, et parconséquent point de racines rationnelles. On voit en général que lorsque X est de la forme $x^n + Ax^{n-1} + Bx^{n-2} + \text{etc.} + N$; A, B, C, etc. étant entiers, et n entier positif, l'équation $X = 0$, (forme à laquelle toute équation algébrique peut se ramener) n'aura aucune racine rationnelle, s'il arrive que pour un certain module la congruence $X \equiv 0$ ne soit pas satisfaite; mais ce caractère qui se présente ici de lui-même, sera développé davantage dans la section VIII. On peut au moins se former par cette esquisse une idée de l'utilité de nos recherches.

12. Plusieurs des théorèmes que l'on a coutume d'exposer dans les traités d'arithmétique, s'appuient sur ceux que nous avons pré-

sentés ; par exemple, la règle pour reconnaître si un nombre est divisible par 9, 11, ou tout autre nombre. Suivant le module 9 toutes les puissances de 10 sont congrues à l'unité ; donc si le nombre est de la forme $a+10b+100c+1000d+$etc., il aura, suivant le module 9, le même résidu *minimum* que $a+b+c+$etc. Il est clair d'après cela, que si l'on ajoute les figures du nombre, sans avoir égard au rang qu'elles occupent, la somme que l'on obtiendra, et le nombre proposé auront les mêmes résidus *minima* ; si donc ce dernier est divisible par 9, la somme des chiffres le sera aussi, et seulement dans ce cas. Il en est de même du diviseur 3. Comme suivant le module 11, $100\equiv+1$, on aura généralement $10^{2k}\equiv 1$, $10^{2k+1}\equiv 10\equiv-1$, et le nombre de la forme $a+10b+100c+$etc., aura le même résidu *minimum* que $a-b+c-$etc. ; d'où dérive sur-le-champ la règle connue. On déduira facilement du même principe toutes les règles semblables.

Ce qui précède donne encore la raison des règles que l'on prescrit ordinairement pour la vérification des opérations arithmétiques ; savoir, lorsque de nombres donnés on doit en déduire d'autres par addition, soustraction, multiplication ou élévation aux puissances. On n'a qu'à substituer dans les opérations, à la place des nombres donnés, leurs résidus *minima*, suivant un module quelconque (ordinairement 9 ou 11, parceque dans le système décimal, comme nous venons de le voir, on trouve facilement les résidus relatifs à ces modules) ; les nombres résultans devront être congrus à ceux qu'on déduirait des nombres donnés, sinon il y aurait un vice dans le calcul.

Mais il serait superflu de nous arrêter plus long-temps sur ces résultats très-connus, ainsi que sur ceux du même genre.

SECTION SECONDE.

Des Congruences du premier degré.

13. THÉORÈME. *Le produit de deux nombres positifs plus petits qu'un nombre premier donné, ne peut être divisé par ce nombre premier.*

Soit p le nombre premier et $a < p$ et > 0; je dis qu'on ne pourra trouver aucun nombre positif b, plus petit que p, qui rende

$$ab \equiv 0 \text{ (module } p \text{)}.$$

En effet, s'il peut y en avoir, supposons que ce soient les nombres b, c, d, etc, tous plus petits que p, ensorte qu'on ait $ab \equiv 0$, $ac \equiv 0$, etc., (mod. p), soit b le plus petit de tous, desorte qu'on n'en puisse supposer un plus petit que b, on aura évidemment $b > 1$; car si $b = 1$, on aurait $ab = a < p$ et partant non divisible par p. Or p comme nombre premier ne peut être divisé par b, mais tombera entre deux multiples de b, mb et $(m+1)\,b$. Soit $p - mb = b'$, b' sera positif et $< b$. Or nous avons supposé $ab \equiv 0$ (mod. p), on aura donc $mab \equiv 0$; et retranchant de $ap \equiv 0$, on aura $a(p - mb) = ab' \equiv 0$; donc b' devrait être mis au rang des nombres b, c, d, etc., et serait plus petit que le plus petit de tous, ce qui est contre la supposition.

14. *Si aucun des deux nombres* a *et* b *n'est divisible par un nombre premier* p, *le produit* ab *ne le sera pas non plus.*

Soient α et β les résidus *minima* positifs des nombres a et b, suivant le module p, aucun d'eux ne sera nul par hypothèse. Or si l'on avait $ab \equiv 0$, comme $ab \equiv \alpha\beta$, on aurait $\alpha\beta \equiv 0$, ce qui serait contraire au théorème précédent.

La démonstration de ce théorème a déjà été donnée par Euclide, *El.* VII, 32. Nous n'avons pas cependant voulu l'omettre, tant parceque plusieurs auteurs modernes ont présenté des raisonnemens vagues au lieu de démonstration, ou bien ont négligé ce théorème; que dans le but de faire mieux saisir, par ce cas très-simple, l'esprit de la méthode que nous appliquerons par la suite à des points bien difficiles.

15. *Si aucun des nombres* a, b, c, d, *etc. n'est divisible par le nombre premier* p, *le produit* abcd, *etc. ne le sera pas non plus.*

Suivant l'article précédent, ab n'est pas divisible par p; donc il en est de même de abc, et ainsi de suite.

16. THÉORÈME. *Un nombre composé ne peut se résoudre que d'une seule manière, en facteurs premiers.*

Il est évident par les élémens, que l'on peut toujours décomposer un nombre quelconque en facteurs premiers; mais on suppose à tort tacitement que cette décomposition ne soit possible que d'une manière. Imaginons qu'un nombre composé..... $A = a^{\alpha} b^{\beta} c^{\gamma}$ etc., a, b, c, etc. étant des nombres premiers inégaux, soit encore décomposable d'une autre manière en facteurs premiers. Il est d'abord manifeste que dans ce second système de facteurs il ne peut entrer d'autres nombres premiers que a, b, c, etc., puisque quelqu'autre que ce fût ne pourrait diviser A, qui est composé des premiers. De même aucun des nombres premiers a, b, c, etc. ne peut y manquer, car sans cela il ne diviserait pas A (n° 15); la différence ne peut donc porter que sur les exposans. Or soit un nombre premier p, qui ait dans l'un des systèmes l'exposant m, et dans l'autre l'exposant n, m étant $> n$: divisons de part et d'autre par p^n, p restera dans l'un affecté de l'exposant $m-n$, et disparaîtra de l'autre, donc $\frac{A}{p^n}$ pourrait se décomposer de deux manières, dans l'une desquelles p n'entrerait pas, tandis qu'il resterait dans l'autre, ce qui est contre ce que nous avons démontré.

17. Si donc le nombre A est le produit de B, C, D, etc., il s'ensuit que les nombres B, C, D, etc ne peuvent avoir de facteurs premiers différens de ceux de A, et que chacun de ces facteurs doit

se trouver autant de fois dans les nombres B, C, D, etc, pris ensemble, que dans A. On déduit de là le caractère pour reconnaître si le nombre B divise ou non un autre nombre A. Il le divisera s'il ne contient aucun facteur premier étranger à A, ni aucune puissance plus grande d'un des facteurs premiers de A. Si une de ces conditions manque, B ne divisera pas A.

A l'aide du calcul des combinaisons, on verra aisément que si... $A = a^{\alpha}\, b^{\beta}\, c^{\gamma}$ etc, a, b, c, etc. étant comme ci-dessus des nombres premiers différens, le nombre des diviseurs différens de A, en y comprenant 1 et A, est $(\alpha+1)(\beta+1)(\gamma+1)$ etc.

18. Si donc $A = a^{\alpha}\, b^{\beta}\, c^{\gamma}$ etc., $K = k^{\kappa} l^{\lambda} m^{\mu}_{,,}$ etc., et si tous les facteurs a, b, c, etc. diffèrent des facteurs k, l, m, etc.; A et K n'auront d'autre diviseur commun que 1, ou bien seront premiers entr'eux.

Le plus grand commun diviseur entre plusieurs nombres donnés A, B, C, etc. se trouve de la manière suivante : On décompose les nombres en facteurs premiers, et l'on prend ceux qui sont communs à tous les nombres A, B, C, etc. (s'il n'y en avait pas de tels, les nombres donnés n'auraient pas de commun diviseur); alors on remarque quels sont les exposans de ces facteurs, dans chacun des nombres A, B, C, etc.; on donne à chaque facteur le plus petit des exposans qu'il a dans A, B, C, etc., et l'on compose un produit des puissances qui en résultent; ce sera le plus grand commun diviseur cherché.

Si l'on cherchait au contraire le plus petit nombre divisible à-la-fois, par les nombres A, B, C, etc., on prendrait tous les nombres premiers qui diviseraient quelqu'un des nombres A, B, C, etc, et on donnerait à chacun d'eux le plus haut exposant qu'il ait dans les nombres A, B, C, etc. Le produit de toutes ces puissances serait le nombre cherché.

Soient, par exemple,

$$A = 504 = 2^3 . 3^2 . 7 \; ; \; B = 2880 = 2^6 . 3^2 . 5 \; ; \; C = 864 = 2^5 . 3^3 .$$

Pour trouver le plus grand diviseur commun, on a les facteurs premiers 2 et 3, qui doivent être affectés des exposans 3 et 2, d'où il vient $2^3 . 3^2 = 72$. Quant au plus petit nombre divisible par A, B, C, il sera $2^6 . 3^3 . 5 . 7 = 6048$.

Nous

Nous omettons les démonstrations à cause de leur facilité ; d'ailleurs on sait par les élémens comment on résout ces problêmes, quand les nombres A, B, C, etc. ne sont point donnés tout décomposés en facteurs.

19. *Si les nombres* a, b, c, etc. *sont premiers avec* k, *leur produit l'est aussi.*

En effet, puisqu'aucun des nombres a, b, c, etc. n'a de facteurs premiers communs avec k, et que le produit de ces nombres ne peut avoir de facteurs premiers qui n'appartiennent à quelqu'un d'entr'eux, ce produit n'aura non plus aucun facteur premier commun avec k.

Si les nombres a, b, c, *etc. sont premiers entr'eux, et que* k *soit divisible par chacun d'eux, il le sera aussi par leur produit.*

C'est une suite des nos 17 et 18. Soit en effet p un diviseur premier quelconque du produit abc etc. et qu'il ait l'exposant π, quelqu'un des nombres a, b, c, etc. sera divisible par p^{π}, parconséquent k, qui est divisible par ce nombre, le sera aussi par p^{π} : il en sera de même des autres diviseurs du produit.

Donc, *si deux nombres* m, n *sont congrus suivant plusieurs modules* a, b, c, etc. *premiers entr'eux, ils le seront aussi suivant leur produit.* En effet, puisque $m-n$ est divisible par chacun des nombres a, b, c, etc., il le sera aussi par leur produit.

Enfin, *si* a *est premier avec* b, *et que* ak *soit divisible par* b, k *sera aussi divisible par* b. En effet, puisque ak est divisible par a et par b, il le sera par leur produit ; donc $\frac{ak}{ab}=\frac{k}{b}$ sera un entier.

20. *Quand* $A=a^{\alpha}b^{\beta}c^{\gamma}$ *etc.* (a, b, c, *etc. étant des nombres premiers inégaux*), *est une puissance parfaite, par exemple, quand* $A=k^n$, *tous les exposans* α, β, γ, *etc. sont divisibles par* n.

En effet, le nombre k n'est pas divisible par d'autres nombres premiers que a, b, c, etc ; soit α' l'exposant de a dans k, dans k^n ce sera $n\alpha'$; donc $n\alpha'=\alpha$ et $\frac{\alpha}{n}$ est un entier. On démontrera de même que $\frac{\beta}{n}, \frac{\delta}{n}$, etc. sont des nombres entiers.

21. *Quand* a, b, c, *etc. sont premiers entr'eux, et que le produit*

abc *etc. est une puissance parfaite* k^n, *chaque nombre* a, b, c, *etc. est une puissance semblable.*

Soit $a = l^\lambda m^\mu p^\pi$ etc., l, m, p, etc. étant des nombres premiers différens, dont aucun par hypothèse ne divise les nombres b, c, etc., puisque le produit abc etc. est divisible par $l^\lambda m^\mu p^\pi$ etc., on se convaincra, comme dans l'article précédent, que λ, μ, π, etc. sont divisibles par n, et partant que $\sqrt[n]{a}$ est entier. Il en sera de même pour b, c, etc.

Après ces notions nécessaires sur les nombres premiers, nous allons nous occuper de ce qui peut nous conduire plus directement à notre but.

22. *Si les nombres* a *et* b *divisibles par* k *sont congrus suivant le module* m *premier avec* k, $\frac{a}{k}$ *et* $\frac{b}{k}$ *sont congrus suivant le même module.*

En effet $a-b$ est évidemment divisible par k, et, suivant l'hypothèse, par m; donc $\frac{a-b}{k}$ sera divisible par m (19), c'est-à-dire, que $\frac{a}{k} \equiv \frac{b}{k}$ (mod. m).

Mais si, toutes choses d'ailleurs égales, m et k ont un diviseur commun e, on aura $\frac{a}{k} \equiv \frac{b}{k} \left(\text{mod.} \frac{m}{e}\right)$; car $\frac{k}{e}$ et $\frac{m}{e}$ sont premiers entr'eux; mais $a-b$ est divisible par k et par m; donc $\frac{a-b}{e}$ est divisible par $\frac{k}{e}$ et par $\frac{m}{e}$, et par conséquent par $\frac{mk}{e^2}$; c'est-à-dire que $\frac{a-b}{k}$ est divisible par $\frac{m}{e}$, ou que $\frac{a}{k} \equiv \frac{b}{k} \left(\text{mod.} \frac{m}{e}\right)$.

23. *Si* a *est premier avec* m, *que* e *et* f *soient des nombres incongrus suivant le module* m, ae *et* af *seront aussi incongrus.*

Cette proposition est l'inverse de celle du n° précédent.

Il est évident d'après cela, que si l'on multiplie a par tous les nombres entiers, depuis o jusqu'à $m-1$, et qu'on cherche les restes *minima* des produits, suivant le module m, ils seront tous inégaux; mais le nombre de ces résidus est m, et comme aucun d'eux n'est $> m$, ils se trouveront tous dans la série depuis o jusqu'à m.

24. L'expression $ax+b$, a et b étant des nombres donnés et x un nombre indéterminé ou variable, peut devenir congrue à un nombre donné quelconque, suivant le module m, premier avec a. Soit c le nombre auquel l'expression $ax+b$ doit être congrue, et e le résidu *minimum* positif de $c-b$. Par le n° précédent on trouvera nécessairement une valeur de $x<m$, telle que le résidu *minimum* du produit ax, suivant le module m, soit e. Nommons ν cette valeur, on aura $a\nu\equiv e\equiv c-b$; donc $a\nu+b\equiv c$ (mod. m).

25. Nous appelons *congruence* l'expression de deux quantités congrues, à l'instar des équations; si elle renferme une inconnue, la *résoudre*, c'est trouver pour cette inconnue une valeur qui satisfasse à la congruence, c'est-à-dire la racine de cette congruence. On conçoit par là ce que c'est qu'une congruence *résoluble*, et une congruence *irrésoluble*. On voit enfin que nous emploierons les mêmes distinctions qui ont lieu dans les équations. Nous verrons plus bas des exemples de congruences *transcendantes*. Quant aux congruences algébriques, elles se divisent selon la plus haute puissance de l'inconnue, en congruences du premier, du second degré, etc. On peut même proposer plusieurs congruences qui renferment plusieurs inconnues, et de l'élimination desquelles nous traiterons.

26. La congruence du premier degré $ax+b\equiv c$ se résout toujours par le n° 24, quand le module est premier avec a; et si ν est la valeur convenable de x, ou la racine de la congruence, il est évident que tous les nombres congrus à ν, suivant le module de la congruence, seront aussi des racines (n° 9). Il n'est pas moins évident que toutes les racines doivent être congrues à ν: en effet, si t est une autre racine, on aura $a\nu+b\equiv at+b$; donc $a\nu\equiv at$, et partant $\nu\equiv t$. On peut conclure de là que la congruence $x\equiv\nu$ (mod. m), donne la résolution complète de la congruence $ax+b\equiv c$.

Comme les résolutions de la congruence par les valeurs de x congrues à ν, se présentent d'elles-mêmes, et que sous cet aspect les nombres congrus doivent être considérés comme équivalens, nous regarderons ces solutions comme une seule et même. C'est pourquoi nous dirons que la congruence $ax+b\equiv c$, qui n'en admet pas d'autres, ne peut être résolue que d'une seule manière ou n'a qu'une seule racine. Ainsi, par exemple, la congruence..... $6x+5\equiv 13$ (mod. 11), n'admet pas d'autres racines que celles qui

sont $\equiv 5$ (mod. 11). La même chose n'a pas lieu dans les congruences des degrés supérieurs, et dans celles du premier degré où le coefficient de l'inconnue n'est pas premier avec le module.

27. Il nous reste à donner quelques détails sur la manière de résoudre ces congruences. Observons d'abord que la congruence..... $ax+t\equiv u$, dans laquelle le module est supposé premier avec a, dépend de celle-ci, $ax\equiv\pm 1$. En effet, si $x\equiv r$ satisfait à celle-ci, $x\equiv\pm r(u-t)$ satisfera à la première; mais en désignant le module par b, la congruence $ax\equiv\pm 1$ équivaut à l'équation indéterminée $ax=by\pm 1$, dont la solution est connue; aussi nous nous contenterons de donner ici l'algorithme du calcul.

Si les quantités A, B, C, etc. dépendent de α, β, γ, etc. de manière qu'on ait $A=\alpha$, $B=\beta A+1$, $C=\gamma B+A$, $D=\delta C+B$, etc.; nous les représenterons pour abréger, par $A=[\alpha]$, $B=[\alpha,\beta]$, $C=[\alpha,\beta,\gamma]$, $D=[\alpha,\beta,\gamma,\delta]$, etc. (*). Soit maintenant l'équation $ax=by\pm 1$, où a et b sont positifs. Supposons, ce qui est permis, que a n'est pas $< b$. Alors en opérant comme on le fait ordinairement pour la recherche du plus grand diviseur commun, on formera par la division les équations

$$a=\alpha b+c,\ b=\beta c+d,\ c=\gamma d+e, \text{ etc.}$$

dans lesquelles $\alpha, \beta, \gamma, \delta$, etc., sont entiers et positifs : et b, c, d, etc. vont en diminuant continuellement jusqu'à ce qu'on

---

(*) On peut considérer cette relation de quantités d'une manière plus générale, ainsi que nous pourrons le faire dans une autre occasion. Nous ajouterons seulement ici deux propositions qui trouvent leur application dans la question présente, savoir :

1°. $[\alpha,\epsilon,\gamma,\ldots\lambda,\mu].[\epsilon,\gamma,\ldots\lambda]-[\alpha,\epsilon,\gamma,\ldots\lambda].[\epsilon,\gamma,\ldots\lambda,\mu]=\pm 1$; où l'on prendra le signe supérieur, lorsque le nombre des quantités $\alpha, \epsilon, \gamma\ldots\lambda, \mu$, sera pair, et le signe inférieur dans le cas contraire.

2°. On peut renverser l'ordre des quantités α, ϵ, γ, etc.; desorte que..... $[\alpha,\epsilon,\gamma,\ldots\lambda,\mu]=[\mu,\lambda,\ldots\gamma,\epsilon,\alpha]$.

Nous supprimons ici les démonstrations qui n'offrent aucune difficulté.

parvienne à $m=\mu n+1$; ce qui doit toujours arriver. Il en résultera $a=[n,\mu\ldots\gamma,\beta,\alpha]$; $b=[n,\mu\ldots\gamma,\beta]$; et si l'on prend $x=[\mu,\ldots\gamma,\beta]$, $y=[\mu,\ldots\gamma,\beta,\alpha]$, on aura $ax=by+1$, quand le nombre des lettres $\alpha,\beta,\gamma\ldots\mu$, n est pair, et $ax=by-1$, quand il est impair.

28. *Euler* est le premier qui ait donné la résolution de ces équations (*Comment. de Petersb. T. VII, p.* 46). La méthode qu'il a employée consiste à substituer d'autres inconnues à la place de x et de y, elle est d'ailleurs assez connue. *Lagrange* a traité le problême d'une manière un peu différente. Il observe que si l'on réduit la fraction $\frac{a}{b}$ en fraction continue

$$\frac{1}{\alpha}+\frac{1}{\beta}+\frac{1}{\gamma}+\text{etc.}+\frac{1}{\mu}+\frac{1}{n}$$

et qu'après avoir effacé sa dernière partie $\frac{1}{n}$, on la ramène à une fraction ordinaire $\frac{x}{y}$, on aura $ax=by\pm 1$. Au reste les deux méthodes conduisent au même algorithme. Les recherches de Lagrange se trouvent dans l'*Histoire de l'Académie de Berlin*, *année* 1767, pag. 175, et avec d'autres, dans les *Additions à l'Algèbre d'Euler*.

29. La congruence $ax+t\equiv u$, dans laquelle le module n'est pas premier avec a, se ramène facilement au cas précédent. Soit m le module et δ le plus grand diviseur commun entre a et m; il est clair d'abord que toute valeur de x qui satisfera à la congruence, suivant le module m, y satisfera aussi suivant le module δ (n° 5). Mais puisque δ divise a, on a toujours $ax\equiv 0$ (mod. δ); donc on doit avoir $t\equiv u$ (mod. δ), ou $t-u$ divisible par δ, pour que la congruence soit résoluble.

Posons donc $a=\delta e$, $m=\delta f$, $t-u=\delta k$; e et f seront premiers entr'eux, et la congruence proposée $\delta ex+\delta k\equiv 0$ (mod. δf), équivaudra à celle-ci, $ex+k\equiv 0$ (mod. f); c'est-à-dire, que toute valeur de x qui satisfera à la seconde, satisfera aussi à la première, *et vice versâ*. En effet, $ex+k$ sera divisible par f, quand $\delta ex+\delta k$ le sera par δf, et réciproquement. Mais nous avons résolu la congruence

$ex+k\equiv 0 \pmod{f}$; il suit de là que si ν est une des valeurs de x, la congruence $x\equiv\nu \pmod{f}$, donne la résolution complète de la proposée.

3o. Quand le module est composé, il est toujours avantageux d'employer la méthode suivante :

Soit le module $=mn$, et la congruence proposée $ax\equiv b$. Résolvons d'abord la congruence suivant le module m, et supposons qu'elle soit satisfaite si $x\equiv\nu\left(\text{mod.}\frac{m}{\delta}\right)$; δ étant le plus grand commun diviseur des nombres m et a. Or il est évident que toute valeur de x qui satisfera à la congruence $ax\equiv b \pmod{mn}$, satisfera aussi à la congruence $ax\equiv b \pmod{m}$, et que partant elle sera comprise dans la formule $\nu+\frac{m}{\delta}x'$, x' désignant un nombre indéterminé. La réciproque de cette proposition n'est pas vraie ; x' doit donc être déterminé de manière à rendre $\nu+\frac{m}{\delta}x'$, racine de la congruence $ax\equiv b \pmod{mn}$; on aura donc $\frac{amx'}{\delta}+a\nu\equiv b \pmod{mn}$ ou $\frac{a}{\delta}x'\equiv\frac{b-a\nu}{m} \pmod{n}$. Il suit de là que la résolution d'une congruence quelconque du premier degré, suivant le module mn, peut se ramener à celle de deux congruences, suivant les modules m et n. On voit facilement que si n est lui-même le produit de deux facteurs, la solution de la congruence, suivant le module n, dépend de la solution de deux congruences dont ces facteurs sont les modules ; et généralement, que la résolution d'une congruence suivant un module composé quelconque, dépend de la résolution d'autres congruences, dont les modules sont les facteurs du premier. Ces modules peuvent être choisis de manière à être des nombres premiers, si on le trouve plus commode.

Soit par exemple la congruence $19x\equiv 1 \pmod{140}$; si on la résout d'abord suivant le module 2, on aura $x\equiv 1 \pmod{2}$; en faisant $x=1+2x'$, il viendra $38x'\equiv -18 \pmod{140}$ ou $19x'\equiv -9 \pmod{70}$. Si l'on résout celle-ci encore suivant le module 2, on aura $x'\equiv 1 \pmod{2}$, et en posant $x'=1+2x''$, on aura $38x''\equiv -28 \pmod{70}$ ou $19x''\equiv -14 \pmod{35}$. Cette congruence résolue suivant le module 5, donne $x''\equiv 4 \pmod{5}$; prenant $x''=4+5x'''$, il vient

$95x''' \equiv -90 \pmod{35}$ ou $19x''' \equiv -18 \pmod{7}$, qui donne $x''' \equiv 4 \pmod{7}$, d'où $x''' = 2 + 7x^{IV}$. Or en remontant à la valeur de x, on trouve $x = 59 + 140x^{IV}$; donc $x \equiv 59$.

31. De la même manière que la racine de l'équation $ax = b$, s'exprime par $\frac{b}{a}$, nous désignerons par $\frac{b}{a}$ la racine d'une congruence $ax \equiv b$, en y joignant le module pour la spécifier. Ainsi $\frac{19}{17} \pmod{12}$ représente un nombre quelconque qui est $\equiv 11 \pmod{12}$, et qui, par analogie, peut s'exprimer par $\frac{11}{1} \pmod{12}$.

Il suit de là généralement que le symbole $\frac{b}{a} \pmod{c}$ ne signifie rien de réel, ou si l'on aime mieux, est une expression imaginaire, si a et c ont un diviseur commun qui ne divise pas b; mais, ce cas excepté, l'expression $\frac{b}{a} \pmod{c}$ a toujours des valeurs réelles, et en a même une infinité : elles seront toutes congrues suivant c, si c est premier avec a et suivant $\frac{c}{\delta}$, quand δ est le plus grand commun diviseur de a et de c.

Ces expressions se calculent presque de même que les fractions ordinaires, et voici quelques propriétés qui se déduisent facilement de ce qu'on a vu.

1°. Si $a \equiv \alpha$, $b \equiv \beta$ suivant le module c, les expressions $\frac{a}{b} \pmod{c}$, $\frac{\alpha}{\beta} \pmod{c}$ sont équivalentes.

2°. $\frac{a\delta}{b\delta} \pmod{c\delta}$ et $\frac{a}{b} \pmod{c}$ sont équivalentes.

3°. $\frac{ak}{bk} \pmod{c}$ et $\frac{a}{b} \pmod{c}$, sont équivalentes quand k est premier avec c.

Nous pourrions rapporter plusieurs propositions semblables; mais comme elles n'ont aucune difficulté, et qu'elles sont inutiles pour ce qui suivra, nous passerons à autre chose.

32. On peut facilement, au moyen de ce qui précède, *trouver tous les nombres qui ont des résidus donnés, suivant des modules*

quelconques; problême qui sera d'un fréquent usage dans la suite. Soient d'abord deux modules, A, B, suivant lesquels le nombre cherché z doit être congru aux nombres a et b. Toutes les valeurs de z sont nécessairement renfermées dans la formule $Ax+a$, où x est indéterminé, mais tel que $Ax+a \equiv b \pmod{B}$, desorte que si δ est le plus grand diviseur commun de A et de B, la résolution complète de cette congruence prendra cette forme $x \equiv v \left(\mathrm{mod.}\frac{B}{\delta}\right)$; ou ce qui revient au même, $x = v + \frac{KB}{\delta}$, K étant unnombre entier indéterminé; donc la formule $a+Av+\frac{KAB}{\delta}$ renferme toutes les valeurs de z, ce qui revient à $z \equiv a+Av \left(\mathrm{mod.}\frac{AB}{\delta}\right)$. S'il y avait un troisième module C, suivant lequel le nombre cherché dût être $\equiv c$, on suivrait la même marche, après avoir réuni les deux premières conditions en une seule. Ainsi soit ε le plus grand commun diviseur des nombres $\frac{AB}{\delta}$ et C, on obtiendra la congruence... $\frac{AB}{\delta}x+a+Av \equiv c \pmod{C}$, qui sera résolue par une congruence de la forme $x \equiv w \left(\mathrm{mod.}\frac{C}{\delta}\right)$, et le sera par la congruence $z \equiv \frac{AB}{\delta}w+a+Av \left(\mathrm{mod.}\frac{ABC}{\delta\varepsilon}\right)$; on procéderait de même, quel que fût le nombre des modules. Il convient d'observer que $\frac{AB}{\delta}$ et $\frac{ABC}{\delta\varepsilon}$, sont respectivement les plus petits nombres divisibles à-la-fois par A et B, ou par A, B et C, et l'on en conclut facilement, quel que soit le nombre des modules A, B, C, etc., que si l'on représente par M le plus petit nombre divisible par chacun d'eux, on aura la résolution complète, en prenant $z \equiv r \pmod{M}$. Au reste, si l'une des congruences n'est pas résoluble, il faut en conclure que le problême est impossible; mais il est évident que cela ne peut arriver si les nombres A, B, C, etc. sont premiers entr'eux.

Soient par exemple $A=504$, $B=35$, $C=16$, $a=17$, $b=-4$, $c=33$; ici les deux conditions que $z \equiv 17 \pmod{504}$, et $\equiv -4 \pmod{35}$, se réduisent à une seule $z \equiv 521 \pmod{2520}$, qui, jointe à la troisième $z \equiv 33 \pmod{16}$, donnera enfin $z \equiv 3041 \pmod{5040}$.

33. Quand tous les nombres A, B, C, etc. sont premiers entre eux, leur produit est le plus petit nombre divisible par chacun d'eux; et dans ce cas il est évident que toutes les congruences $z \equiv a \pmod{A}$, $z \equiv b \pmod{B}$, etc. se ramèneront à une seule $z \equiv r \pmod{R}$ qui leur équivaudra, R étant le produit des nombres A, B, C, etc.: il suit de là réciproquement qu'une seule condition $z \equiv r \pmod{R}$ peut être décomposée en plusieurs $z \equiv r \pmod{A}$, $z \equiv r \pmod{B}$; $z \equiv r \pmod{C}$, etc. si A, B, C, etc. sont les différens facteurs premiers entr'eux qui composent R. Cette observation nous donne non-seulement le moyen de découvrir l'impossibilité lorsqu'elle existe, mais encore une méthode plus commode et plus élégante pour déterminer les racines.

43. Soient comme ci-dessus les conditions $z \equiv a \pmod{A}$, $z \equiv b \pmod{B}$, $z \equiv c \pmod{C}$, etc. On résoudra tous les modules en facteurs premiers entr'eux; A en $A'A''A'''$ etc.; B en $B'B''B'''$ etc.; de manière que les nombres A', A'', etc., B', B'', etc. soient premiers ou puissances de nombres premiers; si l'un des nombres A, B, C, etc. était premier lui-même ou puissance d'un nombre premier, il n'y aurait, pour lui, aucune décomposition à faire. Alors ce qui précède fait voir que l'on peut, aux conditions données, substituer les suivantes $z \equiv a \pmod{A'}$, $z \equiv a \pmod{A''}$, $z \equiv a \pmod{A'''}$, etc.; $z \equiv b \pmod{B'}$, $z \equiv b \pmod{B''}$, etc., etc.; Or, à moins que tous les nombres A, B, C, etc. ne fussent premiers entr'eux; par exemple, si A n'est pas premier avec B, il est évident que tous les diviseurs premiers ne peuvent être différens dans A et dans B, mais qu'il doit y avoir quelqu'un des diviseurs A', A'', etc., qui trouve son égal, son multiple, ou son soumultiple parmi les diviseurs B', B'', etc. Soit d'abord $A' = B'$, les conditions $z \equiv a \pmod{A'}$, $z \equiv b \pmod{B'}$, doivent être identiques, et l'on doit avoir $a \equiv b \pmod{A' \text{ ou } B'}$; ainsi l'une ou l'autre de ces deux conditions peut être rejetée; mais si l'on n'a pas $a \equiv b \pmod{A'}$, le problême est impossible. Soit ensuite B' un multiple de A', la condition $z \equiv a \pmod{A'}$ doit être contenue dans celle-ci, $z \equiv b \pmod{B'}$, ou bien celle-ci, $z \equiv b \pmod{A'}$, qui se déduit de la dernière, doit être équivalente à la première; d'où il suit que la condition $z \equiv a \pmod{A'}$, peut être rejetée, si elle ne contrarie pas l'autre, auquel cas le problême serait im-

possible. Quand toutes les conditions superflues sont ainsi rejetées, il est évident que tous les modules qui restent sont premiers entr'eux ; on est sûr alors de la possibilité du problême, et on peut procéder d'après la manière enseignée plus haut.

35. Si nous supposons comme au n° 32 $z \equiv 17 \pmod{504}$, $\equiv -4 \pmod{35}$, $\equiv 33 \pmod{16}$; ces conditions peuvent se décomposer en celles qui suivent : $z \equiv 17 \pmod{8}$, $\equiv 17 \pmod{9}$, $\equiv 17 \pmod{7}$; $z \equiv -4 \pmod{5}$, $\equiv -4 \pmod{7}$; $z \equiv 33 \pmod{16}$. De ces conditions on peut rejeter $z \equiv 17 \pmod{8}$ et $z \equiv 17 \pmod{7}$, car la première est renfermée dans la condition $z \equiv 33 \pmod{16}$, et la seconde est équivalente à $z \equiv -4 \pmod{7}$: il reste ainsi

$$z \equiv \left\{ \begin{array}{r} 17 \pmod{9} \\ -4 \pmod{5} \\ -4 \pmod{7} \\ 33 \pmod{16} \end{array} \right\} \text{ d'où l'on tire } z \equiv 3041 \pmod{5040}.$$

Au reste il est clair qu'il sera souvent plus commode de ramener à une seule les conditions qui restent et qui proviennent de la même, ce qui se fera sans peine. Par exemple, quand on a rejeté quelques-unes des conditions $z \equiv a \pmod{A'}$, $z \equiv a \pmod{A''}$, etc. celle qui se composera des conditions restantes sera $z \equiv a$, suivant le module formé par le produit de tous les modules qui restent. Ainsi dans notre exemple des conditions $z \equiv -4 \pmod{5}$, $z \equiv -4 \pmod{7}$; on tire sur-le-champ la condition $z \equiv -4 \pmod{35}$, d'où elles dérivent ; il s'ensuit qu'il n'est pas indifférent, quant à la briéveté du calcul, de rejeter l'une ou l'autre des conditions équivalentes ; mais il n'entre pas dans notre plan de parler de ces détails ni d'autres artifices pratiques que l'usage apprend mieux que les préceptes.

36. Quand tous les modules A, B, C, etc. sont premiers entr'eux, il est préférable le plus souvent d'employer la méthode suivante. On déterminera un nombre α congru à l'unité suivant A, et à 0 suivant le produit des autres modules ; c'est-à-dire, que α sera une valeur quelconque de l'expression $\frac{1}{BCD \text{ etc.}} \pmod{A}$, multipliée par BCD etc. (n° 32) ; mais il vaut mieux prendre la plus petite de ces valeurs. Soit de même $\beta \equiv 1 \pmod{B}$, et $\equiv 0 \pmod{ACD \text{ etc.}}$;

$\gamma \equiv 1 \pmod{C}$, et $\equiv 0 \pmod{ABD \text{ etc.}}$. Alors si l'on cherche un nombre z qui soit congru aux nombres a, b, c, etc. suivant les modules A, B, C, etc. respectivement, on pourra poser..... $z \equiv \alpha a + \beta b + \gamma c + \text{etc.} \pmod{ABCD \text{ etc.}}$; en effet on a évidemment $\alpha a \equiv a \pmod{A}$, et les autres termes sont $\equiv 0 \pmod{A}$; donc $z \equiv a \pmod{A}$. La démonstration est la même pour les autres modules. Cette solution est préférable à la première; quand on a à résoudre plusieurs problèmes du même genre, pour lesquels les valeurs de A, B, C, etc. sont les mêmes; car alors on trouve pour α, β, etc. des valeurs constantes. Ceci s'applique au problème de chronologie dans lequel on cherche le quantième de l'année pour laquelle l'indiction, le nombre d'or et le cycle solaire sont donnés. Ici $A = 15$, $B = 19$, $C = 28$; ainsi comme la valeur de l'expression $\frac{1}{19.28} \pmod{15}$, ou $\frac{1}{532} \pmod{15}$ est 13, on aura $\alpha = 6916$; on trouvera de même $\beta = 4200$, $\gamma = 4845$. Donc le nombre cherché sera le résidu *minimum* du nombre $6916\,a + 4200\,b + 4845\,c$, a représentant l'indiction, b le nombre d'or, et c le cycle solaire.

37. Nous n'en dirons pas davantage sur les congruences du premier degré, qui ne renferment qu'une seule inconnue; il nous reste à parler des congruences qui renferment plusieurs inconnues; mais, comme il faudrait donner trop d'extension à ce chapitre, si nous voulions exposer chaque chose en toute rigueur, et notre projet n'étant pas d'épuiser ici la matière, mais seulement de présenter ce qui est le plus digne d'attention; nous bornerons notre recherche à un petit nombre d'observations, réservant l'exposition complète pour une autre occasion.

1°. De même que dans les équations, on voit qu'il faut avoir autant de congruences qu'il y a d'inconnues à déterminer.

2°. Soient donc proposées les congruences

$$a x + b y + c z \ldots \equiv f \pmod{m} \ldots (A)$$
$$a' x + b' y + c' z \ldots \equiv f' \ldots\ldots\ldots (A')$$
$$a'' x + b'' y + c'' z \ldots \equiv f'' \ldots\ldots\ldots (A'')$$
$$\text{etc.}$$

en même nombre que les inconnues x, y, z, etc.

On déterminera les nombres ξ, ξ', ξ'', etc. de manière qu'on ait:

$$b\xi + b'\xi' + b''\xi'' + \text{etc.} = 0,\ c\xi + c'\xi' + c''\xi'' + \text{etc.} = 0,\ \text{etc.}$$

et que ces nombres soient entiers et n'aient aucun diviseur commun à tous, ce qui est toujours possible par la théorie des équations linéaires.

On déterminera de même v, v', v'', etc., ζ, ζ', ζ'', etc., etc., de manière qu'on ait

$$av + a'v' + a''v'' + \text{etc.} = 0,\ cv + c'v' + c''v'' + \text{etc.} = 0,\ \text{etc.}$$
$$a\zeta + a'\zeta' + a''\zeta'' + \text{etc.} = 0,\ b\zeta + b'\zeta' + b''\zeta'' + \text{etc.} = 0,\ \text{etc.}$$
etc.

3°. Il est évident que si l'on multiplie les congruences A, A', A'', etc., d'abord par ξ, ξ', ξ'', etc., ensuite par v, v', v'', etc. etc., et qu'on les ajoute, on obtiendra les congruences suivantes :

$$(a\xi + a'\xi' + a''\xi'' + \text{etc.})\ x \equiv f\xi + f'\xi' + f''\xi'' + \text{etc.}$$
$$(bv + b'v' + b''v'' + \text{etc.})\ y \equiv fv + f'v' + f''v'' + \text{etc.}$$
$$(c\zeta + c'\zeta' + c''\zeta'' + \text{etc.})\ z \equiv f\zeta + f'\zeta' + f''\zeta'' + \text{etc.}$$
etc.

que, pour abréger, nous représenterons ainsi :

$$x.\Sigma(a\xi) \equiv \Sigma(f\xi),\ y.\Sigma(bv) \equiv \Sigma(fv),\ z.\Sigma(c\zeta) \equiv \Sigma(f\zeta),\ \text{etc.}$$

4°. Il y a plusieurs cas à distinguer en premier lieu quand les coefficiens des inconnues, c'est-à-dire quand $\Sigma(a\xi)$, $\Sigma(bv)$, etc. sont premiers avec le module des congruences, ces congruences peuvent être résolues par les méthodes déjà exposées, et la solution complète du problème s'obtient par des congruences de cette forme $x \equiv p \pmod{m}$, $y \equiv q \pmod{m}$, etc. (*). Si l'on propose, par

(*) Il faut observer que cette conclusion manque de démonstration que nous supprimons ici; car il ne suit rigoureusement rien autre chose de notre analyse, si ce n'est que les congruences proposées ne peuvent être résolues par d'autres valeurs de x, y, z etc. mais non pas que celles-ci satisfassent; il serait même possible qu'il n'y eût aucune solution. Le même paralogisme se présente dans la solution des équations linéaires.

exemple, les congruences $x+3y+z\equiv 1$, $4x+y+5z\equiv 7$, $2x+2y+z\equiv 3$ (mod. 8), on trouvera $\xi=9, \xi'=1, \xi''=-14$; donc $\Sigma(a\xi)=-15$, $\Sigma(f\xi)=-26$; donc $-15x\equiv 26$, et partant $x\equiv 2$ (mod. 8). De la même manière on trouvera $15y\equiv -4$, $15z\equiv 1$, et de là, $y\equiv 4$, $z\equiv 7$ (mod. 8).

5°. Si tous les coefficiens $\Sigma(a\xi)$, $\Sigma(bv)$, etc. ne sont pas premiers avec le module, soient α, β, γ, etc. les plus grands diviseurs communs de m et de $\Sigma(a\xi), \Sigma(bv), \Sigma(c\zeta)$, etc. respectivement; et il est évident que le problême est impossible, si α, β, γ, etc. ne divisent aussi $\Sigma(f\xi), \Sigma(fv), \Sigma(f\zeta)$, etc respectivement; mais quand ces conditions auront lieu, le problême sera résolu complètement par des congruences telles que $x\equiv p\left(\text{mod.}\frac{m}{\alpha}\right)$, $y\equiv q\left(\text{mod.}\frac{m}{\beta}\right)$; $z\equiv r\left(\text{mod.}\frac{m}{\gamma}\right)$, etc.; ou si l'on aime mieux, on aura α valeurs différentes pour x, savoir : $p, p+\frac{m}{\alpha}, \ldots\ldots$ $p+\frac{(\alpha-1)m}{\alpha}$, β valeurs pour y, γ valeurs pour z, etc. qui satisferont aux congruences. Toutes les solutions de la question, s'il y en a quelques-unes, devront se trouver parmi celles que nous venons d'indiquer; mais il n'est pas permis de renverser la conclusion; car souvent toutes les combinaisons des α valeurs de x, avec celles de y et celles de z, etc. ne satisfont pas au problême, mais seulement quelques-unes dont la liaison s'exprime au moyen d'une ou de plusieurs équations de condition. Au reste comme la solution complète de ce problême n'est pas nécessaire pour la suite, nous ne nous étendrons pas davantage ici sur ce sujet, et nous nous contenterons d'en donner une idée par un exemple.

Soient proposées les congruences $3x+5y+z\equiv 4$, $2x+3y+2z\equiv 7$, $5x+y+3z\equiv 6$ (mod. 12), on aura ici $\xi=1, \xi'=-2, \xi''=1$; $v=1, v'=1, v''=-1$; $\zeta=-13, \zeta'=22, \zeta''=-1$; d'où $4x\equiv -4$, $7y\equiv 5$, et $28z\equiv 96$; d'où l'on tire quatre valeurs de x, savoir, $x\equiv 2, 5, 8, 11$; une seule de y, $y\equiv 11$; quatre de z, savoir, $z\equiv 0, 3, 6, 9$ (mod. 12). Or pour découvrir quelles combinaisons des valeurs de x et de z on peut admettre, substituons à la place de x, y, z, $2+3t$, 11, $3u$, ce qui change les congruences proposées en $57+9t+3u\equiv 0$, $30+6t+6u\equiv 0$ et $15+15t+9u\equiv 0$ (mod. 12),

congruences qui reviennent à $19+3t+u\equiv 0$, $10+2t+2u\equiv 0$ $5+5t+3u\equiv 0$ (mod. 4). Chacune d'elles sera évidemment satisfaite, si $u\equiv t+1$ (mod. 4). Concluons de là que les valeurs de $x\equiv 2, 5, 8, 11$ que l'on obtient en faisant successivement $t=0, 1, 2, 3$, doivent être combinées respectivement avec les valeurs 3, 6, 9, 0 de z; desorte qu'il y a quatre solutions.

$$x\equiv 2,5,8,11\ldots, y\equiv 11,11,11,11,\ldots; z\equiv 3,6,9,0 \text{ (mod. 12)}.$$

A ces recherches qui remplissent la tâche que nous nous étions proposée dans ce chapitre, nous joindrons quelques propositions qui se rapportent aux mêmes principes, et qui seront d'un fréquent usage par la suite.

38. PROBLÈME. *Trouver combien il y a de nombres plus petits qu'un nombre donné* A, *et premiers avec lui?* Désignons, pour abréger, le nombre cherché par le caractère φ placé avant le nombre donné; le nombre cherché sera φA.

1°. Quand A est premier, il est évident que tous les nombres, depuis 1 jusqu'à $A-1$, sont premiers avec A, et partant, dans ce cas, on a $\varphi A=A-1$.

2°. Quand A est une puissance d'un nombre premier p, p^m par exemple; tous les nombres divisibles par p ne seront pas premiers avec A, les autres le seront; c'est pourquoi de p^m-1 nombres, il faut rejeter ceux-ci : p, $2p$, $3p\ldots(p^{m-1}-1)p$. Il en restera donc $p^m-1-(p^{m-1}-1)=p^m-p^{m-1}=p^{m-1}(p-1)$ donc..... $\varphi p^m=p^{m-1}.(p-1)$.

3°. Les autres cas se ramènent facilement à ceux-ci, au moyen de la proposition suivante : *Si on décompose* A *en facteurs*.... M, N, P, *etc. premiers entr'eux, on aura* $\varphi A=\varphi M.\varphi N.\varphi P.$, etc., qui se démontre ainsi qu'il suit. Soient m, m', m'', etc. les nombres premiers avec M et plus petits que lui. Soient de même n, n', n'', etc., p, p', p'', etc., etc. les nombres premiers avec N, P, etc. respectivement, et plus petits qu'eux; il est évident que tous les nombres premiers avec A le seront aussi avec les facteurs M, N, P, etc., et réciproquement (n° 19), et que tous les nombres qui seront congrus à l'un quelconque des nombres m, m', etc. suivant le module M, seront premiers avec M; de même pour N, P, etc. La

question est donc réduite à déterminer combien il y a de nombres au dessous de A, qui soient congrus à quelqu'un des nombres m, m', etc. suivant le module M, à quelqu'un des nombres n, n', etc. suivant le module N, etc.; mais (n° 32) tous les nombres qui ont des résidus donnés suivant chacun des modules M, N, P, etc. doivent être congrus suivant leur produit A, et parconséquent il ne peut y en avoir qu'un seul congru à des résidus donnés suivant les modules M, N, P, etc., et qui soit plus petit que A. Ainsi le nombre cherché sera égal au nombre des combinaisons des différens nombres m, m', m'', etc. avec les nombres n, n', n'', etc. et les nombres p, p', p'', etc., etc. Or par la théorie des combinaisons, ce nombre est $\varphi(M).\varphi(N).\varphi(P)$. etc.

4°. On voit facilement comment on peut appliquer cette proposition au cas dont il s'agit. On décomposera A en facteurs premiers; c'est-à-dire, qu'on le réduira à la forme $a^{\alpha}b^{\beta}c^{\gamma}$ etc., a, b, c, etc. étant des nombres premiers différens. Alors on aura

$$\varphi A = \varphi a^{\alpha}.\varphi b^{\beta}.\varphi c^{\gamma}.\text{ etc.} = a^{\alpha-1}(a-1).b^{\beta-1}(b-1).c^{\gamma-1}(c-1)\text{ etc.},$$

qui peut se mettre sous la forme plus élégante

$$\varphi A = A.\frac{a-1}{a}.\frac{b-1}{b}.\frac{c-1}{c}\text{ etc.}$$

Exemple : Soit $A = 60 = 2^2.3.5$, on aura $\varphi A = 60.\frac{1}{2}.\frac{2}{3}.\frac{3}{4}.\frac{4}{5} = 16$ Ces nombres premiers avec 60, sont : 1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59.

La première solution de ce problême se trouve dans le Mémoire d'Euler, intitulé : *Theoremata arithmetica novâ methodo demonstrata.* (Comment. nov. acc. Petrop. VIII, pag. 74). La démonstration en a été donnée encore dans une autre dissertation intitulée : *Speculationes circa quasdam insignes proprietates numerorum.* (Acta Petrop. VIII, p. 17).

39. Si la signification du caractère φ est déterminée de manière à ce que φA exprime combien il y a de nombres premiers avec A, et non plus grands que A; alors on n'aura plus $\varphi 1 = 0$, mais $= 1$; mais dans tous les autres cas il n'y aura rien de changé. En adoptant cette définition, nous aurons le théorême suivant :

Si a, a′, a″, *etc. sont tous les diviseurs de* A, *l'unité et* A *y compris, on aura* $\varphi a+\varphi a'+\varphi a''+$ *etc.* $=A$. Par exemple, si $A=30$, on aura

$$\varphi 1+\varphi 2+\varphi 3+\varphi 5+\varphi 6+\varphi 10+\varphi 15+\varphi 30=1+1+2+4+2+4+8+8=30.$$

Démonstration. Si l'on multiplie tous les nombres premiers avec a et non plus grands que lui par $\frac{A}{[a]}$, de même tous les nombres premiers avec a' par $\frac{A}{a'}$, etc.; on aura $\varphi a+\varphi a'+\varphi a''+$ etc., nombres tous non plus grands que A; mais

1°. Tous ces nombres seront inégaux; car il est évident que ceux qui proviennent du même diviseur de A sont tous inégaux. D'ailleurs s'il en résultait deux égaux provenant de diviseurs différens M et N, et de nombres μ et ν qui leur soient respectivement premiers; c'est-à-dire, si l'on avait $\frac{A}{M}\mu=\frac{A}{N}\nu$, ou bien $N\mu=M\nu$; en posant $M>N$, (ce qui est permis), il s'ensuivrait, puisque M est premier avec μ et qu'il divise $N\mu$, qu'il devrait aussi diviser N, ce qui est absurde.

2°. Entre ces nombres on trouvera tous ceux qui composent la suite 1, 2, 3.... A. En effet, soit t un nombre quelconque qui ne surpasse pas A, et δ le plus grand commun diviseur entre A et t, $\frac{A}{\delta}$ sera le diviseur de A avec lequel $\frac{t}{\delta}$ sera premier. Donc le nombre t se trouvera parmi ceux qui ont été produits par le diviseur $\frac{A}{\delta}$;

3°. Il suit de là que le nombre total en est A; donc..... $A=\varphi a+\varphi a'+\varphi a''+$ etc.

4o. *Si* μ *est le plus grand diviseur commun des nombres...* A, B, C, D, *etc. on peut toujours déterminer les nombres* a, b, c, d, *etc. de manière qu'on ait* $aA+bB+cC+$ *etc.* $=\mu$.

Considérons d'abord deux nombres A et B seulement, et soit λ leur plus grand diviseur commun. Alors la congruence $Ax\equiv\lambda$ (mod. B) sera résoluble (n° 30). Soit la racine $\equiv\alpha$, et que l'on fasse $\frac{\lambda-A\alpha}{B}=\beta$. on aura $\alpha A+\beta B=\lambda$.

S'il

S'il y a un troisième nombre C, soit λ' le plus grand diviseur commun de λ et de C, il sera en même temps celui des trois nombres A, B, C, (*). On déterminera les nombres k et γ de manière qu'on ait $k\lambda+\gamma C=\lambda'$, et l'on aura $k\alpha A+k\beta B+\gamma C=\lambda'$.

S'il y a un quatrième nombre D, soit λ'' le plus grand diviseur commun de λ' et de D, il sera en même temps celui des quatre nombres A, B, C, D. On fera $k'\lambda'+\delta D=\lambda''$, et partant on aura $k'k\alpha A+k'k\beta B+k''\gamma+\delta D=\lambda''$.

On procéderait de la même manière s'il y avait plus de nombres.

Si les nombres A, B, C, etc. n'avaient pas de diviseur commun, il est clair qu'on aurait $aA+bB+cC+$ etc. $=1$.

41. *Si* p *est un nombre premier, et qu'on ait* p *choses parmi lesquelles il peut s'en trouver un certain nombre d'égales entr'elles, pourvu que toutes ne le soient pas : le nombre des permutations de ces choses sera divisible par* p.

Par exemple, cinq choses A, A, A, B, B peuvent se disposer de dix manières différentes.

La démonstration de ce théorême se déduit facilement de la théorie connue des permutations. En effet, supposons que, parmi ces p choses, il y en ait a égales à A, b égales à B, c égales à C, etc., desorte qu'on ait $a+b+c+$ etc. $=p$, les nombres a, b, c, etc. pouvant aussi désigner l'unité. Le nombre des permutations sera $=\frac{1.2.3\ldots p}{1.2..a.1.2..b.1.2\ldots c.\text{ etc.}}$; or le numérateur est évidemment divisible par le dénominateur, puisque le nombre des permutations est entier; mais il est divisible par p, tandis que le dénominateur, qui est composé de facteurs plus petits que p, n'est pas divisible par p (n°. 15); donc le nombre des permutations sera divisible par p.

Nous espérons cependant que la démonstration suivante ne déplaîra pas à quelques lecteurs.

(*) En effet si λ' n'était pas le plus grand commun diviseur de A, B, C, il y en aurait un plus grand que λ'. Or celui-ci divisera A et B, partant il divisera $\alpha A+\beta B$ ou λ, ce qui est absurde.

Lorsque dans deux permutations l'ordre des choses ne différera qu'en ce que celle qui tient la première place dans l'une, en occupe une différente dans l'autre, mais que du reste toutes les autres choses, à partir de celle-là, suivent le même ordre dans chacune des permutations, de manière que la dernière de l'une se trouve placée immédiatement avant la première dans l'autre; nous les appellerons *permutations semblables* (*). Ainsi $ABCDE$ et $DEABC$, $ABAAB$ et $ABABA$ seront semblables.

Or comme chaque permutation est composée de p choses, il est clair qu'on pourra en trouver $p-1$, semblables à une quelconque d'entre elles, si l'on met successivement à la seconde, à la troisième place, etc., la chose qui occupait la première; donc si aucunes de ces permutations semblables ne sont identiques, il est évident que le nombre total des permutations sera égal à p fois le nombre des permutations dissemblables, et conséquemment sera divisible par p. Supposons que deux permutations semblables $PQ\ldots TV\ldots YZ$, $V\ldots YZPQ\ldots T$ puissent être identiques, et que P qui occupe la première place dans la première, occupe la $n+1^{\text{ième}}$ dans la seconde : on aura dans la dernière série le $n+1^{\text{ième}}$ terme égal au 1er, le $n+2^{\text{ième}}$ égal au $2^{\text{ième}}$, etc., d'où résulte que le $2n+1^{\text{ième}}$ est encore égal au premier, et par-conséquent le $3n+1^{\text{ième}}$, et généralement le $kn+m^{\text{ième}}$ égal au $m^{\text{ième}}$ (où quand $kn+m>p$, il faut imaginer qu'on reprenne toujours par le commencement, la série $V\ldots YZPQ\ldots T$, à moins qu'on ne retranche de $kn+m$, le multiple de p, qui en approche le plus en moins). Cela posé, si on détermine k de manière que $kn\equiv 1 \pmod{p}$, ce qui peut toujours se faire, puisque p est premier, il suivra de là que généralement le $m^{\text{ième}}$ terme serait égal au $m+1^{\text{ième}}$, c'est-à-dire qu'un terme quelconque serait égal au suivant, ou que tous les termes seraient égaux entre eux, ce qui est contre l'hypothèse.

42. *Si les coefficiens* a, b, c, *etc.*, n; a′, b′, c′, *etc.*, n′; *de deux fonctions de la forme*

(*) Si l'on écrivait en cercle les permutations semblables, de manière que la dernière chose touchât à la première, il n'y aurait aucune différence entre elles, parcequ'aucune place ne peut s'appeler la première ni la dernière.

$x^m+ax^{m-1}+bx^{m-2}+\ldots+n\ldots(P)$, $x^{m'}+a'x^{m'-1}+b'x^{m'-2}+\ldots+n'\ldots(Q)$

sont tous rationnels, mais non pas tous entiers, et que le produit soit $x^{m+m'}+Ax^{m+m'-1}+\ldots+N$, *les coefficiens* A, B, C, etc., N *ne peuvent être tous entiers.*

En effet, réduisons à leur plus simple expression toutes les fractions qui peuvent se trouver parmi les nombres a, b, c, etc.; a', b', c', etc.; et choisissons un nombre premier p qui divise un ou plusieurs des dénominateurs de ces fractions. Supposons que p divise le dénominateur d'un coefficient fractionnaire de (P), il est clair qu'en divisant (Q) par p, on aura aussi dans $\frac{(Q)}{p}$ au moins un coefficient fractionnaire dont le dénominateur sera divisible par p (le coefficient du premier terme $\frac{1}{p}$, par exemple). Or on voit facilement qu'on pourra toujours trouver un terme fractionnaire de (P) dont le dénominateur contienne p élevé à une puissance plus grande que dans tous les termes qui précèdent, et non moindre que dans tous ceux qui suivent. Soit ce terme Gx^g et t l'exposant de p dans le dénominateur. On trouvera un terme pareil dans $\frac{(Q)}{p}$, que nous supposerons être Γx^γ, l'exposant de p dans le dénominateur, étant τ; on aura au moins $t+\tau=2$. Cela posé, le terme $x^{g+\gamma}$ du produit de (P) par (Q) aura un coefficient fractionnaire dont le dénominateur renfermera p élevé à la puissance $t+\tau-1$.

En effet, soient $'Gx^{g+1}$, $''Gx^{g+2}$, etc., les termes qui précèdent Gx^g dans (P); $G'x^{g-1}$, $G''x^{g-2}$, etc. ceux qui le suivent. Soient de même dans $\frac{(Q)}{p}$, $'\Gamma x^{\gamma+1}$, $\Gamma''x^{\gamma+2}$, etc., les termes qui précèdent Γx^γ; et $\Gamma'x^{\gamma-1}$, $\Gamma''x^{\gamma-2}$, etc. ceux qui le suivent. Dans le produit de (P) par $\frac{(Q)}{p}$ le coefficient de $x^{g+\gamma}$ sera évidemment

$$G\Gamma+'G\Gamma'+''G\Gamma''+\text{etc.}$$
$$+'\Gamma G'+''\Gamma G''+\text{etc.}$$

Le premier terme $G\Gamma$ sera une fraction qui, réduite à sa plus

simple expression, aura son dénominateur divisible par $p^{t+\tau}$. Si les autres termes sont fractionnaires, leurs dénominateurs ne contiendront que des puissances de p moindres que $p^{t+\tau}$, puisque chacun d'eux est le produit de deux facteurs, dont l'un ne contient qu'une puissance de p plus petite que p^t ou p^τ, et l'autre une puissance non plus grande que p^τ ou p^t. Ainsi $G\Gamma$ sera de la forme.... $\frac{e}{fp^{t+\tau}}$, et le reste de la forme $\frac{e'}{f'p^{t+\tau-\delta}}$, e, f, et f' étant indépendans de p. Donc la somme sera $\frac{ef'+e'fp^\delta}{ff'p^{t+\tau}}$ dont le numérateur n'est pas divisible par p, et dont parconséquent le dénominateur ne peut être ramené à renfermer une puissance de p moindre que $p^{t+\tau}$. Donc le coefficient du terme $x^{\beta+\gamma}$ dans le produit de (P) par (Q) sera $\frac{ef'+e'fp^\delta}{ff'p^{t+\tau-1}}$, c'est-à-dire une fraction dont le dénominateur renferme la puissance $t+\tau-1$ de p.

43. *La congruence du degré* m

$$Ax^m+Bx^{m-1}+Cx^{m-2}+\text{etc.}+Mx+N\equiv 0,$$

dont le module est un nombre premier p *qui ne divise pas* A, *ne peut pas être résolue de plus de* m *manières, ou n'a pas plus de* m *racines incongrues suivant* p.

En effet, supposons, s'il est possible, qu'on donne des congruences de différens degrés m, n, etc., qui aient plus de m, n, etc. racines; soit m le plus petit des nombres m, n, etc.; desorte que toutes les congruences d'un degré inférieur à m s'accordent avec notre proposition. Comme elle est démontrée plus haut (n° 26) pour le premier degré, m sera $=2$ ou >2. Admettons donc que la congruence $Ax^m+Bx^{m-1}+\text{etc.}+Mx+N\equiv 0$, ait au moins $m+1$ racines $x\equiv\alpha$, $x\equiv\beta$, $x\equiv\gamma$, etc.; et supposons que tous les nombres α, β, γ, etc., sont positifs et plus petits que p, ce qui est permis, et en outre que α soit le plus petit. Faisons dans la congruence proposée $x\equiv y+\alpha$, elle deviendra

$$Ay^m+B'y^{m-1}+\text{etc.}+M'y+N'\equiv 0.$$

Or il est évident que cette congruence sera satisfaite si $y \equiv 0$ ou $\equiv \beta - \alpha$, ou $\equiv \gamma - \alpha$, etc., racines toutes différentes, et en nombre $m+1$; mais de ce que $y \equiv 0$ est une racine, il suit que N' est divisible par p, on aura donc

$$y\,(Ay^{m-1} + B'y^{m-2} + \text{etc.} + M') \equiv 0 \pmod{p},$$

congruence qui sera satisfaite, en y substituant à la place de y une quelconque des m valeurs : $\beta - \alpha$, $\gamma - \alpha$, etc., qui sont toutes > 0 et $< p$. Parconséquent, dans ces différens cas,..... $Ay^{m-1} + B'y^{m-2} + \text{etc.} + M'$ deviendra $\equiv 0$ (n° 22); c'est-à-dire que la congruence $Ay^{m-1} + B'y^{m-2} + \text{etc.} + M' \equiv 0$ qui est du degré $m-1$, aurait m racines; ce qui ne s'accorde pas avec notre théorême, quoique nous ayons supposé que toutes les congruences d'un degré inférieur à m, y satisfissent; ce qui est absurde.

44. Nous avons supposé ici que le module p ne divisait pas le coefficient du premier terme; mais le théorême n'est pas restreint à ce seul cas. En effet, si le premier coefficient, et même quelques-uns des suivans étaient divisibles par p, on pourrait les négliger sans erreur, la congruence serait réduite à un degré inférieur, et le coefficient du premier terme ne serait plus divisible par p, à moins que tous les coefficiens ne le fussent, auquel cas la congruence deviendrait identique, et l'inconnue serait absolument indéterminée.

Lagrange est le premier qui ait proposé et démontré ce théorême (Mémoires de l'Académie de Berlin, ann. 1768, p. 192). Il se trouve aussi dans la Dissertation de Legendre, intitulée *Recherches d'Analyse indéterminée* (Histoire de l'Académie de Paris, 1785, p. 466). Euler dans les *Nouveaux Commentaires Académiques. Pétersb. XVIII, p.* 93, a démontré que la congruence $x^n - 1 \equiv 0$ ne pouvait pas avoir plus de n racines. Quoique ce ne soit qu'un cas particulier, la méthode dont ce célèbre Géomètre s'est servi, peut s'appliquer facilement à toutes les congruences. Il s'était déjà occupé d'un cas plus particulier (Comment. Ac. Pétersb. V. p. 6); mais cette méthode ne peut s'employer géné-

ralement. Dans la section VIII, nous démontrerons ce théorême d'une autre manière; mais quoique toutes ces méthodes puissent paraître différentes au premier aspect, les gens instruits qui voudront les comparer, s'assureront aisément qu'elles partent toutes du même principe. Au reste ce théorême ne devant être considéré ici que comme un lemme, et l'exposition complète n'appartenant pas à cette section, nous ne nous arrêterons pas à parler des modules composés.

SECTION TROISIÈME.

Des Résidus des Puissances.

45. THÉORÈME. *Dans toute progression géométrique....* $1, a^2, a^3$ *etc., outre le premier terme* 1, *il y en a encore un autre* a^t *congru à l'unité suivant le module* p *premier avec* a, *l'exposant* t *étant* $<$ p.

Puisque le module p est premier avec a, et parconséquent avec une puissance quelconque de a, aucun terme de la progression ne sera $\equiv 0 \pmod{p}$, mais chacun d'eux sera congru à quelqu'un des nombres $1, 2, 3, 4 \ldots p-1$. Comme le nombre de ces derniers est $p-1$, il est évident que si l'on considère plus de $p-1$, termes de la progression, ils ne pourront pas avoir tous des résidus *minima* différens. Ainsi parmi les nombres $1, a^2, a^3 \ldots a^{p-1}$, on en trouvera au moins deux congrus. Soit donc $a^m \equiv a^n$ et $m > n$, on aura, en divisant par a^n (n° 22), $a^{m-n} \equiv 1$, où $m-n < p$ et > 0.

Exemple. Dans la progression 1, 2, 4, 8, etc. le premier terme qui est congru avec l'unité suivant le module 13, se trouve être $2^{12} = 4096$, mais suivant le module 23, on a dans la même progression, $2^{11} = 2048 \equiv 1$; de même $5^6 = 15625 \equiv 1 \pmod{7}$; et $5^5 \equiv 3125 \equiv 1 \pmod{11}$. Ainsi dans quelques cas la puissance de a congrue avec l'unité, est plus petite que a^{p-1}, et dans d'autres, il faut remonter jusqu'à la puissance $p-1$ elle-même.

46. Quand la progression est continuée au delà du terme qui est congru à l'unité, on retrouvera les mêmes résidus qu'on avait à partir du commencement. Ainsi, soit $a^t \equiv 1$, on aura $a^{t+1} \equiv a$, $a^{t+2} \equiv a^2$, etc., jusqu'à ce qu'on parvienne au terme a^{2t}, dont le résidu *minimum* sera de nouveau $\equiv 1$, et la *période* des résidus

recommencera. On aura ainsi une période de t résidus qui se répétera continuellement, et l'on ne pourra trouver un seul résidu qui ne fasse partie de cette période. On aura en général $a^{mt} \equiv 1$ et $a^{mt+n} \equiv a^n$; ce qui peut se présenter ainsi suivant notre notation : si $r \equiv \rho \pmod{t}$, on aura $a^r \equiv a^\rho \pmod{p}$.

47. Ce théorème fournit le moyen de trouver facilement les résidus des puissances, quelle que soit la grandeur de l'exposant dont elles sont affectées, en même temps qu'on découvrira la puissance congrue à l'unité. Si, par exemple, on demande le reste de la division de 3^{1000} par 13, comme $3^3 \equiv 1 \pmod{13}$, on a $t = 3$, et comme d'ailleurs $1000 \equiv 1 \pmod{3}$, on trouvera $3^{1000} \equiv 3 \pmod{13}$.

48. Si a^t est la plus petite puissance congrue à l'unité, (en exceptant $a^0 = 1$, cas que nous ne considérons pas), les t restes qui composent la période seront tous différens, comme on le voit sans difficulté par la démonstration du n° 45. Alors la proposition du n° 46 peut être renversée. Savoir, si $a^m \equiv a^n \pmod{p}$, on aura $m \equiv n \pmod{t}$: car si m et n étaient incongrus suivant t, leurs résidus *minima* μ et ν seraient différens. Mais $a^\mu \equiv a^m$, $a^\nu \equiv a^n$; donc $a^\mu \equiv a^\nu$, c'est-à-dire, que toutes les puissances au dessous de a^t ne seraient pas incongrues, ce qui est contre l'hypothèse.

Si donc $a^k \equiv 1 \pmod{p}$, on aura $k \equiv 0 \pmod{t}$, c'est-à-dire que k sera divisible par t.

Nous avons parlé jusqu'ici de modules quelconques, pourvu qu'ils fussent premiers avec a. A présent examinons à part les modules qui sont des nombres premiers absolus, et établissons sur ce fondement des recherches plus générales.

49. THÉORÈME. *Si* p *est un nombre premier qui ne divise pas* a, *et que* a^t *soit la plus petite puissance de* a *congrue à l'unité, l'exposant* t *sera* $= p - 1$, *ou une partie aliquote de* $p - 1$.

Voyez pour des exemples le n° 45.

Comme nous avons déjà prouvé que t est $= p - 1$ ou $< p - 1$, il reste à faire voir que dans le dernier cas il est toujours une partie aliquote de $p - 1$.

1°. Rassemblons les résidus *minima* positifs de tous les termes, $1, a, a^2, a^3 \ldots a^{t-1}$, et désignons-les par $\alpha, \alpha', \alpha''$, etc. desorte qu'on ait $\alpha \equiv 1$, $\alpha' \equiv a$, $\alpha'' \equiv a^2$, etc. il est visible qu'ils seront tous différens; car si deux termes a^m, a^n donnaient les mêmes résidus, on aurait $a^{m-n} \equiv 1$ (en supposant $m > n$ et $m - n < t$); ce qui est absurde, puisque a^t est la plus petite puissance de a congrue à l'unité. Au reste tous les nombres α, α', α'', etc. sont compris dans la série $1, 2, 3, 4 \ldots\ldots p-1$, série qu'ils n'épuisent pas lorsque $t < p-1$. Nous désignerons par (A) la somme de tous ces résidus, et (A) comprendra un nombre t de termes.

2°. Prenons un nombre quelconque β, parmi ceux de la série $1, 2, 3 \ldots p-1$ qui manquent dans (A). Multiplions β par α, α', α'', etc. et nommons β, β', β'', etc. les résidus *minima* qui en proviendront, et qui seront aussi en nombre t. Ces résidus seront différens entr'eux, et différeront des nombres α, α', α'', etc. En effet, si la première assertion était fausse, on aurait $\beta a^m \equiv \beta a^n$; d'où l'on tire, en divisant par β, $a^m \equiv a^n$: ce qui est contre ce que nous venons de démontrer : si la dernière l'était, on aurait $\beta a^m \equiv a^n$; d'où, quand $n > m$, $\beta \equiv a^{n-m}$, c'est-à-dire que β serait congru à quelqu'un des nombres α, α', α'', etc. : ce qui est contre l'hypothèse; mais si $n < m$, on aura, en multipliant par a^{t-m}, $\beta a^{t} \equiv a^{t+n-m}$, ou, comme $a^t \equiv 1$, $\beta \equiv a^{t-(m-n)}$, d'où résulte la même absurdité. Désignons par (B) la somme des nombres β, β', β'', etc. qui sont en nombre t; on aura déjà $2t$ nombres parmi ceux-ci $1, 2, 3 \ldots p-1$. Donc si (A) et (B) épuisent cette série, on aura $t = \frac{p-1}{2}$.

3°. Mais s'il en manque quelques-uns, soit γ un de ceux-là. Multiplions α, α', α'', etc. par γ, et soient γ, γ', γ'', etc. les résidus *minima* de ces produits, dont nous désignerons l'ensemble par (C); (C) comprendra t nombre pris dans la série $1, 2, 3 \ldots p-1$ qui seront tous différens entr'eux et non-compris dans (A) et (B). Les deux premières assertions se démontrent comme ci-dessus (2°); quant à la troisième, si l'on avait $\gamma a^m \equiv \beta a^n$, on en tirerait $\gamma \equiv \beta a^{n-m}$, ou $\gamma \equiv \beta a^{t-(m-n)}$, suivant que $m < n$ ou $> n$. Dans l'un ou l'autre cas γ serait congru à quelqu'un des nombres qui composent (B); ce qui serait contre l'hypothèse. On aura ainsi $3t$

nombres pris dans la série 1, 2, 3... $p-1$, et s'il n'en reste plus, $t=\frac{p-1}{3}$, conformément au théorême.

4°. Mais s'il en reste encore quelques-uns, on arrivera de même à une quatrième somme de nombres (D), etc.; et comme la série 1, 2, 3, etc. $p-1$ est finie, on voit que l'on parviendra nécessairement à l'épuiser, et $p-1$ sera un multiple de t; donc t sera une partie aliquote de $p-1$.

5o. Puisque $\frac{p-1}{t}$ est un nombre entier, il suit qu'en élevant chaque membre de la congruence $a^t \equiv 1 \pmod{p}$ à la puissance $\frac{p-1}{t}$, on aura $a^{p-1} \equiv 1 \pmod{p}$; c'est-à-dire, que $a^{p-1}-1$ *sera toujours divisible par* p *quand* p *est premier et qu'il ne divise pas* a.

Ce théorême remarquable, tant par son élégance que par sa grande utilité, s'appelle ordinairement *théorême de Fermat*, du nom de l'inventeur. (*Fermatii opera Math. Tolosæ* 1679. *Fol. p.* 163.) Fermat n'en a pas donné la démonstration, bien qu'il ait assuré qu'il l'avait trouvée. Euler en a le premier publié une dans la Dissertation intitulée : *Démonstration de quelques théorêmes relatifs aux nombres premiers.* (Comm. Ac. Pétrop. T. VIII) (*); elle est tirée du développement de $(a+1)^p$, qui fait voir par la forme des coefficiens, que $(a+1)^p - a^p - 1$ est toujours divisible par p, et que parconséquent $(a+1)^p-(a+1)$ le sera si a^p-a l'est. Or comme 1^p-1 est divisible par p, 2^p-2 le sera donc; et partant 3^p-3, et généralement a^p-a. Donc si p ne divise pas a, on aura aussi $a^{p-1}-1$ divisible par p. Ce que nous venons de dire suffit pour faire connaître l'esprit de la démonstration.

(*) Antérieurement (Comm. Petr. T. VI. p. 106) ce grand homme n'était pas parvenu encore au but. Dans la fameuse discussion entre Maupertuis et Konig, sur le principe de la moindre action, discussion qui les jeta dans des digressions étrangères, Konig assura qu'il avait entre les mains un manuscrit autographe de Leibnitz, qui contenait une démonstration de ce théorême conforme à celle d'Euler (*Appel au Public.* p. 106). Quoique nous ne voulions pas refuser de croire à ce témoignage, il est sûr cependant que Leibnitz n'a jamais publié sa démonstration. (*Voyez* Hist. de l'Acad. de Berlin. 1750. p. 530).

Lambert en a donné une semblable, (*Acta eruditorum.* 1769, p. 109.). Mais comme le développement de la puissance d'un binome semble étranger à la théorie des nombres, Euler (Comm. nov. Petrop. T. VIII, p. 70.) donna une autre démonstration qui est conforme à celle que nous venons d'exposer. Dans la suite il s'en présentera encore d'autres : ici nous nous contenterons d'en donner encore une déduite du même principe que celle d'Euler. La proposition suivante, dont le théorême en question n'est qu'un cas particulier, nous sera utile pour d'autres recherches.

51. *Si* p *est un nombre premier, la puissance* p *du polynome* $a+b+c+$ *etc. est* $\equiv a^p+b^p+c^p+$ *etc. suivant le module* p.

On sait que $(a+b+c+\text{etc.})^p$ est composé de termes de la forme $Pa^\alpha b^\beta c^\gamma$ etc. où l'on a $\alpha+\beta+\gamma+\text{etc.}=p$, P étant le nombre de permutations de p choses, dont α, β, γ, etc. sont respectivement égales à a, b, c, etc. Mais nous avons fait voir (n° 41) que ce nombre était toujours divisible par p, à moins que toutes les lettres ne fussent égales entr'elles ; c'est-à-dire, à moins que l'un des nombres α, β, γ, etc. ne fût égal à p, et les autres égaux à zéro ; d'où il suit que tous les termes du développement, excepté a^p, b^p, etc. sont divisibles par p, et que parconséquent $(a+b+c+\text{etc.})^p \equiv a^p+b^p+c^p+\text{etc.}\ (\text{mod.}\ p)$.

Si toutes les quantités a, b, c, etc. sont supposées $=1$, et que leur nombre soit k, on aura $k^p \equiv k$, comme dans le n° précédent.

52. Comme les nombres qui sont diviseurs de $p-1$ sont les seuls qui puissent servir d'exposans aux plus petites puissances congrues avec l'unité, on est porté à chercher si tous les diviseurs de $p-1$ jouissent de cette propriété ; et, quand on classe tous les nombres non divisibles par p suivant l'exposant de leur plus petite puissance congrue à l'unité, combien il y en a pour chaque exposant. Nous observerons d'abord qu'il suffit de considérer les nombres positifs depuis 1 jusqu'à $p-1$: il est évident en effet que les nombres congrus doivent être élevés à la même puissance pour devenir congrus à l'unité, et que parconséquent un nombre quelconque doit être rapporté au même exposant que son résidu *minimum*

positif; ainsi nous avons à rechercher comment les nombres $1, 2, 3 \ldots p-1$, doivent être distribués sous ce point de vue, relativement aux facteurs de $p-1$. Pour abréger, si d est un des facteurs de $p-1$, entre lesquels on doit compter 1 et $p-1$, nous représenterons par $\downarrow d$ la multitude des nombres positifs plus petits que p, dont la puissance d est la plus petite qui soit congrue à l'unité.

53. Pour nous faire entendre plus facilement, nous présenterons d'abord un exemple. Soit $p=19$, les nombres $1, 2, 3 \ldots 18$ peuvent se distribuer de la manière suivante relativement aux diviseurs de 18 :

$$1\{1,\quad 2\{18,\quad 3\begin{cases}7\\11\end{cases},\quad 6\begin{cases}8\\12\end{cases},\quad 9\begin{cases}4,\ 5,\ 6\\9,\ 16,\ 17\end{cases},\quad 18\begin{cases}2,\ 3,\ 10\\13,\ 14,\ 15\end{cases}$$

Ainsi dans cas $\downarrow 1=1$, $\downarrow 2=1$, $\downarrow 3=2$, $\downarrow 6=2$, $\downarrow 9=6$, $\downarrow 18=6$. Avec une légère attention on voit qu'il y en a, relativement à chaque exposant, autant qu'il y a de nombres premiers avec cet exposant et non plus grands que lui, ou bien, en reprenant le signe du n° 40, que $\downarrow d=\varphi d$. Mais on peut démontrer généralement cette observation de la manière suivante :

1°. S'il y a un nombre a appartenant à l'exposant d, c'est-à-dire dont la puissance d soit congrue à l'unité, et les puissances inférieures incongrues, toutes les puissances de ce nombre, savoir $a, a^2, a^3, a^4 \ldots\ldots a^d$, ou leurs résidus *minima*, auront leur puissance d congrue avec l'unité; et comme cela peut s'exprimer en disant que les résidus *minima* des nombres $a, a^2, a^3, \ldots a^d$ qui sont tous différens sont les racines de la congruence $x^d \equiv 1$, qui ne peut avoir plus de d racines différentes, il est évident qu'il n'y a pas de nombres autres que les résidus *minima* de $a, a^2\ a^3, \ldots a^d$, dont les puissances d soient congrues à l'unité; d'où il suit que les nombres appartenans à l'exposant d se trouvent tous entre les résidus *minima* des nombres $a, a^2, a^3, \ldots a^d$. On déterminera comme il suit quels ils sont et quel est leur nombre. Si k est un nombre premier avec d, toutes les puissances de a^k, dont les exposans sont $<d$, ne seront pas congrues à l'unité. Soit en effet $\frac{1}{k}(\text{mod. } d)=m$ (voyez n° 31), on aura $a^{km} \equiv a$; donc si la

puissance e de a^k était congrue à l'unité, et que l'on eût $e < d$, on aurait aussi $a^{kme} \equiv 1$, et parconséquent $a^e \equiv 1$; ce qui est contre l'hypothèse. Il est évident, d'après cela, que le résidu *minimum* de a^k appartiendra à d; mais si k a un commun diviseur δ avec d, le résidu *minimum* de a^k n'appartiendra pas à l'exposant d. Car $\frac{kd}{\delta}$ est divisible par d, ou bien $\frac{kd}{\delta} \equiv 0 \pmod{d}$; parconséquent $a^{\frac{kd}{\delta}} \equiv 1$; c'est-à-dire $(a^k)^{\frac{d}{\delta}} \equiv 1$. Nous conclurons de là qu'il y a autant de nombres appartenans à l'exposant d, qu'il y a de nombres premiers avec d dans la série $1, 2, 3 \ldots d$. Mais il faut se souvenir que cette conclusion suppose qu'il existe déjà un nombre a appartenant à l'exposant d; parconséquent il reste douteux s'il ne pourrait pas se faire qu'aucun nombre n'appartînt à un exposant donné, et la conclusion se réduit à $\psi d = 0$, ou $= \varphi d$.

54. 2°. Soient d, d', d'', etc. les diviseurs de $p-1$; comme tous les nombres $1, 2, 3 \ldots p-1$ doivent être distribués entre ces diviseurs, on aura $\psi d + \psi d' + \psi d'' + \text{etc.} = p-1$. Mais (n° 40) nous avons démontré que $\varphi d + \varphi d' + \varphi d'' + \text{etc.} = p-1$, et du n° précédent il suit que $\psi d = 0$ ou $= \varphi d$; et parconséquent que ψd ne peut pas être $> \varphi d$; ce qui s'étend à $\psi d'$ et $\varphi d'$, etc. Si donc un ou plusieurs des nombres ψd, $\psi d'$, etc. étaient plus petits que son correspondant parmi les nombres φd, $\varphi d'$, etc., la somme des premiers ne pourrait être égale à la somme des derniers. D'où nous concluons enfin que dans tous les cas, $\psi d = \varphi d$, et que parconséquent ψd ne dépend point de la grandeur de $p-1$.

55. Il y a un cas particulier de la proposition précédente qui mérite de fixer notre attention; le voici : *il existe toujours des nombres dont aucune puissance plus petite que* p — 1 *n'est congrue à l'unité*; il y en a même autant entre 1 et $p-1$, qu'il y a au-dessous de $p-1$ de nombres qui lui soient premiers. Comme il s'en faut bien que la démonstration de ce théorème soit aussi évidente qu'elle le paraît d'abord, nous en donnerons une un peu différente de celle qui précède, d'autant plus que la diversité des méthodes aide beaucoup à jeter du jour sur les points les plus obscurs.

On décomposera $p-1$ en facteurs premiers, de manière qu'on ait $p-1=a^\alpha b^\beta c^\gamma$ etc. a, b, c, etc. étant des nombres premiers inégaux. Alors nous composerons la démonstration des deux propositions suivantes :

1°. On peut toujours trouver un nombre A, ou plusieurs appartenans à l'exposant a^α, et de même des nombres B, C, etc. appartenans aux exposans b^β, c^γ, etc.

2°. Le produit des nombres A, B, C, etc. ou le résidu *minimum* de ce produit appartiendra à l'exposant $p-1$; ce qui se démontre ainsi qu'il suit.

1°. Soit g un des nombres $1, 2, 3 \ldots p-1$ qui ne satisfasse pas à la congruence $x^{\frac{p-1}{a}} \equiv 1 \pmod{p}$; car tous les nombres ne peuvent pas satisfaire à cette congruence, dont le degré est $< p-1$. Alors je dis que si l'on fait $g^{\frac{p-1}{a^\alpha}} \equiv h$, h ou son résidu *minimum* appartiendra à l'exposant a^α.

En effet il est évident que $h^{a^\alpha} \equiv g^{p-1} \equiv 1$; mais $h^{a^{\alpha-1}} \equiv g^{\frac{p-1}{a}}$, et parconséquent sera incongru à l'unité, et à plus forte raison les puissances $h^{a^{\alpha-2}}$, $h^{a^{\alpha-3}}$ le seront aussi. Or l'exposant de la plus petite puissance de h congrue à l'unité, c'est-à-dire l'exposant auquel h appartient, doit être un diviseur de a^α (n° 48) ; et comme a^α n'est divisible que par lui-même, ou par les puissances inférieures de a, il s'ensuit nécessairement que a^α sera l'exposant auquel b appartient. On démontrera de la même manière, qu'on peut trouver des nombres appartenans aux exposans b^β, c^γ, etc.

2°. Si nous supposons que le produit de tous les nombres A, B, C, etc. n'appartienne pas à l'exposant $p-1$, etc., mais à un exposant t plus petit, t devra être un des diviseurs de $p-1$ (n° 48), ou $\frac{p-1}{t}$ sera un entier > 1. Il suit de là que ce quotient sera un

des nombres premiers a, b, c, etc., ou du moins qu'il sera divisible par quelqu'un d'eux (n° 17), par a, par exemple, car le raisonnement est le même pour les autres. t divisera ainsi $\frac{p-1}{a}$; donc le produit ABC etc. serait encore congru à l'unité, en l'élevant à la puissance $\frac{p-1}{a}$ (n° 46). Mais il est évident que tous les nombres, B, C, D, etc. (excepté A) deviennent congrus à l'unité, si on les élève à la puissance $\frac{p-1}{a}$, puisque les exposans auxquels ils appartiennent b^β, c^γ, etc. divisent $\frac{p-1}{a}$. Donc $A^{\frac{p-1}{a}}$. $B^{\frac{p-1}{a}}$. $C^{\frac{p-1}{a}}$. etc. $\equiv A^{\frac{p-1}{a}} \equiv 1$; donc a^α doit diviser $\frac{p-1}{a}$ (n° 48), c'est-à-dire que $\frac{p-1}{a^{\alpha+1}}$ doit être entier, ce qui est absurde (n° 15). Donc enfin notre supposition ne peut subsister, c'est-à-dire que le produit ABC etc. appartient réellement à l'exposant $p-1$.

La dernière démonstration semble un peu plus longue que la première, mais elle est plus directe.

56. Ce théorème nous fournit un exemple remarquable de la circonspection dont on a besoin dans la théorie des nombres, pour ne pas regarder comme démontrées des choses qui ne le sont pas. Lambert, dans la Dissertation que nous avons citée plus haut, fait mention de cette proposition, mais ne dit pas un mot de la nécessité de la démontrer. Personne même n'a tenté de le faire, excepté Euler (*Comm. nov. Ac. Pétrop. T. XVIII, p.* 85), dans son Mémoire intitulé : *Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia.* On peut voir surtout l'art. 37, dans lequel il a parlé avec étendue de la nécessité de démontrer cette proposition. Cependant la démonstration de cet homme pénétrant présente deux défauts ; l'un tient à ce qu'il suppose tacitement, art. 31 et suivans, que la congruence $x^n \equiv 1$, (en ramenant ses raisonnemens à notre notation) a réellement n racines différentes, tandis qu'il était seulement démontré que cette congruence ne peut en avoir davantage ; l'autre, à ce qu'il ne déduit que par induction la formule du n° 34.

57. Nous nommerons avec Euler, *racines primitives* les nombres qui appartiennent à l'exposant $p-1$. Si donc a est une racine primitive, tous les résidus *minima* des puissances $a, a^2, a^3, \ldots a^{p-1}$ seront différens; d'où l'on déduit facilement qu'ils se trouvent tous parmi les nombres $1, 2, 3, \ldots p-1$ qui sont en même nombre qu'eux, c'est-à-dire que tout nombre non divisible par p est congru à quelque puissance de a. Cette propriété remarquable est d'une bien grande utilité, et peut considérablement abréger les opérations arithmétiques relatives aux congruences, à peu près de la même manière que l'introduction des logarithmes dans l'arithmétique ordinaire en abrège les opérations. Nous prendrons arbitrairement pour *base* une racine primitive a, à laquelle nous rapporterons tous les nombres non divisibles par p; et si on a $a^e \equiv b \pmod{p}$, nous appellerons e l'*indice* de b. Par exemple, 2 est une racine primitive suivant le module 19; si on la prend pour base,

aux nombres	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18
répondront les indices	0, 1, 13, 2, 16, 14, 6, 3, 8, 17, 12, 15, 5, 7, 11, 4, 10, 9.

Au reste il est évident que pour la même base chaque nombre a plusieurs indices, mais qui seront tous congrus suivant le module $p-1$; aussi quand il sera question d'indices, ceux qui seront congrus suivant le module $p-1$, seront regardés comme équivalens, de même que les nombres sont regardés comme équivalens lorsqu'ils sont congrus suivant le module p.

58. Les théorèmes qui regardent les indices sont absolument analogues à ceux qui regardent les logarithmes.

L'indice d'un produit de tant de facteurs qu'on voudra, est congru à la somme des indices des différens facteurs, suivant le module $p-1$.

L'indice de la puissance d'un nombre est congru, suivant le module $p-1$, *au produit de l'exposant par l'indice du nombre donné.*

Nous omettons les démonstrations à cause de leur simplicité.

On voit par là que si nous voulions construire une table qui donnât

donnât les indices de tous les nombres pour différens modules, nous pourrions nous dispenser de tenir compte de tous les nombres plus grands que le module et de tous les nombres composés. On trouvera à la fin de cet ouvrage un essai de cette table (Tab. I). Dans la première colonne sont rangés les nombres premiers et les puissances de nombres premiers depuis 3 jusqu'à 97, qui doivent être regardés comme des modules : à côté de chacun d'eux, dans la colonne suivante, les nombres pris pour bases ; suivent alors les indices des nombres premiers successifs, qui sont écrits par tranches composées de cinq chacune ; en tête se trouvent les nombres premiers disposés dans le même ordre. Desorte qu'on peut trouver facilement l'indice qui répond à un nombre premier donné, suivant un module donné.

Soit par exemple $p=67$; l'indice de 60, en prenant 12 pour base, sera

$$\equiv 2\,\text{Ind.}\,2+\text{Ind.}\,3+\text{Ind.}\,5\,(\text{mod.}\,66)\equiv 58+9+39\equiv 40.$$

59. L'indice de la valeur d'une expression quelconque $\frac{a}{b}(\text{mod.}\,p)$, (n° 31) est congru suivant le module $p-1$, à la différence des indices du numérateur a et du dénominateur b, pourvu que les nombres a et b ne soient pas divisibles par p.

Soit en effet c une valeur quelconque de cette expression ; on aura $bc\equiv a\,(\text{mod.}\,p)$; donc $\text{Ind.}\,b+\text{Ind.}\,c\equiv\text{Ind.}\,a\,(\text{mod.}\,p-1)$, et

$$\text{Ind.}\,c\equiv\text{Ind.}\,a-\text{Ind.}\,b.$$

Si donc on a deux tables, dont l'une donne les indices qui répondent à chaque nombre pour un module quelconque, et dont l'autre donne les nombres qui répondent à des indices donnés, on pourra résoudre facilement toutes les congruences du premier degré, puisqu'on peut toujours les ramener à d'autres dont les modules soient premiers (n° 30).

Soit par exemple la congruence $29x+7\equiv 0\,(\text{mod.}\,47)$, on aura $x\equiv\frac{-7}{29}\,(\text{mod.}\,47)$.

De là

$$\text{Ind.}\,x\equiv\text{Ind.}\,-7-\text{Ind.}\,29\equiv\text{Ind.}\,40-\text{Ind.}\,29\equiv 15-43\equiv 18\,(\text{mod.}\,46);$$

or 3 est le nombre qui a pour indice 18; donc $x \equiv 3 \pmod{47}$. Nous n'avons point ajouté la seconde table, mais on verra dans la section VI comment on peut la remplacer par une autre.

60. De même que dans le n° 31 nous avons désigné par un signe particulier, les racines des congruences du premier degré, dans ce qui va suivre, nous représenterons par un autre signe les racines des congruences à deux termes des degrés supérieurs; et comme $\sqrt[n]{A}$ ne signifie autre chose que la racine de l'équation $x^n = A$; en ajoutant le module, $\sqrt[n]{A} \pmod{p}$ représentera une racine quelconque de la congruence $x^n \equiv A \pmod{p}$. Ainsi nous dirons que l'expression $\sqrt[n]{A} \pmod{p}$ a autant de valeurs qu'elle en a d'incongrues suivant p; car toutes celles qui sont congrues suivant p doivent être regardées comme équivalentes (n° 26). Au reste il est clair que si A et B sont congrus suivant p, les expressions $\sqrt[n]{A} \pmod{p}$, $\sqrt[n]{B} \pmod{p}$ seront équivalentes.

Maintenant si l'on fait $\sqrt[n]{A} \equiv x \pmod{p}$, on aura..... $n \operatorname{Ind}. x \equiv \operatorname{Ind}. A \pmod{p-1}$. On déduit de cette congruence, d'après les règles de la section II, les valeurs de Ind. x, et de là les valeurs correspondantes de x; mais on voit facilement que x a autant de valeurs qu'il y a de racines dans la congruence..... $n \operatorname{Ind}. x \equiv \operatorname{Ind}. A \pmod{p-1}$; donc $\sqrt[n]{A}$ n'aura qu'une valeur, quand n sera premier avec $p-1$; mais lorsque n et $p-1$, auront un commun diviseur, et que δ sera le plus grand, Ind. x aura δ valeurs incongrues suivant $p-1$, et parconséquent $\sqrt[n]{A}$ aura autant de valeurs incongrues suivant p, pourvu que Ind. A soit divisible par δ. Sans cette condition, $\sqrt[n]{A}$ n'aurait aucune valeur réelle.

Si l'on cherche par exemple les valeurs de l'expression $\sqrt[15]{11} \pmod{19}$, il faut résoudre la congruence $15 \operatorname{Ind}. x \equiv \operatorname{Ind}. 11 \equiv 6 \pmod{18}$, on trouvera trois valeurs de Ind. $x \equiv 4, 10, 16 \pmod{18}$, d'où il résulte $x \equiv 6, 9, 4$.

61. Quoique cette méthode soit très-expéditive, quand on a les tables nécessaires, nous ne devons cependant pas oublier qu'elle est indirecte; il sera donc utile de chercher ce que peuvent donner les méthodes directes. Nous allons exposer ici les observations que l'on peut déduire des notions précédentes; quant à ce qui exige des considérations plus profondes, nous le réserverons pour la section VIII.

Nous commencerons par le cas le plus simple; celui où $A=1$, c'est-à-dire, dans lequel on cherche les racines de la congruence $x^n \equiv 1 \pmod{p}$. En prenant pour base une racine primitive quelconque, on doit avoir $n \text{ Ind. } x \equiv 0 \pmod{p-1}$. Quand n est premier avec $p-1$, cette congruence n'aura qu'une seule racine, savoir..... $\text{Ind. } x \equiv 0 \pmod{p-1}$; donc, dans ce cas $\sqrt[n]{1} \pmod{p}$ n'aura qu'une valeur $x \equiv 1 \pmod{p}$; mais quand n et $p-1$ ont δ pour plus grand diviseur commun, la solution complète de la congruence $n \text{ Ind. } x \equiv 0 \pmod{p-1}$ sera $x \equiv 0 \left(\text{mod.} \frac{p-1}{\delta}\right)$ (n° 30), c'est-à-dire, que Ind. x devra être congru suivant le module $p-1$ à quelqu'un des nombres $0, \frac{p-1}{\delta}, \frac{2(p-1)}{\delta}, \ldots \frac{(\delta-1)(p-1)}{\delta}$, ou qu'il aura δ valeurs incongrues suivant le module $p-1$; donc aussi, dans ce cas, x aura δ valeurs incongrues suivant p. On voit aussi que l'expression $\sqrt[\delta]{1} \pmod{p}$ a aussi δ valeurs dont les indices sont absolument les mêmes que les précédens; donc l'expression $\sqrt[\delta]{1} \pmod{p}$ est tout-à-fait équivalente à l'expression $\sqrt[n]{1} \pmod{p}$, ou ce qui revient au même, la congruence $x^{\delta} \equiv 1 \pmod{p}$ et la congruence $x^n \equiv 1 \pmod{p}$ ont les mêmes racines; mais la première est d'un degré inférieur à moins qu'on n'ait $\delta = n$.

Ex. $\sqrt[15]{1} \pmod{19}$ a trois valeurs, parceque 3 est le plus grand commun diviseur de 15 et 18; elles seront également celles de l'expression $\sqrt[3]{1} \pmod{19}$. Ces valeurs sont 1, 7, 11.

62. Cette réduction nous offre un grand avantage, puisqu'on n'a plus besoin de résoudre parmi les congruences de la forme $x^n \equiv 1 \pmod{p}$

que celles où n est diviseur du module diminué de l'unité. Mais nous ferons voir plus bas que les congruences de cette forme peuvent encore s'abaisser davantage, quoique ce qui précède ne suffise pas pour cela. Il y a cependant un cas que nous pouvons traiter ici à fond, celui où $n=2$. Il est évident en effet que les valeurs de l'expression $\sqrt[n]{1}$ (mod. p) seront $+1$ et -1, puisqu'elle n'en peut avoir plus de deux, et que $+1$ et -1 sont incongrus, à moins que le module ne soit $=2$, cas auquel il est clair que $\sqrt{2}$ n'aurait qu'une seule valeur. Il suit de là que $+1$ et -1 sont aussi les valeurs de l'expression $\sqrt[2m]{1}$ (mod. p), quand m est premier avec $\frac{p-1}{2}$, ce qui arrivera toujours lorsque le module sera tel que $\frac{p-1}{2}$ soit un nombre absolument premier; par exemple, quand $p=3, 5, 7, 11, 23$, etc., à moins que $p-1=2m$, cas auquel tous les nombres $1, 2, 3 \ldots p-1$ sont racines. Remarquons, comme conséquence, que l'indice de -1 est toujours $\equiv \frac{p-1}{2}$ (mod. $p-1$), quelle que soit la racine primitive que l'on prenne pour base; car 2 Ind. $(-1) \equiv 0$ (mod. $p-1$); donc Ind. (-1) sera $\equiv 0$ ou $\equiv \frac{p-1}{2}$; mais 0 est toujours l'indice de $+1$, et $+1$ et -1 doivent avoir des indices différens, excepté dans le cas où $p=2$, qu'il n'est pas nécessaire de considérer.

63. Nous avons fait voir (n° 61) que l'expression $\sqrt[n]{A}$ (mod. p) a δ valeurs différentes ou n'en a absolument aucune, si δ est le plus grand commun diviseur des nombres n et $p-1$. Or de même que nous avons trouvé que $\sqrt[n]{A}$ et $\sqrt[\delta]{A}$ étaient équivalentes quand on a $A \equiv 1$, nous prouverons plus généralement que l'expression $\sqrt[n]{A}$ peut toujours être ramenée à une autre $\sqrt[\delta]{B}$, à laquelle elle est équivalente. Soit en effet $x^n \equiv A$, et t une valeur quelconque de l'expression $\frac{\delta}{n}$ (mod. $p-1$) qui aura toujours (n° 31) des valeurs réelles. De la congruence $x^n \equiv A$ on déduit $x^{tn} \equiv A^t$; mais à cause de $tn \equiv \delta$ (mod. $p-1$), $x^{tn} \equiv x^\delta$; donc $x^\delta \equiv A^t$. Ainsi une valeur quelconque

de $\sqrt[n]{A}$ sera aussi une valeur de $\sqrt[\delta]{A'}$; et toutes les fois que $\sqrt[n]{A}$ aura des valeurs réelles, elle sera absolument équivalente à l'expression $\sqrt[\delta]{A'}$, puisqu'elle ne peut avoir de valeurs différentes, ni en moindre nombre. Il est vrai cependant que $\sqrt[\delta]{A'}$ peut avoir des valeurs réelles, sans que pour cela $\sqrt[n]{A}$ en ait nécessairement.

Exemple. Si l'on cherche les valeurs de l'expression $\sqrt[21]{2}$ (mod. 31), le plus grand commun diviseur des nombres 21 et 30 est 3, et 3 est une valeur de $\frac{3}{21}$ (mod. 30); donc si $\sqrt[21]{2}$ a des valeurs réelles, elle équivaudra à l'expression $\sqrt[3]{2^3}$ ou $\sqrt[3]{8}$; on trouve effectivement que les valeurs de la dernière qui sont 2, 10 et 19, satisfont aussi à la première.

64. Mais afin de ne pas entreprendre inutilement cette opération, il est nécessaire de chercher le caractère auquel on pourra reconnaître si $\sqrt[n]{A}$ admet ou non des valeurs réelles. Si on a une table d'indices la chose est facile, car (n° 60) $\sqrt[n]{A}$ aura des valeurs réelles quand Ind. A sera divisible par δ, en prenant pour base une racine primitive quelconque, et dans le cas contraire elle n'en aura pas; mais on peut aussi le découvrir sans le secours de cette table. Soit en effet k=Ind. A, si k est divisible par δ, $\frac{k(p-1)}{\delta}$ sera divisible par $p-1$ et réciproquement; mais l'indice du nombre $A^{\frac{p-1}{\delta}}$ est $\frac{k(p-1)}{\delta}$; donc si $\sqrt[n]{A}$ (mod. p) a des valeurs réelles, $A^{\frac{p-1}{\delta}}$ sera congru à l'unité; sinon, il sera incongru. Ainsi dans l'exemple de l'article précédent, on a $2^{10}=1024\equiv 1$ (mod. 31), d'où l'on conclut que l'expression $\sqrt[21]{2}$ (mod. 31) a des valeurs réelles. De même nous voyons par là que $\sqrt[2]{-1}$ (mod. p) a toujours deux valeurs réelles, quand p est de la forme $4m+1$, et n'en a aucune quand p est de la forme $4m+3$, car... $(-1)^{2m}=1$ et $(-1)^{2m+1}=-1$. Ce théorème élégant qui

s'énonce ordinairement ainsi: *Si* p *est un nombre premier de la forme* $4m+1$, *on peut trouver un quarré* a^2 *qui rende* a^2+1 *divisible par* p; *mais si* p *est de la forme* $4m-1$, *on ne le pourra pas*, a été démontré de cette manière par *Euler* (*Comment. nov. Ac. Petrop. T.* XVIII, *p.* 112, 1773). Il en avait donné une autre démonstration bien antérieurement (*Comm. nov. T.*v, *p.* 5, 1760); dans une première dissertation (T. IV, p. 25), il n'était pas encore parvenu au but. *Lagrange* a depuis donné aussi une démonstration de ce théorème (*Nouv. Mém. de l'Ac. de Berlin.* 1775, *p.* 342). Nous en exposerons encore une différente dans la section suivante, qui sera consacrée à ce genre de considérations.

65. Après avoir examiné comment on peut réduire toutes les expressions $\sqrt[n]{A}\pmod p$ à d'autres dans lesquelles n soit diviseur de $p-1$, et après avoir trouvé le caractère auquel on reconnaît s'il y a des racines réelles ou non, considérons avec plus de soin les expressions $\sqrt[n]{A}\pmod p$, dans lesquelles n est diviseur de $p-1$. Nous ferons voir d'abord quelle est la relation qu'ont entr'elles les différentes valeurs de cette expression, ensuite nous indiquerons quelques artifices au moyen desquels on peut le plus souvent trouver une des valeurs.

1°. Quand $A\equiv 1$, et que r sera une des valeurs de l'expression $\sqrt[n]{1}\pmod p$, ou que $r^n\equiv 1\pmod p$, toutes les puissances de r seront aussi des valeurs de cette expression; et il y en aura autant de différentes qu'il y a d'unités dans l'exposant auquel r appartient (n° 48). Si donc r est une valeur appartenant à l'exposant n, les puissances $r, r^2, r^3, r^4, \ldots r^n$ (où l'unité peut remplacer la dernière) renfermeront toutes les valeurs de l'expression $\sqrt[n]{1}\pmod p$. Nous expliquerons plus en détail dans la section VIII comment on peut trouver ces valeurs qui appartiennent à l'exposant n.

2°. Quand A est incongru à l'unité, et que l'on connaît une valeur z de l'expression $\sqrt[n]{A}\pmod p$, on trouve les autres de la manière suivante: soient $1, r, r^2, r^3, \ldots, r^{n-1}$ les valeurs de $\sqrt[n]{1}$, on aura $z, zr, zr^2, zr^3 \ldots zr^{n-1}$ pour les valeurs de $\sqrt[n]{A}$; car il est évident que tous ces nombres satisferont à la congruence $x^n\equiv A$; puis-

qu'en effet, si zr^k est un des nombres de la suite, comme $r^k \equiv 1$ et que $z^n \equiv A$, on aura $r^{nk} \equiv 1$, et partant $z^n r^{nk} = (zr^k)^n \equiv A$. Il est aisé de juger que toutes ces valeurs sont différentes (n° 23); donc l'expression $\sqrt[n]{A}$ ne peut avoir d'autres valeurs, puisqu'elle ne peut en avoir plus de n. Par exemple, si une valeur de $\sqrt[2]{A}$ est z, l'autre sera $-z$. On doit conclure de ce qui précède, que l'on ne peut trouver toutes les valeurs de $\sqrt[n]{A}$, à moins qu'on ne puisse avoir toutes celles de $\sqrt[n]{1}$.

66. La seconde recherche que nous nous étions proposée, consiste à déterminer le cas où l'on peut trouver directement une valeur de l'expression $\sqrt[n]{A}$ (mod. p), dans laquelle n est diviseur de $p-1$. Cela arrive quand il y a une valeur congrue à une puissance de A, et comme ce cas est très-fréquent, il ne sera pas déplacé de s'y arrêter un instant. Soit z cette valeur, si elle existe, on aura $z \equiv A^k$ et $z^n \equiv A$ (mod. p); donc $A \equiv A^{kn}$; et si l'on peut déterminer k de manière que cette condition soit remplie, A^k sera la valeur cherchée; mais la condition précédente revient à celle-ci $kn \equiv 1$ (mod. t), t étant l'exposant auquel A appartient. Or pour que cette congruence soit possible, il faut que n soit premier avec t, et dans ce cas on aura $k = \frac{1}{n}$ (mod. t); si au contraire t et n ont un diviseur commun, aucune valeur de z ne sera congrue à une puissance de A.

67. Mais comme il est nécessaire pour cette solution de connaître t, voyons comment il faut procéder quand on ne le connaît pas. On voit d'abord facilement que t doit être diviseur de $\frac{p-1}{n}$, lorsque $\sqrt[n]{A}$ (mod. p) a des valeurs réelles, ce que nous supposons ici. Soit en effet y l'une quelconque de ces valeurs, on aura (n° 50) $y^{p-1} \equiv 1$, et $y^n \equiv A$ (mod. p); en élevant à la puissance $\frac{p-1}{n}$ les deux membres de la congruence $y^n \equiv A$, on aura $y^{p-1} \equiv A^{\frac{p-1}{n}} \equiv 1$; d'ailleurs $A^t \equiv 1$; donc $\frac{p-1}{n} \equiv 0$ (mod. t) (n° 48). Or si $\frac{p-1}{n}$ est

premier avec n, la congruence $kn \equiv 1$ pourra être résolue suivant le module $\frac{p-1}{n}$, et toute valeur de k qui y satisfera suivant ce module, y satisfera aussi (n° 5) suivant le module t diviseur de $\frac{p-1}{n}$; donc on trouvera alors ce qu'on cherchait. Si $\frac{p-1}{n}$ n'est pas premier avec n, soit q le produit des facteurs premiers de $\frac{p-1}{n}$ qui divisent en même temps n; $\frac{p-1}{nq}$ sera premier avec n, et si la condition que t soit premier avec n a lieu, t sera aussi premier avec q, et comme il divise $\frac{p-1}{n}$, il divisera donc $\frac{p-1}{nq}$; ainsi en résolvant la congruence $kn \equiv 1 \left(\text{mod.} \frac{p-1}{nq}\right)$, ce qui peut se faire puisque n est premier avec $\frac{p-1}{nq}$, la valeur de k satisfera aussi à la congruence, suivant le module t. Tout l'artifice consiste à trouver un nombre qui puisse remplacer t, que nous ne connaissons pas; mais il faut se souvenir que dans le cas où $\frac{p-1}{n}$ n'est pas premier avec n, nous avons supposé n premier avec t; et si cette condition manque, toutes les conclusions sont fausses; c'est pourquoi, si en suivant témérairement les règles, on trouve pour z une valeur dont la puissance n ne soit pas congrue à A; le résultat prouvera que cette condition n'a pas lieu, et que partant la méthode n'est pas applicable.

68. Mais dans ce cas même, il est souvent avantageux de faire cette recherche: elle offre l'avantage de faire trouver de vraies valeurs au moyen des fausses. Supposons en effet que les nombres k et z aient été convenablement déterminés, mais qu'on n'ait pas $z^n \equiv A \ (\text{mod. } p)$. Alors si on pouvait seulement déterminer les valeurs de $\sqrt[n]{\frac{A}{z^n}} \ (\text{mod. } p)$, ces différentes valeurs étant multipliées par z donneraient celles de $\sqrt[n]{A}$: en effet, si ν est une valeur de $\sqrt[n]{\frac{A}{z^n}}$ on aura $\nu^n z^n \equiv A$; mais l'expression $\sqrt[n]{\frac{A}{z^n}}$ est plus simple que $\sqrt[n]{A}$, parceque le plus souvent $\frac{A}{z^n}$ appartient à un exposant moindre que A; car si d est le plus grand commun diviseur

seur de t et de q, $\frac{A}{z^n}$ (mod. p) appartiendra à l'exposant d, ce qui se démontre ainsi : puisque $z \equiv A^k$, il vient $\frac{A}{z^n} \cdot A^{kn-1} \equiv 1$ (mod. p); mais $kn-1$ est divisible par $\frac{p-1}{nq}$ (n° préc.), $\frac{p-1}{n}$ l'est par t, ou $\frac{p-1}{nd}$ par $\frac{t}{d}$. D'ailleurs $\frac{t}{d}$ est premier avec $\frac{q}{d}$; donc aussi $\frac{p-1}{nd}$ est divisible par $\frac{tq}{d^2}$, ou $\frac{p-1}{nq}$ par $\frac{t}{d}$, et partant $kn-1$ par $\frac{t}{d}$, ou $(kn-1)d$ par t. Donc $A^{(kn-1)d} \equiv 1$ (mod. p); d'où l'on déduit facilement que $\frac{A}{z^n}$ élevé à la puissance d est congru à l'unité. Il serait facile de démontrer que $\frac{A}{z^n}$ ne peut pas appartenir à un exposant plus petit que d; mais comme cette démonstration ne peut nous être utile, nous ne nous y arrêterons pas. Nous sommes donc certains que $\frac{A}{z^n}$ (mod. p) appartient toujours à un plus petit exposant que A, excepté dans le cas unique où l'on aurait $d = t$.

Mais à quoi sert que $\frac{A}{z^n}$ appartienne à un plus petit exposant que A? Il y a plus de nombres qui peuvent être A qu'il n'y en a qui peuvent être $\frac{A}{z^n}$, et quand on a occasion de résoudre plusieurs expressions de la forme $\sqrt[n]{A}$, suivant le même module, on y gagne de pouvoir tirer d'une même source la solution de plusieurs. Ainsi, par exemple, on déterminera au moins une valeur de $\sqrt[3]{A}$ (mod. 29), si l'on connaît seulement les valeurs de $\sqrt[3]{-1}$ (mod. 29), qui sont ± 12; en effet l'on voit sans peine, par les articles précédens, que l'on déterminera d'une manière directe une valeur quand t est impair, et que d sera $= 2$ quand t est pair; or il n'y a que -1 qui appartienne à l'exposant 2.

Exemples.

Soit $\sqrt[3]{31}$ (mod. 37); on a $p-1 = 36$, $n = 3$, $\frac{p-1}{n} = 12$, et partant $q = 3$; il faut donc qu'on ait $3k \equiv 1$ (mod. 4), ce qui

donne $k \equiv 3$. Donc $z \equiv 31^3 \pmod{37} \equiv 6$; l'on trouve effectivement $6^3 = 31 \pmod{37}$. Si les valeurs de $\sqrt[3]{1} \pmod{37}$ étaient connues, on pourrait aussi déterminer les autres valeurs de $\sqrt[3]{31}$: or les valeurs de $\sqrt[3]{1} \pmod{37}$ sont 1, 10, 26; donc celles de $\sqrt[3]{31}$ seront 6, 23, 8.

Soit maintenant $\sqrt[2]{3} \pmod{37}$; on aura $p-1 = 36$, $n = 2$, $\frac{p-1}{n} = 18$, et partant $q = 2$; donc on doit avoir $2k \equiv 1 \pmod{9}$, d'où $k \equiv 5$; donc $z \equiv 3^5 \equiv 21 \pmod{37}$; mais 21^2 n'est pas congru avec 3, mais avec 34; or on a $\frac{3}{34} \pmod{37} \equiv -1$ et $\sqrt[2]{-1} \pmod{37} \equiv \pm 6$; d'où l'on tire les vraies valeurs $\pm 6.21 \equiv \pm 15$.

Voilà à-peu-près tout ce que nous pouvions exposer ici sur la résolution de ces expressions. Il est clair que les méthodes directes deviennent souvent assez longues; mais cet inconvénient a lieu dans presque toutes les méthodes directes de la théorie des nombres: Aussi nous n'avons pas cru devoir négliger de faire voir ce qu'on peut en attendre. Il convient aussi d'observer que les artifices particuliers qui se présentent à un homme exercé, n'entrent pas dans notre plan.

69. Revenons maintenant aux racines que nous avons appelées *primitives*. Nous avons fait voir que, si l'on prenait pour base une racine primitive quelconque, tous les nombres dont les indices sont premiers avec $p-1$, étaient aussi des racines primitives, et qu'il n'y en aurait pas d'autres, d'où nous avons conclu le nombre de ces racines (n° 53): et comme le choix de celle que l'on prend pour base est en général arbitraire, on voit qu'ici, comme dans les logarithmes, on peut avoir plusieurs systèmes (*). Cherchons les relations qui les lient entr'eux. Soient a et b deux racines primitives, et m un autre nombre. Soit de plus Ind. $b \equiv \beta$, quand a est pris pour base, Ind. $m \equiv \mu \pmod{p-1}$. Soit au contraire Ind. $a \equiv \alpha$, Ind. $m \equiv \nu \pmod{p-1}$ dans l'hypothèse où l'on prend b pour base; on aura $a^{\beta} \equiv b$,

(*) Mais ils diffèrent en cela, que dans les logarithmes le nombre des systèmes est infini, et qu'il est ici égal au nombre des racines primitives, car les bases congrues produisent évidemment les mêmes systèmes.

donc $a_{\alpha}^{\beta} \equiv b^{\alpha} \equiv a$, d'où $\alpha\beta \equiv 1 \pmod{p-1}$. On trouvera de même $\nu \equiv \alpha\mu$, $\mu \equiv \beta\nu \pmod{p-1}$. Si donc on a une table d'indices construite pour la base a, on pourra facilement la changer en une autre dont la base est b. En effet, si Ind. $b \equiv \beta$ pour la base a, Ind. a sera $\equiv \frac{1}{\beta} \pmod{p-1}$ pour la base b, et multipliant par ce nombre tous les indices de la table, on aura tous les indices pour la base b,

70. Mais quoiqu'un nombre donné puisse avoir plusieurs indices, en prenant pour base différentes racines primitives, tous ces indices auront cette propriété commune, que leur plus grand commun diviseur avec $p-1$ sera le même. En effet, A étant un nombre donné, si Ind. $A \equiv m$ pour la base a, et Ind. $A \equiv n$ pour la base b, et si leurs plus grands communs diviseurs μ et ν avec $p-1$ sont supposés inégaux; soit $\mu > \nu$, μ ne divisera pas n; mais si Ind. $a \equiv \alpha$ pour la base b, on aura (art. précéd.) $n \equiv \alpha m \pmod{p-1}$, et partant μ divisera aussi n.

On peut encore s'assurer que ce diviseur commun des indices d'un nombre donné et de $p-1$, est indépendant de la base en observant qu'il est égal à $\frac{p-1}{t}$, t étant l'exposant auquel appartient le nombre dont il s'agit. En effet, si l'indice est k pour une base quelconque, t sera le plus petit nombre (zéro excepté), qui multiplié par k, donne un produit divisible par $p-1$, ou la plus petite valeur de l'expression $\frac{0}{k} \pmod{p-1}$; mais on déduit sans peine du n° 29 que cette valeur est égale au plus grand commun diviseur des nombres k et $p-1$. (*)

(*) La dernière phrase de l'auteur ne me semble point prouver ce qu'il a avancé; il s'y est sans doute glissé quelques fautes d'impression qui lui ont échappé. Au reste je crois que l'on peut y suppléer de la manière suivante :

Puisque t est le plus petit nombre qui rende kt divisible par $p-1$, ce sera aussi celui qui rendra $\frac{kt}{d}$ divisible par $\frac{p-1}{d}$, d étant le plus grand commun diviseur entre k et $p-1$. Or $\frac{k}{d}$ et $\frac{p-1}{d}$ étant premiers entre eux, la plus petite valeur de t convenable est $\frac{p-1}{d}$; donc $\frac{p-1}{d} = t$ et $d = \frac{p-1}{t}$. (*Note du traducteur.*)

71. On démontre facilement que l'on peut toujours trouver une base telle, qu'un nombre appartenant à l'exposant t ait un indice donné à volonté. Le plus grand commun diviseur de cet indice et de $p-1$ étant $\frac{p-1}{t}$, désignons par d ce diviseur, et soit l'indice proposé $\equiv dm$; soit dn l'indice du nombre donné quand on prend pour base la racine primitive quelconque a; on aura m et n premiers avec $\frac{p-1}{d}$ ou t. Or si ε est une valeur de l'expression $\frac{dn}{dm}$ (mod. $p-1$), et en même temps premier avec $p-1$, a^{ε} sera la racine primitive cherchée, car on aura $a^{\varepsilon dm} \equiv a^{dn} \equiv$ au nombre proposé (mod. p). Il nous reste à prouver que l'expression $\frac{dn}{dm}$ (mod. $p-1$) peut admettre des valeurs premières avec $p-1$; elle équivaut à $\frac{n}{m}$ (mod. $\frac{p-1}{d}$) ou $\frac{n}{m}$ (mod. t), (n° 31, 2°) et toutes les valeurs en seront premières avec t; car si une valeur e avait un diviseur commun avec t, ce diviseur devrait aussi diviser me, et partant diviser n qui est congru à me, suivant le module t, ce qui est contre l'hypothèse suivant laquelle n est premier avec t. Ainsi, quand tous les diviseurs premiers de $p-1$ divisent aussi t, toutes les valeurs de l'expression $\frac{n}{m}$ (mod. t) sont premières avec $p-1$, et leur nombre est d; mais quand $p-1$ renferme encore d'autres facteurs premiers f, g, h, etc. qui ne divisent pas t, soit e une valeur de $\frac{n}{m}$ (mod. t), comme t, f, g, h, etc. sont premiers entre eux, on peut trouver un nombre ε congru à e suivant le module t, et congru, suivant f, g, h, etc., à des nombres quelconques premiers avec ceux-ci (n° 32). Ce nombre ne sera divisible par aucun facteur de $p-1$, et partant sera premier avec lui, comme il est nécessaire. On pourrait démontrer sans peine par la théorie des combinaisons, que le nombre de ces valeurs est $\frac{p-1}{t} \cdot \frac{f-1}{f} \cdot \frac{g-1}{g} \cdot \frac{h-1}{h}$. etc.; mais nous omettons cette démonstration qui ne peut nous être d'aucune utilité.

72. Quoiqu'en général on puisse prendre arbitrairement pour base une racine primitive quelconque, certains avantages parti-

culiers peuvent faire préférer une base à toute autre. Dans la table I nous avons toujours pris 10 pour base quand il était racine primitive, et dans les autres cas nous avons choisi la base de manière que l'indice du nombre 10 fût le plus petit possible, c'est-à-dire $=:\frac{p-1}{t}$, t étant l'exposant auquel 10 appartient. On en reconnaîtra l'avantage dans la sect. VI, où la même table sera employée à d'autres usages. Mais comme il peut encore rester ici quelque chose d'arbitraire, ainsi qu'on le voit par l'article précédent, nous avons toujours choisi, parmi toutes les racines primitives qui satisfont à la question, la plus petite pour base : ainsi pour $p=73$, on a $t=8$ et $d=9$, et a $\frac{72.2}{8.3}=6$ valeurs qui sont 5, 14, 20, 28, 39, 40, et nous avons pris 5 pour base.

73. La plupart des méthodes qui servent à trouver les racines primitives reposent en grande partie sur le tâtonnement. Si l'on réunit ce que nous avons dit (n° 55) avec ce que nous dirons plus bas sur la résolution de la congruence $x^n\equiv 1$, on aura à-peu-près tout ce qui peut se faire par les méthodes générales. Euler avoue (*Opuscula analyt. T.* 1, *p.* 152.) qu'il lui semble extrêmement difficile d'assigner ces nombres, et que leur nature doit être rangée dans les points les plus épineux de la théorie des nombres; mais on les trouve assez facilement par la méthode suivante. Les hommes exercés préviendront facilement la longueur du calcul par beaucoup d'artifices; mais l'usage les indique mieux que les préceptes.

1°. On prendra à volonté un nombre a premier avec le module p (*), et souvent le calcul devient plus simple lorsqu'on prend a le plus petit possible, 2 par exemple; on déterminera sa période (n° 46), c'est-à-dire les résidus *minima* de ses puissances, jusqu'à ce que l'on parvienne à une puissance a^t, qui ait 1 pour résidu *minimum* (**). Si l'on a $t=p-1$, a sera une racine primitive.

(*) Nous désignerons toujours le module par p.

(**) Il est aisé de voir qu'il n'est pas nécessaire de connaître ces puissances, car on peut obtenir le résidu *minimum* d'une puissance au moyen de la puissance précédente.

2°. Mais si $t<p-1$, on prendra un autre nombre b, qui ne soit pas contenu dans la période de a, et l'on cherchera de la même manière sa période. En nommant u l'exposant auquel b appartient, on voit facilement que u n'est ni égal à t, ni une de ses parties aliquotes, car dans les deux cas on aurait $b^t\equiv 1$, ce qui est impossible, la période de a renfermant tous les nombres dont la puissance t est congrue à l'unité (n° 53). Or si $u=p-1$, b sera une racine primitive; si u n'est pas $=p-1$, mais un multiple de t, nous aurons encore l'avantage de connaître un nombre qui appartienne à un exposant plus grand, et partant nous approcherons de notre but, puisque nous cherchons le nombre qui appartient à l'exposant *maximum*; mais si u n'est ni $=p-1$, ni multiple de t, nous pouvons trouver un nombre appartenant à un exposant plus grand que t et u; cet exposant sera le plus petit nombre divisible à la fois par t et u. En effet, soit y ce dernier nombre; on décomposera y en deux facteurs m et n premiers entre eux, dont l'un divise t et l'autre u (*).

Soit $a^{\frac{t}{m}}\equiv A$, $b^{\frac{u}{n}}\equiv B \pmod{p}$, AB appartiendra à l'exposant y; car on voit facilement que A appartient à l'exposant m, B à l'exposant n, et parconséquent AB appartiendra à l'exposant mn, puisque m et n sont premiers entre eux, comme on peut le démontrer en suivant exactement le procédé du n° 55.

3°. Si $y=p-1$, AB sera une racine primitive, sinon on prendra de même un troisième nombre qui ne se trouve pas dans la période de AB; ce nombre sera une racine primitive, ou bien il appartiendra à un exposant $>y$, ou bien enfin par son moyen on déterminera un nombre appartenant à un exposant $>y$: donc, comme les nombres qui résultent de la répétition de cette opération, appartiennent à des

---

(*) On voit facilement par le n° 18 comment on peut faire cette décomposition. On décomposera y en facteurs qui soient des nombres premiers ou des puissances de nombres premiers différens; chacun d'eux divisera t ou u, ou tous les deux. On écrira sous t ou sous u ceux qui divisent t ou u. Quant à ceux qui diviseront u et t, peu importe sous lequel on les écrive. Si l'on fait $m=$ le produit de ceux qui sont écrits sous t, $n=$ le produit de ceux qui sont écrits sous u, il est évident que m divisera t, que n divisera u et que $mn=y$.

exposans qui vont toujours en augmentant, et sont néanmoins diviseurs de $p-1$, il est évident qu'on en trouvera enfin un qui appartiendra au *maximum* $p-1$, ce sera la racine primitive.

74. Eclaircissons ceci par un exemple. Soit $p=73$, pour lequel on demande une racine primitive. Essayons d'abord le nombre 2, dont la période est

1.2.4.8.16.32.64.55.37.1 etc.
0.1.2.3. 4. 5. 6. 7. 8.9 etc.

Donc puisque $2^9\equiv 1$, 2 n'est pas racine primitive. Essayons le nombre 3 qui ne se trouve pas dans la période de 2, sa période est

1.3.9.27.8.24.72.70.64.46.65.49. 1 etc.
0.1.2. 3.4. 5. 6. 7. 8. 9.19.11.12 etc.

Donc 3 n'est pas non plus racine primitive; mais le plus petit nombre divisible à la fois par les exposans 9 et 12, auxquels 2 et 3 appartiennent, est 36, qui donne $m=9$ et $n=4$. Donc élevant 2 à la puissance $\frac{9}{9}=1$, 3 à la puissance $\frac{12}{4}=3$, le produit de ces deux puissances est 54, qui appartiendra à l'exposant 36. Si enfin on calcule la période de 54, et qu'on essaye un nombre qui n'y soit pas contenu, 5 par exemple, on trouve qu'il est racine primitive.

75. Avant d'abandonner ce sujet, nous présenterons quelques propositions qui ne nous paraissent pas indignes d'attention, à cause de leur simplicité.

Le produit de tous les termes de la période d'un nombre quelconque est $\equiv 1$ *quand leur nombre ou l'exposant auquel appartient le nombre dont il s'agit est impair, et* $\equiv -1$ *quand il eis pair.*

Par exemple, pour le module 13, la période de 5 est composée des termes 1, 5, 12, 8, dont le produit $480\equiv -1$ (mod. 13), suivant le même module, la période de 3 est composée des termes 1, 3, 9, dont le produit $27\equiv 1$ (mod. 13).

Soit t l'exposant auquel le nombre appartient; on peut toujours trouver (n° 71) une base pour laquelle l'indice du nombre soit $\frac{p-1}{t}$

Or l'indice du produit de tous les termes sera

$$\equiv(1+2+3+\text{etc.}+t-1)\,\frac{p-1}{t} = \frac{(t-1)(p-1)}{2};$$

donc il sera $\equiv 0 \pmod{p-1}$, quand t est impair; et $\equiv \frac{p-1}{2}$, quand t est pair. Dans le premier cas, le produit est $\equiv 1 \pmod{p}$; dans le second, $\equiv -1 \pmod{p}$.

76. Si le nombre du théorème précédent est une racine primitive, sa période comprendra tous les nombres $1, 2, 3, 4, \ldots p-1$, dont le produit sera parconséquent toujours $\equiv -1$; car $p-1$ est toujours pair, excepté dans le cas où $p=2$, et alors on a indifféremment $+1$ ou -1. Ce théorème élégant qu'on énonce ordinairement de cette manière: *Le produit de tous les nombres plus petits qu'un nombre premier étant augmenté de l'unité, est divisible par ce nombre premier*, a été publié par *Waring* qui l'attribue à *Wilson* (*Meditationes Algeb. Ed.* 3, *p.* 380); mais aucun des deux n'a pu le démontrer, et *Waring* avoue que la démonstration lui en semble d'autant plus difficile qu'il n'y a point de *notation* par laquelle on puisse exprimer un nombre premier; pour nous, nous pensons que la démonstration de cette sorte de vérités doit être puisée dans les principes plutôt que dans la notation. *Lagrange* en a depuis donné une démonstration (*Nouv. Mém. de l'Ac. de Berlin*, 1771), dans laquelle il s'appuie sur la considération des coefficiens que l'on trouve en développant le produit

$$(x+1)(x+2)(x+3)\ldots(x+p-1):$$

et il fait voir qu'en supposant ce produit

$$= x^{p-1} + Ax^{p-2} + Bx^{p-3} + \text{etc.} + Mx + N,$$

les coefficiens A, B, etc. M sont divisibles par p; or

$$N = 1.2.3\ldots p-1.$$

Maintenant si $x=1$, le produit est divisible par p; mais alors il sera $\equiv 1 + N \pmod{p}$, donc $1+N$ est divisible par p.

Enfin Euler (*Opusc. analyt. T.* 1, *p.* 329) en a donné une démonstration qui rentre dans celle que nous venons d'exposer; ainsi puisque de tels hommes n'ont pas cru ce sujet indigne de leurs méditations

méditations, nous espérons qu'on ne nous désapprouvera pas d'offrir encore ici une autre manière de démontrer ce théorème.

77. Nous dirons que deux nombres sont *associés*, comme l'a fait *Euler*, lorsque leur produit sera congru à l'unité. Cela posé, par la section précédente, tout nombre positif moindre que p, aura toujours un nombre associé moindre que p et il n'en aura qu'un; or il est facile de prouver que parmi les nombres $1, 2, 3, \ldots p-1$, il n'y a que 1 et $p-1$ qui soient eux-mêmes leurs associés, car ceux qui jouiront de cette propriété seront donnés par la congruence $x^2 \equiv 1$ qui ne peut avoir que deux racines 1 et $p-1$. Supprimant donc ces deux nombres, les autres $2, 3, 4 \ldots p-2$, seront associés deux à deux; donc leur produit sera $\equiv 1$; enfin multipliant par $p-1$, le produit de tous $1.2.3.4 \ldots p-1 \equiv p-1 \equiv -1$.

Par exemple, pour $p=13$, les nombres $2, 3, 4, 5, \ldots 11$ s'associent de la manière suivante: 2 avec 7, 3 avec 9, 4 avec 10, 5 avec 8, 6 avec 11; donc $2.3.4 \ldots 11 \equiv 1$, et partant..... $1.2.3 \ldots 12 \equiv 12 \equiv -1$.

78. Le théorème de *Wilson* peut être rendu plus général en l'énonçant comme il suit : *Le produit de tous les nombres premiers avec un nombre donné* A *et moindres que ce nombre, est congru suivant* A, *à l'unité prise positivement ou négativement.* L'unité doit être prise négativement quand A est de la forme p^m ou $2p^m$, p étant un nombre premier différent de 2, ou encore quand $A=4$, et positivement dans tous les autres cas. Le théorème de Wilson est contenu dans le premier cas. *Exemple.* Pour $A=15$, le produit des nombres 1, 2, 4, 7, 8, 11, 13, 14, est $\equiv 1$ (mod. 15). Nous supprimons, pour abréger, la démonstration. Nous observerons seulement qu'on peut y parvenir comme dans l'article précédent, excepté que la congruence $x^2 \equiv 1$ peut avoir plus de deux racines, ce qui demande certaines considérations particulières. On pourrait aussi la tirer de la considération des indices, comme dans le n° 75, si l'on y joint ce que nous dirons tout à l'heure des modules composés.

79. Revenons à l'énumération des autres propositions (n° 75).

La somme de tous les termes de la période d'un nombre quelconque est $\equiv 0$.

Ainsi dans l'exemple du n° 75

$$1+5+12+8=26\equiv 0 \pmod{13}.$$

Soit a le nombre dont il s'agit, et t l'exposant auquel il appartient. La somme de tous les termes de la période sera.....
$\equiv 1+a+a^2+a^3+\ldots\ldots+a^{t-1}\equiv\frac{a^t-1}{a-1}\pmod{p}$; or $a^t-1\equiv 0$, donc aussi $\frac{a^t-1}{a-1}\equiv 0$, si $a-1$ n'est pas divisible par p; il faut donc excepter ce cas, si nous voulons regarder même un seul terme comme une *période*.

80. *Le produit de toutes les racines primitives est* $\equiv 1$, excepté le cas où $p=3$, car alors il n'y a qu'une racine primitive 2.

Si l'on prend pour base une racine primitive quelconque, les indices de toutes les racines primitives seront des nombres premiers avec $p-1$ et moindres que lui; mais la somme de tous ces nombres, c'est-à-dire l'indice du produit de toutes les racines primitives, est $\equiv 0 \pmod{p-1}$; donc le produit est $\equiv 1 \pmod{p}$. En effet on voit facilement que si k est un nombre premier avec $p-1$, $p-1-k$ le sera aussi, et que parconséquent la somme des nombres premiers avec $p-1$ est composée de couples dont la somme est divisible par $p-1$. Il est bon d'observer que k ne peut être égal à $p-1-k$, à moins que $\frac{p-1}{2}$ ne soit premier avec $p-1$, ce qui exige que $p-1=2$ ou $p=3$, cas que nous exceptons.

81. *La somme des racines primitives est* $\equiv 0$ quand $p-1$ est divisible par un quarré, *ou* $\equiv\pm 1$ quand $p-1$ est le produit de facteurs premiers inégaux. Le signe $+$ appartenant au cas où le nombre de ces facteurs est pair, le signe $-$ au cas où il est impair.

Ex. 1°. Pour $p=13$, on a les racines primitives 2, 6, 7, 11 dont la somme $26\equiv 0 \pmod{13}$. 2°. Pour $p=11$, les racines primitives sont 2, 6, 7, 8, dont la somme $23\equiv +1 \pmod{11}$. 3°. Pour $p=31$, les racines primitives sont 3, 11, 12, 13, 17, 21, 22, 24, dont la somme $123\equiv -1 \pmod{31}$.

Nous avons démontré plus haut (n° 55, 2°) que si l'on a... $p-1=a^\alpha b^\beta c^\gamma$ etc., et que A, B, C, etc. soient des nombres quelconques qui appartiennent aux exposans a^α, b^β, c^γ, etc. respectivement, tous les produits ABC etc. seront des racines primitives;

mais on peut aussi démontrer facilement qu'une racine primitive quelconque peut s'exprimer par un produit de cette espèce et d'une seule façon (*).

Il suit de là que ces produits peuvent être pris au lieu des racines primitives; mais, comme dans ces produits il faut combiner toutes les valeurs de A avec toutes celles de B, etc., la somme de tous ces produits sera égale au produit de la somme des valeurs de A, multipliée par la somme des valeurs de B, etc. Désignons toutes les valeurs de A, B, C, etc. par A, A', A'', etc. B, B', B'', etc. C, C', C'', etc. La somme de toutes les racines primitives sera congrue au produit $(A+A'+\text{etc.})\,(B+B'+\text{etc.})$ etc.; or je dis que si $\alpha=1$, la somme $A+A'+A''+\text{etc.}$, sera $\equiv -1 \pmod{p}$, que si $\alpha>1$, cette somme sera $\equiv 0$, et de même pour β, γ, etc. Si ces

(*) On déterminera des nombres α', β', γ', etc. tels qu'on ait $\alpha' \equiv 1 \pmod{a^\alpha}$ et $\equiv 0 \pmod{b^\beta\, c^\gamma}$ etc.); $\beta' \equiv 1 \pmod{b^\beta}$ et $\equiv 0 \pmod{a^\alpha\, c^\gamma}$ etc.), etc. (*v.* n° 32); donc on aura $\alpha'+\beta'+\gamma'+\text{etc.} \equiv 1 \pmod{p-1}$, (n° 19). Or si l'on doit exprimer une racine primitive quelconque r par un produit de la forme ABC etc.; on prendra $A \equiv r^{\alpha'}$, $B \equiv r^{\beta'}$, $C \equiv r^{\gamma'}$, etc. A, B, C appartiendront respectivement aux exposans a^α, b^β, c^γ, etc., et le produit ABC etc. sera $\equiv r \pmod{p}$. Or il est facile de voir que A, B, C, etc. ne peuvent se déterminer d'une autre manière (1).

(1) Cette note nous semble avoir besoin de quelques éclaircissemens. Il est aisé de voir que tous les nombres, excepté α', sont divisibles par a^α; que partant leur somme l'est aussi, ou est $\equiv 0 \pmod{a^\alpha}$; mais comme $\alpha' \equiv 1 \pmod{a^\alpha}$, il vient donc $\alpha'+\beta'+\gamma'+\text{etc.} \equiv 1 \pmod{a^\alpha}$, de même $\alpha'+\beta'+\gamma'+\text{etc.} \equiv 1 \pmod{b^\beta}$, etc.; donc $\alpha'+\beta+\gamma'+\text{etc.} \equiv 1 \pmod{a^\alpha\, b^\beta\, c^\gamma}$, etc.) $\equiv 1 \pmod{p-1}$. Or si l'on fait $A \equiv r^{\alpha'}$, $B \equiv r^{\beta'}$, $C \equiv r^{\gamma'}$, etc. A, B, C, etc. appartiendront aux exposans a^α, b^β, c^γ, etc. respectivement. En effet $A^{a^\alpha} \equiv r^{\alpha' a^\alpha} \equiv 1 \pmod{p}$, $\alpha' a^\alpha$ étant $\equiv 0 \pmod{p-1}$, et il est visible que l'on ne peut supposer $A^t \equiv 1 \pmod{p}$, t étant $<\alpha$, et de même pour B, C, etc., car on aurait $\alpha' t \equiv 0 \pmod{p-1}$, ce qui ne peut avoir lieu à moins que t ne soit $= a^\alpha$ ou $\equiv 0 \pmod{a^\alpha}$. Or il est aisé de s'assurer encore qu'on ne peut trouver de nombres A', B', C', etc. respectivement incongrus à A, B, C, etc., et qui puissent les remplacer. En effet on aurait $A' \equiv r^{\alpha''}$, α'' étant un nombre déterminé comme α'; mais on a aussi $A \equiv r^{\alpha'}$; or comme α' et α'' sont congrus au même nombre suivant le module $p-1$, ils sont congrus entr'eux suivant ce même module; donc $r^{\alpha'} \equiv r^{\alpha''} \pmod{p}$, et partant $A \equiv A'$. (*Note du traducteur.*)

deux assertions sont démontrées, la vérité du théorème sera manifeste. En effet, quand $p-1$ est divisible par un quarré, quelqu'un des exposans α, β, γ, etc. sera >1, et partant un des facteurs dont le produit est congru à la somme des racines primitives, sera $\equiv 0$, c'est-à-dire que le produit lui-même le sera. Quand $p-1$ ne pourra être divisé par aucun quarré, tous les exposans α, β, γ, etc. seront égaux à l'unité, et la somme des racines primitives sera congrue au produit d'autant de facteurs dont chacun $\equiv -1$, qu'il y a de nombres a, b, c, etc.; donc partant le produit sera $\equiv \pm 1$, suivant qu'ils seront en nombre pair ou impair; or ces deux assertions se prouvent ainsi qu'il suit :

1°. Quand $\alpha = 1$, et que A est un nombre appartenant à l'exposant a, les autres nombres qui appartiennent aussi à cet exposant sont A^2, A^3, $\ldots A^{a-1}$; or $1 + A + A^2 + A^3 + A^4 + \ldots A^{a-1}$ est la somme de la période complète, et partant $\equiv 0$ (n° 79); donc

$$A + A^2 + A^3 + \ldots + A^{a-1} \equiv -1.$$

2°. Quand $\alpha > 1$, et que A est un nombre appartenant à l'exposant a^α, on aura les autres nombres appartenans au même exposant, si de la suite A^2, A^3, A^4, $\ldots A^{a^\alpha - 1}$, on retranche A^a, A^{2a}, A^{3a}, etc. (n° 53), leur somme sera donc

$$\equiv 1 + A + A^2 + \ldots + A^{a^\alpha - 1} - (1 + A^a + A^{2a} + \ldots + A^{a^\alpha - a});$$

c'est-à-dire congrue à la différence de deux périodes, et par-conséquent $\equiv 0$.

82. Tout ce que nous avons exposé jusqu'à présent, suppose que le module soit un nombre premier. Il nous reste à considérer le cas où l'on prend pour module un nombre composé; mais comme il n'en résulte pas des propriétés aussi élégantes que dans le premier cas, et qu'il n'y a pas besoin d'artifices bien délicats pour les trouver, tout se déduisant presque de la seule application des principes précédens, il serait superflu et fastidieux d'épuiser ici tous les détails. Aussi nous exposerons en peu de mots ce que ce second cas a de commun avec le premier, et ce qui lui est propre.

83. Les propositions des nos 45—48 ont déjà été démontrées généralement, mais celle du n° 49 doit être changée ainsi :

Si f *désigne combien il y a de nombres premiers avec* m *et moindres que lui, c'est-à-dire si* f=φm (*art.* 38), *l'exposant* t *de la plus petite puissance d'un nombre donné* a *premier avec* m, *qui est congrue à l'unité suivant le module* m *sera* =f, *ou une partie aliquote de* f.

La démonstration de la proposition du n° 49 peut servir également dans ce cas-ci, en y substituant m pour p, f pour $p-1$, et au lieu des nombres $1, 2, 3, \ldots p-1$, les nombres premiers avec m et moindres que lui; ainsi nous y renvoyons le lecteur. Mais les autres démonstrations dont nous avons parlé (n°s 50, 51), ne peuvent s'appliquer à ce cas sans beaucoup d'embarras. A l'égard des propositions suivantes (n° 52 et suivans), il y a une grande différence entre les modules qui sont les puissances d'un nombre prémier et ceux qui sont divisibles par plusieurs nombres premiers. Nous considérerons donc à part les modules du premier genre.

84. Si le module $m=p^n$, p étant un nombre premier, on aura $f=p^{n-1}(p-1)$, (n° 38). Or si l'on applique à ce cas les recherches contenues (n°s 53, 55), *mutatis mutandis* comme dans l'article précédent, on trouvera que tout ce qui y a été démontré aurait lieu également, s'il était prouvé que la congruence $x^t-1\equiv 0 \pmod{p^n}$, ne peut avoir plus de t racines différentes. C'est d'une proposition plus générale (n° 43) que nous avons déduit cette vérité pour un module premier : mais cette proposition n'a lieu que pour les modules premiers, et partant ne peut s'appliquer à ce cas. Nous allons donc la démontrer par une méthode particulière, et plus bas (sect. VIII) nous le prouverons encore plus facilement.

85. Nous nous proposons de démontrer ce théorème: *Si le plus grand commun diviseur des nombres* t *et* $p^{n-1}(p-1)$ *est* e, *la congruence* $x^t\equiv 1 \pmod{p^n}$ *aura* e *racines différentes.*

Soit $e=kp^\nu$, desorte que k ne renferme point le facteur p, et qu'il divise parconséquent $p-1$. Alors la congruence $x^t\equiv 1$ suivant le module p, aura k racines différentes, et si on les désigne par $A, B, C,$ etc., une racine quelconque de cette même congruence, suivant le module p^n, devra être congrue à quelqu'un des nombres $A, B, C,$ etc., suivant le module p. Or nous démontrerons que la congruence $x^t\equiv 1 \pmod{p^n}$, a p^ν racines congrues à A, autant

à B, etc. suivant le module p, d'où il résultera que le nombre de toutes les racines sera kp^{ν} ou e, comme nous l'avons avancé. Cela posé, nous allons démontrer que

1°. Si α est une racine congrue à A, suivant le module p, $\alpha+p^{n-\nu}$, $\alpha+2p^{n-\nu}$, $\alpha+3p^{n-\nu}\ldots\alpha+p^{\nu-1}.p^{n-\nu}$, seront aussi des racines.

2°. Aucun nombre congru avec A ne pourra être racine, s'il n'est de la forme $\alpha+hp^{n-\nu}$, h étant un nombre entier quelconque; d'où il suit qu'on aura p^{ν} racines différentes, et qu'on n'en aura pas davantage; la même chose aura lieu par rapport à B, C, etc.

3°. Nous ferons voir comment on peut toujours trouver une racine congrue à A suivant le module p.

86. Théorème. *Si* t *est comme dans l'article précédent un nombre divisible par* p^{ν} *et non par* $p^{\nu+1}$, *on aura* $(\alpha+hp^{\mu})^t-\alpha^t\equiv 0 \pmod{p^{\mu+\nu}}$, et $\equiv \alpha^{t-1}hp^{\mu}t \pmod{p^{\mu+\nu+1}}$. La seconde partie du théorème n'a pas lieu quand $p=2$ et $\mu=1$.

On pourrait déduire la démonstration de ce théorème du développement de la puissance d'un binome, si on faisait voir que tous les termes, après le second, sont divisibles par $p^{\mu+\nu+1}$; mais comme la considération des dénominateurs des coefficiens jette dans quelque embarras, nous préférons la méthode suivante:

Supposons d'abord $\mu>1$ et $\nu=1$, on a généralement $x^t-y^t=(x-y)(x^{t-1}+x^{t-2}y+x^{t-3}y^2+\ldots+y^{t-1})$; donc..... $(\alpha+hp^{\mu})^t-\alpha^t=hp^{\mu}\{(\alpha+hp^{\mu})^{t-1}+(\alpha+hp^{\mu})^{t-2}\alpha+\text{etc.}+\alpha^{t-1}\}$; mais on a $\alpha+hp^{\mu}\equiv\alpha \pmod{p^2}$; donc chaque terme $(\alpha+hp^{\mu})^{t-1}$, $(\alpha+hp^{\mu})^{t-2}\alpha$, etc. sera $\equiv\alpha^{t-1} \pmod{p^2}$, et parconséquent la somme de tous $\equiv t\alpha^{t-1} \pmod{p^2}$, ou bien cette somme sera de la forme $t\alpha^{t-1}+Vp^2$, V étant un nombre quelconque. Donc $(\alpha+hp^{\mu})^t-\alpha^t$ sera de la forme $\alpha^{t-1}hp^{\mu}t+Vhp^{\mu+2}$, c'est-à-dire qu'il sera $\equiv\alpha^{t-1}hp^{\mu}t \pmod{p^{\mu+2}}$ et $\equiv 0 \pmod{p^{\mu+1}}$. Ainsi, pour ce cas, le théorème est démontré.

Or si le théorème n'était pas vrai pour les autres valeurs de ν, μ restant >1, il y aurait nécessairement une limite jusqu'à laquelle le théorème serait vrai, et passé laquelle il serait faux. Soit φ la plus petite valeur de ν qui se refuse au théorème. On voit facilement que le théorème est vrai si t est divisible par $p^{\varphi-1}$ et non par p^{φ}; mais que si l'on substitue tp à la place de t, il ne l'est plus. On a donc $(\alpha+hp^{\mu})^t \equiv \alpha^t + \alpha^{t-1}hp^{\mu}t \pmod{p^{\mu+\varphi}}$, ou $= \alpha^t + \alpha^{t-1}hp^{\mu}t + up^{\mu+\varphi}$, u étant un nombre entier quelconque; mais comme le théorème est déjà démontré pour $\nu=1$, on aura $(\alpha^t + \alpha^{t-1}hp^{\mu}t + up^{\mu+\varphi})^p \equiv \alpha^{tp} + \alpha^{tp-1}hp^{\mu+1}t + \alpha^{tp-1}up^{\mu+\varphi+1} \pmod{p^{\mu+\varphi+1}}$, et partant $(\alpha+hp^{\mu})^{tp} \equiv \alpha^{tp} + \alpha^{tp-1}hp^{\mu}tp \pmod{p^{\mu+\varphi+1}}$; c'est-à-dire que le théorème est encore vrai si on substitue tp au lieu de t ou $\varphi+1$ au lieu de φ, contre l'hypothèse; donc le théorème est vrai pour toutes les valeurs de ν.

87. Il reste le cas où $\mu=1$. Par une méthode absolument semblable à celle de l'article précédent, on démontrera, sans faire usage du développement du binome, que

$$(\alpha+hp)^{t-1} \equiv \alpha^{t-1} + \alpha^{t-2}(t-1)hp \pmod{p^2}$$
$$\alpha(\alpha+hp)^{t-2} \equiv \alpha^{t-1} + \alpha^{t-2}(t-2)hp \pmod{p^2}$$
$$\alpha^2(\alpha+hp)^{t-3} \equiv \alpha^{t-1} + \alpha^{t-2}(t-3)hp \pmod{p^2}, \text{ etc;}$$

donc (puisque le nombre des termes est t) la somme sera $\equiv t\alpha^{t-1} + \frac{(t-1)t}{2}\alpha^{t-2}hp \pmod{p^2}$; mais, comme t est divisible par p, $\frac{(t-1)t}{2}$ le sera aussi, excepté le cas où $p=2$; que nous avons exclu, et dans les autres cas, la somme sera $\equiv t\alpha^{t-1} \pmod{p^2}$, puisque $\frac{(t-1)t}{2}\alpha^{t-2}hp$ est divisible par p^2. Le reste de la démonstration est comme dans l'article précédent.

Il résulte de là généralement qu'en exceptant le cas où $p=2$, on a $(\alpha+hp^{\mu})^t \equiv \alpha^t \pmod{p^{\mu+\nu}}$ et $(\alpha+hp^{\mu})$ *non* $\equiv \alpha^t$ pour un module qui est une puissance de p plus haute que $p^{\mu+\nu}$, pourvu toutefois

que h ne soit pas divisible par p, et que p^{ν} soit la plus haute puissance de p qui divise t.

De là suivent sur-le-champ les deux premières propositions que nous nous étions proposé de démontrer (n° 85), savoir:

1°. Si $\alpha^t \equiv 1$, on aura aussi $(\alpha + hp^{n-\nu})^t \equiv 1 \pmod{p^n}$.

2°. Si un nombre α' congru à A et partant à α, suivant le module p, mais incongru à α, suivant le module $p^{n-\nu}$, satisfesait à la congruence $x^t \equiv 1 \pmod{p^n}$, supposons $\alpha' = \alpha + lp^{\lambda}$, desorte que l ne soit pas divisible par p, on aura $\lambda < n-\nu$; alors $(\alpha + lp^{\lambda})^t \equiv \alpha^t \pmod{p^{\lambda+\nu}}$ et non suivant p^n, qui est une puissance de p plus haute que $p^{\lambda+\nu}$; donc α' ne peut être racine de la congruence $x^t \equiv 1$.

88. Nous devions en troisième lieu trouver une racine de la congruence $x^t \equiv 1 \pmod{p^n}$, qui fut congrue à A. Il nous suffira de faire voir ici comment on peut y parvenir, si l'on connaît une racine de la congruence suivant le module p^{n-1}, puisque l'on pourra passer du module p, pour lequel A est racine, au module p^2, et de là à toutes les puissances consécutives.

Soit donc α une racine de la congruence $x^t \equiv 1 \pmod{p^{n-1}}$ et que l'on cherche une racine de la même congruence suivant le module p^n, nous la supposerons $= \alpha + hp^{n-\nu-1}$, forme qu'elle doit avoir d'après l'article précédent: nous considérerons à part le cas où $\nu = n-1$, et ν ne peut-être $> n-1$. On aura donc $(\alpha + hp^{n-\nu-1})^t \equiv 1 \pmod{p^n}$; mais $(\alpha + hp^{n-\nu-1})^t \equiv \alpha^t + \alpha^{t-1} htp^{n-\nu-1} \pmod{p^n}$; si donc on détermine h de manière qu'on ait $1 \equiv \alpha^t + \alpha^{t-1} htp^{n-\nu-1} \pmod{p^n}$; ou, comme par hypothèse $1 \equiv \alpha^t \pmod{p^{n-1}}$ et que t est divisible par p^{ν}, de manière qu'on ait $\frac{\alpha^t - 1}{p^{n-1}} + \alpha^{t-1} h \frac{t}{p^{\nu}}$ divisible par p, le problême sera résolu; or il est prouvé, dans la section précédente, que cela est toujours possible, puisque t ne peut être divisé par une puissance de p plus haute que p^{ν}, et que partant $\alpha^{t-1} \frac{t}{p}$ est premier avec p.

Mais

Mais si $\nu = n-1$, c'est-à-dire si t est divisible par p^{n-1} ou par une plus haute puissance de p, toute valeur A qui satisfera à la congruence $x^t \equiv 1$, suivant le module p, y satisfera aussi suivant le module p^n. Soit en effet $t = p^{n-1}\tau$, on aura $t \equiv \tau \pmod{p-1}$; donc puisque $A^t \equiv 1 \pmod{p}$, on aura aussi $A^\tau \equiv 1 \pmod{p}$. Soit donc $A^\tau = 1 + hp$, on aura $A^t = (1+hp)^{p^{n-1}} \equiv 1 \pmod{p^n}$, (n° 87).

89. Tout ce que nous avons démontré (n°s 57 et suivans) à l'aide du théorème du n° 43, a lieu pour un module qui est une puissance d'un nombre premier, et si l'on appelle *racines primitives* les nombres qui appartiennent à l'exposant $p^{n-1}(p-1)$, c'est-à-dire ceux dans la période desquels se trouvent tous les nombres non divisibles par p, il y aura également ici des racines primitives; tout ce que nous avons dit des indices et de leur usage, ainsi que de la résolution de la congruence $x^t \equiv 1$, peut s'appliquer à ce cas: comme toutes les démonstrations n'ont aucune difficulté, il serait superflu de les répéter. Nous avons en outre fait voir comment on déduit des racines de la congruence $x^t \equiv 1 \pmod{p}$, celles de la congruence $x^t \equiv 1 \pmod{p^n}$; mais il faut ajouter quelque chose sur le cas où $p = 2$, que nous avions exclu dans ce qui précède.

90. *Si l'on prend pour module une puissance de 2 plus haute que la seconde, 2^n par exemple, la puissance 2^{n-2} de tout nombre impair sera* $\equiv 1$.

Par exemple, $3^8 = 6561 \equiv 1 \pmod{32}$.

En effet tout nombre impair est de la forme $1+4h$ ou de celle-ci $-1+4h$, d'où la proposition suit immédiatement (86).

Ainsi l'exposant auquel appartient un nombre impair quelconque suivant le module 2^n, doit être un diviseur de 2^{n-2}; ce nombre appartiendra donc à l'un des suivans $1, 2, 4, 8, \ldots . 2^{n-2}$; et d'ailleurs on jugera facilement auquel il appartient. Soit le nombre proposé $= 4h \pm 1$, et 2^m la plus haute puissance de 2 qui puisse diviser h (m est $= 0$ quand h est impair). Alors l'exposant auquel appartient le nombre donné sera $= 2^{n-m-2}$, si $n > m+2$; mais si $n =$ ou $< m+2$, le nombre proposé sera $\equiv \pm 1$, et partant appartiendra à l'exposant 1 ou à l'exposant 2. En effet $4h \pm 1 = \pm 1 + 2^{m+2}k$, et ce nombre élevé à la puissance 2^{n-m-2} devient congru à l'unité suivant le mo-

dule p^n; or on déduit sans peine du n° 86 que si on élevait ce nombre à une puissance de degré moindre, le résultat serait incongru à l'unité. Ainsi tout nombre de la forme $\pm 1 + 4h$, où h est impair, c'est-à-dire tout nombre de la forme $8k+3$ ou $8k+5$, appartient à l'exposant p^{n-2}.

91. Il suit de là qu'il n'y a pas dans ce cas-ci de *racines primitives*, dans le sens que nous avons donné à cette expression, c'est-à-dire qu'il n'y a pas de nombres dont la période renferme tous les nombres premiers avec le module, et plus petits que lui; mais on voit facilement qu'il arrive ici quelque chose d'analogue. En effet toute puissance impaire d'un nombre de la forme $8k+3$ est elle-même de la forme $8k+3$, et toute puissance paire est de la forme $8k+1$; donc aucune ne peut être de la forme $8k+5$ ou $8k+7$; donc comme la période d'un nombre de la forme $8k+3$ est composée de 2^{n-2} termes différens, dont chacun est de la forme $8k+1$ ou $8k+3$, et qu'il n'y a pas plus de 2^{n-2} de ces nombres qui soient plus petits que le module, il est évident que tout nombre de la forme $8k+1$ ou $8k+3$ est congru suivant le module 2^n, à une puissance d'un nombre quelconque de la forme $8k+3$. On peut faire voir de la même manière que la période d'un nombre de la forme $8k+5$ comprend tous les nombres de la forme $8k+1$ et $8k+5$. Si donc on prend pour base un nombre de la forme $8k+5$, on trouvera des indices réels pour tous les nombres de la forme $8k+1$ et $8k+5$ pris positivement, et pour tous les nombres de la forme $8k+3$ et $8k+7$ pris négativement : on doit encore regarder comme équivalens les indices congrus suivant 2^{n-2}. C'est ainsi qu'on doit entendre la table I, dans laquelle pour les modules 16, 32 et 64 (car il n'y a besoin d'aucune table pour le module 8), nous avons toujours pris 5 pour base. Par exemple, le nombre 19, qui doit être pris négativement, puisqu'il est de la forme $8n+3$, a pour le module 64 l'indice 7, ce qui signifie que $5^7 \equiv -19 \pmod{64}$. Si l'on prenait négativement les nombres de la forme $8n+1$ et $8n+5$, et positivement ceux de la forme $8n+3$ et $8n+7$, il faudrait leur donner des indices pour ainsi dire imaginaires; en les introduisant dans le calcul des indices, on le réduirait à un algorithme très-simple; mais comme nous serions conduits trop loin si nous voulions traiter ce sujet en toute rigueur, nous réservons

ce point pour une autre occasion, quand peut-être nous entreprendrons de traiter plus en détail la théorie des quantités imaginaires, qui nous semble jusqu'à présent n'avoir été réduite par personne à des notions claires. Les gens instruits parviendront aisément à cet algorithme; ceux qui sont moins exercés pourront néanmoins se servir de cette table, comme ceux qui ne sont point au fait des connaissances modernes sur les logarithmes imaginaires se servent des logarithmes, pourvu qu'ils possèdent bien les principes antérieurement établis.

92. Presque tout ce qui a rapport aux résidus des puissances, suivant un module composé de plusieurs nombres premiers, peut se déduire de la théorie générale des congruences; mais comme nous exposerons plus bas une manière de ramener les congruences dont le module est composé de plusieurs nombres premiers, à d'autres dont le module est un nombre premier, ou une puissance d'un nombre premier, nous ne nous arrêterons pas beaucoup ici sur cette matière. Nous nous contenterons d'observer que la belle propriété qui a lieu pour les autres modules, savoir: qu'il existe toujours des nombres dont la période renferme tous les nombres premiers avec le module, n'a pas lieu ici, excepté dans le seul cas où le module est double d'un nombre premier, ou d'une puissance d'un nombre premier. En effet si l'on ramène le module m à la forme $A^a B^b C^c$ etc., A, B, C, etc. étant des nombres premiers différens, qu'on fasse en outre $A^{a-1}(A-1)=\alpha$, $B^{b-1}(B-1)=\beta$, $C^{c-1}(C-1)=\gamma$, etc. et que z soit un nombre premier avec m, on aura $z^{\alpha}\equiv 1 \pmod{A^a}$, $z^{\beta}\equiv 1 \pmod{B^b}$, etc.; si donc μ est le plus petit nombre divisible par α, β, γ, etc., on aura $z^{\mu}\equiv 1$ suivant chacun des modules A^a, B^b, etc., et partant, suivant m qui est égal à leur produit; mais excepté le cas où m est double d'un nombre premier ou d'une puissance d'un nombre premier, on a toujours $\mu < \alpha\beta\gamma$ etc., puisque les nombres α, β, etc. ne peuvent être premiers entre eux, ayant au moins le diviseur commun 2. Ainsi la période d'aucun nombre ne peut comprendre autant de termes qu'il y a de nombres premiers avec le module, et moindres que lui, puisque leur nombre est égal au produit $\alpha\beta\gamma$ etc. Ainsi, par exemple, pour $m=1001=7.11.13$, la puissance

60 d'un nombre quelconque premier avec m, est congrue à l'unité, puisque 60 est le plus petit nombre divisible à-la-fois par 6, 10 et 12. Le cas où le module est double d'un nombre premier ou d'une puissance d'un nombre premier, est tout-à-fait semblable à celui où le module est un nombre premier ou une puissance d'un nombre premier.

93. Nous avons déjà cité en plusieurs endroits les ouvrages dans lesquels les autres géomètres ont parlé du sujet que nous avons traité dans cette section-ci; mais nous renvoyons ceux qui voudraient avoir plus de détails que le desir d'abréger ne nous a permis d'en donner, aux ouvrages suivans d'Euler, recommandables par la perspicacité qui a toujours distingué ce grand homme.

Theoremata circa residua ex divisione potestatum relicta (Comm. nov. Petrop. T. VII, p. 49).

Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia. (Ibid. T. XVIII, p. 85).

On peut y joindre les dissertations 5 et 8 des *Opuscula analytica*. T. I.

SECTION QUATRIÈME.

Des Congruences du second degré.

94. THÉORÈME. *Un nombre quelconque* m *étant pris pour module, il ne peut y avoir dans la suite* $1, 2, 3 \ldots m-1$, *plus de* $\frac{1}{2}m+1$ *nombres, quand* m *est pair, et plus de* $\frac{1}{2}m+\frac{1}{2}$, *quand* m *est impair, qui soient congrus à un quarré.*

Comme les quarrés des nombres congrus sont congrus entre eux, un nombre qui peut être congru à un quarré, le sera à un autre quarré, dont la racine est plus petite que m. Il suffit donc de considérer les résidus *minima* des quarrés $0, 1, 4, 9 \ldots \overline{m-1}^2$; mais on voit facilement qu'on a $(m-1)^2 \equiv 1$, $(m-2)^2 \equiv 2^2$, $(m-3)^2 \equiv 3^2$, etc. Donc aussi, quand m est pair, les quarrés $\left(\frac{m}{2}-1\right)^2$ et $\left(\frac{m}{2}+1\right)^2$, $\left(\frac{m}{2}-2\right)^2$ et $\left(\frac{m}{2}+2\right)^2$, etc., auront les mêmes résidus *minima*; et quand m est impair, $\left(\frac{m-1}{2}\right)^2$ et $\left(\frac{m+1}{2}\right)^2$, $\left(\frac{m-3}{2}\right)^2$ et $\left(\frac{m+3}{2}\right)^2$, etc. seront congrus. D'où il suit évidemment qu'il n'y a pas d'autres nombres congrus à un quarré que ceux qui le sont à l'un des quarrés : $0, 1, 4, 9, \ldots \left(\frac{m}{2}\right)^2$, quand m est pair; et que quand m est impair, il n'y en a pas d'autres que ceux qui sont congrus à l'un des quarrés $0, 1, 4, 9 \ldots \left(\frac{m-1}{2}\right)^2$ Donc il y aura au plus $\frac{m}{2}+1$ résidus *minima*, différens dans le premier cas, et $\frac{m+1}{2}$ dans le second.

Exemple. Suivant le module 13, les résidus *minima* des quarrés des nombres $0, 1, 2, 3, \ldots 6$, sont $0, 1, 4, 9, 3, 12, 10$, et après

cela ils reviennent dans l'ordre inverse 10, 12, 3, etc. Ainsi un nombre qui n'est pas congru avec l'un de ceux-là, ou qui l'est à l'un des nombres 2, 5, 6, 7, 8, 11, ne peut être congru à aucun quarré.

Suivant le module 15, on trouve pour résidus *minima* 0, 1, 4, 9, 1, 10, 6, 4, qui reviennent ensuite dans l'ordre inverse; ainsi le nombre des résidus qui peuvent être congrus à un quarré, est ici moindre que $\frac{m+1}{2}$, puisqu'ils sont 0, 1, 4, 6, 9, 10. Les nombres 2, 3, 5, 7, 8, 11, 12, 13, 14, et ceux qui leur sont congrus, ne peuvent être congrus à aucun quarré.

95. Il résulte de là que pour un module quelconque, tous les nombres peuvent se distinguer en deux classes, dont l'une renferme tous ceux qui peuvent être congrus à un quarré, et l'autre tous ceux qui ne le peuvent pas. Nous appellerons les premiers *résidus quadratiques* (*) du nombre que nous prenons pour module, et les derniers *non-résidus quadratiques*; ou même plus simplement toutes les fois qu'il n'en résultera pas d'ambiguité, *résidus* et *non-résidus*. Au reste il est évident qu'il suffit de classer les nombres $0, 1, 2 \ldots m-1$: car les nombres congrus doivent être rapportés à la même classe.

Nous commencerons aussi dans ces Recherches par les modules premiers, ce qui doit toujours être sous-entendu, quand nous n'en avertirons pas expressément. Mais il faut exclure le nombre 2, ou ne considérer que des nombres impairs.

96. *Le nombre premier* p *étant pris pour module, la moitié des nombres* $1, 2, 3 \ldots p-1$, *sera composée de résidus quadratiques, et l'autre moitié de non-résidus, c'est-à-dire qu'il y aura* $\frac{1}{2}(p-1)$ *résidus, et autant de non-résidus.*

(*) Dans ce cas-ci, nous donnons à ces expressions un sens un peu différent de celui qu'elles ont eu jusqu'à présent, car lorsque $r \equiv a^2 \pmod{m}$, il faudrait dire que r est résidu du quarré a^2, suivant le module m; mais pour abréger, nous appellerons dans cette section r, résidu quadratique de m, et il n'y a pas d'ambiguité à craindre, car nous n'emploîrons plus dorénavant l'expression *résidu*, quand elle signifiera un nombre congru, à moins qu'il ne soit question de résidus *minima*, et dans ce cas il n'y aura pas d'obscurité.

On prouve facilement que tous les quarrés $1, 4, 9, \ldots \left(\frac{p-1}{2}\right)^2$ sont incongrus; car si l'on pouvait avoir $r^2 \equiv r'^2 \pmod{p}$ et que les nombres r et r' fussent inégaux et $< \frac{p-1}{2}$, soit $r > r'$, on aurait $(r-r')(r+r')$, divisible par p; mais chaque facteur étant $< p$, la supposition ne peut subsister (n° 13). Il y a donc $\frac{p-1}{2}$, résidus quadratiques entre les nombres $1, 2, 3 \ldots p-1$; il ne peut y en avoir davantage, car en y joignant 0, le nombre en devient $\frac{1}{2}(p+1)$, limite qu'il ne peut pas dépasser. Donc les autres nombres seront non-résidus, et il y en aura $\frac{p-1}{2}$.

Comme zéro est toujours résidu, nous l'excluons, ainsi que les nombres divisibles par le module, parceque ce cas est clair par lui-même, et ne pourrait que nuire à l'élégance des théorèmes; par la même raison nous excluons aussi le nombre 2.

97. Comme la plupart des choses que nous exposerons dans cette section peuvent être déduites des principes exposés dans la section première, et comme il n'est pas inutile de rechercher la vérité par différentes voies; nous nous attacherons à faire voir la liaison des différentes méthodes. Par exemple, il est aisé de voir que tous les nombres congrus à un quarré ont des indices pairs, et que ceux qui ne sont congrus à aucun quarré ont des indices impairs. Mais puisque $p-1$ est un nombre pair, il y aura autant d'indices pairs qu'il y en a d'impairs, savoir: $\frac{1}{2}(p-1)$; parconséquent il y aura autant de résidus que de non-résidus.

Exemples.

Pour les modules	on a les résidus
3	1
5	1, 4
7	1, 2, 4
11	1, 3, 4, 5, 9
13	1, 3, 4, 9, 10, 12
17	1, 2, 4, 8, 9, 13, 15, 16,

etc.

et les autres nombres moindres que ces modules sont non-résidus.

98. THEORÈME. *Le produit de deux résidus quadratiques d'un nombre premier* p *est un résidu; le produit d'un résidu et d'un non-résidu est non-résidu; enfin le produit de deux non-résidus est résidu.*

1°. Soient A et B les résidus qui proviennent des quarrés a^2, b^2, ou soient $A \equiv a^2 \pmod{p}$ et $B \equiv b^2$, on aura $AB \equiv a^2 b^2$, c'est-à-dire qu'il sera un résidu.

2°. Quand A est résidu, ou que $A \equiv a^2$, mais que B est non-résidu, AB est non-résidu. Soit en effet, s'il se peut $AB \equiv k^2$ et $\frac{k}{a} \pmod{p} \equiv b$, on aura $a^2 B \equiv a^2 b^2$, et partant $B \equiv b^2$, contre l'hypothèse.

Autrement. Si l'on multiplie par A les $\frac{p-1}{2}$ nombres de la suite $1, 2, 3 \ldots p-1$, qui sont résidus, tous les produits seront des résidus quadratiques, et ils seront tous incongrus. Or si l'on multiplie par A un nombre B non-résidu, le produit ne sera congru à aucun des précédens: donc, s'il était résidu, il y aurait $\frac{1}{2}(p+1)$ résidus incongrus, parmi lesquels ne serait pas 0, ce qui est impossible (n° 96).

3°. Soient A et B deux nombres non-résidus, en multipliant par A tous les nombres qui sont résidus dans la suite $1, 2, 3, \ldots p-1$, on aura $\frac{p-1}{2}$ non-résidus incongrus entr'eux (2°). Or le produit AB ne peut être congru à aucun de ceux-là; donc s'il était non-résidu, on aurait $\frac{p+1}{2}$ non-résidus incongrus entr'eux; ce qui est impossible (n° 96).

Ces théorèmes se déduisent encore plus facilement des principes de la section précédente. En effet, puisque l'indice d'un résidu est toujours pair, et celui d'un non-résidu toujours impair, l'indice du produit de deux résidus ou non-résidus sera pair, et partant, le produit sera lui-même un résidu. Au contraire, si l'un des facteurs est non-résidu, et l'autre résidu, l'indice sera impair, et le produit non-résidu.

On

On peut aussi faire usage des deux méthodes pour démontrer ce théorème : *la valeur de l'expression* $\frac{a}{b}$ (*mod.* p), *sera un résidu*, quand *les nombres* a *et* b *seront tous les deux résidus ou non-résidus. Elle sera un non-résidu, quand l'un des nombres* a *et* b *sera résidu et l'autre non-résidu.* On le démontrerait encore en renversant les théorèmes précédens.

99. Généralement, le produit de tant de facteurs qu'on voudra est un résidu, soit lorsque tous les facteurs en sont eux-mêmes, soit lorsque le nombre de facteurs non-résidus est pair; mais quand le nombre des facteurs non-résidus est impair, le produit est non-résidu. On peut donc juger facilement si un nombre composé est résidu ou non; pourvu qu'on sache ce que sont ses différens facteurs. Aussi dans la table II, nous n'avons admis que les nombres premiers. Quant à sa disposition, les modules sont en marge (*), en tête les nombres premiers successifs; quand l'un de ces derniers est résidu, on a placé un trait dans l'espace qui correspond au module et à ce nombre; quand il est non-résidu, on a laissé l'espace vide.

100. Avant de passer à des sujets plus difficiles, nous devons dire un mot des modules composés.

Si l'on prend pour module la puissance p^n d'un nombre premier p, p étant > 2, une moitié des nombres non-divisible par p et $< p^n$ seront des résidus, et l'autre des non-résidus; c'est-à-dire qu'il y en aura $\frac{p-1}{2} . p^{n-1}$ de chaque espèce.

En effet, si r est un résidu, il sera congru à un quarré dont la racine ne surpasse pas la moitié du module (n° 94); et l'on voit facilement qu'il y a $\frac{1}{2} p^{n-1} (p-1)$ nombres $< \frac{p^n}{2}$ et non divisible par p. Ainsi il reste à démontrer que les quarrés de tous ces nombres sont incongrus, ou qu'ils donnent des résidus différens. Or si deux nombres a et b non-divisibles par p et plus petits que la moitié du module, avaient leurs quarrés congrus, on

(*) On verra bientôt comment on peut se passer des modules composés.

aurait $a^2 - b^2$ ou $(a+b)(a-b)$ divisible par p^n, en supposant $a > b$, ce qui est permis. Mais cette condition ne peut avoir lieu, à moins que l'un des deux nombres $a-b$, $a+b$ ne soit divisible par p^n, ce qui est impossible, puisque chacun d'eux est plus petit que p^n, ou bien que l'un étant divisible par p^μ, l'autre le soit par $p^{n-\mu}$ ou chacun d'eux par p; ce qui est encore impossible, puisqu'il s'ensuivrait que la somme $2a$ et la différence $2b$, et partant a et b eux-mêmes seraient divisibles par p, contre l'hypothèse. Donc enfin parmi les nombres non-divisibles par p, et moindres que le module, il y a $\frac{p-1}{2} p^{n-1}$ résidus, et les autres, en même nombre, sont non-résidus.

Ce théorème peut se déduire aussi de la considération des indices, comme au n° 97.

101. *Tout nombre non-divisible par* p, *qui est résidu de* p, *sera aussi résidu de* p^n; *celui qui ne sera pas résidu de* p *ne le sera pas non plus de* p^n.

La seconde partie de cette proposition est évidente par elle-même; ainsi si la première n'était pas vraie, parmi les nombres plus petits que p^n et non-divisibles par p, il y en aurait plus qui fussent résidus de p qu'il n'y en aurait qui le fussent de p^n, c'est-à-dire plus de $\frac{1}{2} p^{n-1}(p-1)$. Mais on peut voir sans peine que le nombre des résidus de p qui se trouvent entre 1 et p^n, est précisément $= \frac{1}{2} p^{n-1}(p-1)$.

Il est tout aussi facile de trouver effectivement un quarré qui soit congru à un résidu donné, suivant le module p^n, si l'on connaît un quarré congru à ce résidu suivant le module p.

Soit en effet a^2 un quarré congru au résidu donné A, suivant le module p^μ, on en déduira, de la manière suivante, un quarré $\equiv A$, suivant le module p^ν, ν étant $> \mu$ et non plus grand que 2μ. Supposons que la racine du quarré cherché soit $\pm a + xp^\mu$; et il est aisé de s'assurer que c'est là la forme qu'elle doit avoir. Il faut donc qu'on ait $a^2 \pm 2axp^\mu + x^2 p^{2\mu} \equiv A \pmod{p^\nu}$, ou comme $2\mu \geq \nu$, on aura,

$\pm 2axp^{\mu} \equiv A - a^2 \pmod{p^{\nu}}$. Soit $A - a^2 = p^{\mu}.d$, on aura $\pm 2ax \equiv d \pmod{p^{\nu-\mu}}$; donc x sera la valeur de l'expression $\pm\frac{d}{2a} \pmod{p^{\nu-\mu}}$.

Ainsi étant donné un quarré congru à A, suivant le module p, on en déduira un quarré congru à A, suivant le module p^2; de là au module p^4, au module p^8, etc.

Exemple. Etant proposé le résidu 6 congru au quarré 1, suivant le module 5, on trouve le quarré 9^2 auquel il est congru suivant le module 25, 16^2 auquel il est congru suivant le module 125, etc.

102. Quant à ce qui regarde les nombres divisibles par p, il est clair que leurs quarrés seront divisibles par p^2, et que partant tous les nombres qui seront divisibles par p et non par p^2, seront non-résidus de p^n. Et en général, si l'on propose le nombre $p^k A$, A n'étant pas divisible par p, il y a trois cas à distinguer:

1°. Si $k =$ ou $> n$, on aura $p^k A \equiv 0 \pmod{p^n}$, c'est-à-dire qu'il sera résidu.

2°. Si $k < n$ et impair, $p^k A$ sera non-résidu.

En effet, si l'on avait $p^k A = p^{2k'+1} A \equiv s^2 \pmod{p^n}$, s^2 serait divisible par $p^{2k'+1}$, ce qui ne peut avoir lieu, à moins que s ne le soit par $p^{k'+1}$; donc alors s^2 serait aussi divisible par $p^{2k'+2}$, ce qui conduirait, à cause de $2k'+2$ non plus grand que n, à $p^k A$ aussi divisible par $p^{2k'+2}$; ce qui supposerait A divisible par p, contre l'hypothèse.

3°. Si $k < n$ et pair, $p^k A$ sera résidu ou non-résidu de p^n, suivant que A sera résidu ou non-résidu de p. En effet, quand A sera résidu de p, il le sera aussi de p^{n-k} (n° précédent). Mais si l'on suppose $A \equiv a^2 \pmod{p^{n-k}}$, on aura $Ap^k \equiv a^2 p^k \pmod{p^n}$; or $a^2 p^k$ est un quarré. Quand au contraire A est non-résidu de p, $p^k A$ ne peut être résidu de p^n. Supposons en effet $p^k A \equiv a^2 \pmod{p^n}$, a^2 serait nécessairement divisible par p^k, et le quotient serait un quarré auquel A serait congru, suivant le module $p-k$, et par-conséquent suivant le module p, c'est-à-dire, que A serait résidu de p, contre l'hypothèse.

103. Comme nous avons commencé (n° 100) par exclure le cas où $p=2$, il faut ajouter quelque chose à ce sujet. Quand 2 est module, tous les nombres sont résidus, et il n'y en a point de non-résidus. Quand le module est 4, tous les nombres impairs de la forme $4k+1$ sont résidus, et tous ceux de la forme $4k+3$ sont non-résidus. Enfin, quand le module est 8 ou une plus haute puissance de 2, tous les nombres impairs de la forme $8k+1$ sont résidus, et les autres, ou ceux qui sont de la forme $8k+3$, $8k+5$, $8k+7$ sont non-résidus; la dernière partie de cette proposition est évidente, puisque le quarré d'un nombre impair de la forme $4k+1$ ou $4k-1$ est toujours de la forme $8k+1$. On peut démontrer la première comme il suit.

1°. Si la somme ou la différence de deux nombres est divisible par 2^{n-1}, les quarrés de ces nombres seront congrus suivant le module 2^n. En effet, soit a un de ces nombres, l'autre sera $2^{n-1}h\pm a$, dont le quarré est $\equiv a^2 \pmod{2^n}$.

2°. Tout nombre impair qui est résidu quadratique de 2^n, est congru à un quarré dont la racine est un nombre impair et $<2^{n-2}$. Soit en effet a^2 un quarré quelconque, auquel ce nombre soit congru, et $\alpha\equiv a \pmod{2^{n-1}}$, α n'étant pas plus grand que la moitié du module (n° 4), on aura $a^2\equiv\alpha^2$, et partant le nombre proposé sera $\equiv\alpha^2$. Mais il est évident que a et α seront impairs, et que parconséquent $a<2^{n-2}$.

3°. Les quarrés de tous les nombres impairs moindres que 2^{n-2} seront incongrus, suivant le module 2^n. Soient en effet deux nombres r et s, deux nombres impairs moindres que 2^{n-2}; si leurs quarrés étaient congrus suivant 2^n, on aurait $(r-s)(r+s)$ divisibles par 2^n. r étant $>s$; mais on voit aisément que $r+s$ et $r-s$ ne peuvent être à-la-fois divisibles par 4, et si l'un est seulement divisible par 2, l'autre doit l'être par 2^{n-1}, ce qui est absurde, puisque chacun d'eux est $<2^{n-2}$.

4°. Si l'on ramène ces quarrés à leurs *résidus minima positifs*, on aura 2^{n-3}, résidus quadratiques différens, et plus petits que le module; mais comme il y a précisément 2^{n-3}, nombres de la forme $8k+1$ plus petits que le module, nécessairement tous ces nombres se trouveront parmi les résidus.

Pour trouver un quarré congru à un nombre donné de la forme $8k+1$, suivant le module 2^n, on peut employer une méthode semblable à celle du n° 101, ou suivre le procédé du n° 88. Pour les nombres pairs, on peut faire usage de ce que nous avons dit généralement n° 102.

104. Pour ce qui regarde le nombre de valeurs différentes, c'est-à-dire incongrues suivant le module, que peut admettre l'expression $V = \sqrt{A} \pmod{p^n}$, pourvu que A soit un résidu de p^n, on déduit facilement de ce qui précède, les conclusions suivantes. Nous supposons toujours que p est un nombre premier et, pour abréger, nous considérons en même temps le cas où $n=1$.

1°. Si A n'est pas divisible par p, V n'a qu'une seule valeur pour $p=2$ et $n=1$; ce sera $V \equiv 1$; il en a deux quand p est impair, ou bien quand on a $p=2$ et $n=2$; et, si l'une est $\equiv v$, l'autre sera $\equiv -v$; il en a quatre pour $p=2$ et $n>2$; et si l'une est $\equiv v$, les autres seront $\equiv v+2^{n-1}$, $-v+2^{n-1}$, $-v$.

2°. Si A est divisible par p, mais non par p^n, soit $p^{2\mu}$ la plus haute puissance de p qui divise A, car cette puissance doit être paire (n° 102), et $A = ap^{2\mu}$; il est clair que toutes les valeurs de V doivent être divisibles par p^μ, et que tous les quotiens donnés par ces divisions seront les valeurs de l'expression $V' = \sqrt{a}. \pmod{p^{n-2\mu}}$; on aura donc toutes les valeurs différentes de V, en multipliant par p^μ, toutes celles de V' contenues entre 0 et $p^{n-\mu}$. Elles seront, par conséquent,

$$v p^\mu,\ v p^\mu + p^{n-\mu},\ v p^\mu + 2p^{n-\mu},\ \ldots\ldots v p^\mu + (p^\mu - 1)\, p^{n-\mu},$$

v étant une valeur quelconque de V': suivant donc que V' aura 1, ou 2, ou valeurs, V en aura p^μ, ou $2p^\mu$, ou $4p^\mu$ (1°.).

3°. Si A est divisible par p^n, on voit facilement, en posant $n=2m$ ou $=2m-1$, suivant que n est pair ou impair, que tous les nombres divisibles par p^m sont des valeurs de V, et qu'il n'y en a pas d'autres; mais les nombres divisibles par p^m sont $0, p^m, 2p^m \ldots (p^{n-m}-1)\, p^m$, dont le nombre est p^{n-m}.

105. Il reste à examiner le cas où le module m est composé de plusieurs nombres premiers. Soit $m = abc$ etc., a, b, c, etc. étant des nombres premiers différens, ou des puissances de nombres premiers différens. Il est clair d'abord que si n est résidu de m, il le sera aussi des différens nombres a, b, c, etc., et que partant il sera non-résidu de m, s'il est non-résidu de quelqu'un de ces nombres. Réciproquement, si n est résidu des différens nombres a, b, c, etc., il le sera de leur produit m; en effet, si l'on a $n \equiv A^2$, B^2, C^2, etc., suivant les modules a, b, c, etc. respectivement, et qu'on cherche un nombre N congru aux nombres A, B, C, etc., suivant les modules a, b, c, etc. respectivement (n° 32), on aura $n \equiv N^2$, suivant tous ces modules, et conséquemment suivant leur produit.

Comme on voit facilement que la valeur de N résulte de la combinaison d'une valeur quelconque de A, ou de l'expression $\sqrt{n}$. (mod. a), avec une valeur quelconque de B, avec une valeur quelconque de C, etc, que les différentes combinaisons donneront des valeurs différentes, et qu'elles les donneront toutes; le nombre des valeurs de N sera égal au produit des nombres de valeurs de A, B, C, etc. que nous avons appris à déterminer dans l'article précédent.

Il est évident que si l'on connaît une valeur de l'expression $\sqrt{n}$ (mod. m), ou de N, ce sera aussi une valeur de A, B, C, etc.; et comme par l'article précédent on peut en déduire toutes les autres valeurs de ces quantités, il s'ensuit que l'on pourra trouver toutes les valeurs de N, lorsqu'on en connaîtra une.

Exemple. Soit le module 315; on demande si 46 est un résidu ou un non-résidu. Les diviseurs premiers de 315 sont 3, 5, 7, et 46 est résidu de chacun d'eux; donc il est résidu de 315. Or comme $46 \equiv 1$ et $\equiv 64$ (mod. 9), $\equiv 1$ et $\equiv 16$ (mod. 5), $\equiv 4$ et $\equiv 25$ (mod. 7), on trouve pour les racines des quarrés congrus à 46 suivant le module 315, les nombres 19, 26, 44, 89, 226, 271, 289, 296.

106. On voit par ce qui précède, qu'il suffit de reconnaître si un nombre donné est résidu ou non-résidu d'un nombre premier donné, et que tous les cas reviennent à celui-là. Nous devons donc chercher pour ce cas des caractères certains; mais avant d'en-

freprendre cette recherche, nous présenterons un caractère qui se déduit de la section précédente, et qui est digne d'être conservé à cause de sa simplicité et de sa généralité, quoiqu'il ne soit presque d'aucune utilité dans la pratique.

Un nombre quelconque A, *non divisible par un nombre premier* $2m+1$, *est résidu ou non-résidu de ce nombre premier suivant que* $A^m \equiv +1$ *ou* $\equiv -1$ (*mod.* $2m+1$).

Soit en effet, pour le module $2m+1$, a l'indice du nombre A, dans un système quelconque, a sera pair quand A sera un résidu, et impair quand A sera non-résidu; mais l'indice du nombre A^m est ma, c'est-à-dire $\equiv 0$ ou $\equiv m$ (mod. $2m$) suivant que a est pair ou impair. Donc dans le premier cas on aura $A^m \equiv 1$ et dans le second $\equiv -1$ (mod. $2m+1$) (nos 57, 62).

Exemple. 3 est résidu de 13, parceque $3^6 \equiv 1$ (mod. 13); au contraire 2 n'est pas résidu de 13, parceque $2^6 \equiv -1$ (mod. 13); mais pour peu que les nombres à examiner soient grands, ce caractère devient tout-à-fait inutile à cause de l'immensité du calcul.

107. Il est très-facile d'assigner tous les nombres qui sont résidus ou non-résidus d'un nombre donné. Soit en effet m ce nombre; on déterminera les quarrés dont les racines ne surpassent pas $\frac{m}{2}$, ou des nombres congrus à ces quarrés suivant le module m (pour la pratique il y a encore des méthodes plus expéditives); alors tous les nombres congrus à quelqu'un de ceux-là, suivant le module m, seront résidus, et tous ceux qui ne seront congrus à aucun, seront non-résidus; mais la question inverse, *étant donné un nombre quelconque, assigner tous ceux dont il est résidu ou non-résidu*, est d'une bien plus grande difficulté; aussi nous allons nous occuper de ce problême, de la solution duquel dépend ce que nous nous sommes proposé dans l'article précédent; et nous commencerons par les cas les plus simples.

108. THÉORÈME. -1 *est résidu de tous les nombres premiers de la forme* $4n+1$, *et non-résidu de tous les nombres premiers de la forme* $4n+3$.

Exemple. -1 est résidu des nombres 5, 13, 17, 29, 37, 41, 53,

61, 73, 89, 97, etc.; il provient des quarrés des nombres 2, 5, 4, 12, 6, 9, 23, 11, 27, 34, 22, etc., respectivement. Il est au contraire non-résidu des nombres 3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83, etc.

Nous avons déjà fait mention de ce théorème (n° 64); mais on le démontre facilement par le n° 106. En effet, pour un nombre premier de la forme $4n+3$, on a $(-1)^{2n} \equiv +1$, et pour un nombre de la forme $4n+3$, on a $(-1)^{2n+1} \equiv -1$. Cette démonstration revient à celle du n° 64; mais à cause de l'élégance du théorème et de son utilité, il ne sera pas inutile de le démontrer encore d'une autre manière.

109. Désignons par C la somme de tous les résidus du nombre premier p; leur nombre, en excluant 0, est $\frac{p-1}{2}$, qui sera pair toutes les fois que p sera de la forme $4n+1$, et impair lorsque p sera de la forme $4n+3$. Par analogie avec la nomenclature adoptée dans le n° 77, dans lequel il était question de nombres en général, nous appellerons, *résidus associés*, ceux dont le produit sera $\equiv 1 \pmod{p}$; en effet il est évident que si r est un résidu, $\frac{1}{r} \pmod{p}$ en sera un aussi, et comme le même résidu ne peut avoir plusieurs associés dans C, il est clair que C peut être distribué en classes, dont chacune contiendra deux résidus associés. Or il est évident que, s'il n'y avait aucun résidu qui n'eût d'autre associé que lui-même, c'est-à-dire si chaque classe contenait deux résidus différens, le nombre des résidus serait double de celui des classes. Si donc il y a des nombres qui soient eux-mêmes leurs associés, c'est-à-dire quelques classes qui ne contiennent qu'un résidu, ou, si on aime mieux, qui contiennent deux fois le même; soit a le nombre de ces classes, b le nombre des autres, le nombre de tous les résidus sera $= a+2b$: donc a sera pair ou impair suivant que p sera de la forme $4n+1$ ou $4n+3$; mais (n° 77) il n'y a pas de nombres plus petits que p, autres que 1 et $p-1$ qui soient eux-mêmes leurs associés, et le premier 1 fait certainement partie des résidus; ainsi dans le premier cas $p-1$ ou, ce qui revient au même, -1 doit être résidu, et dans le second il doit être non-résidu; autrement dans le premier cas on aurait $a=1$, et dans le second $a=2$, ce qui est impossible.

110. Cette démonstration est encore due à *Euler*, ainsi que la précédente qu'il a donnée le premier (*Opusc. analyt. T. 1, p.* 135). Il est aisé de voir qu'elle repose sur des principes semblables à ceux sur lesquels nous avons appuyé notre seconde démonstration du théorème de *Wilson* (n° 77). Mais en supposant ce théorème, la démonstration précédente se simplifierait beaucoup. En effet, entre les nombres $1, 2, 3 \ldots p-1$, il y en a $\frac{p-1}{2}$ qui sont résidus et autant de non-résidus; donc le nombre des non-résidus est pair ou impair suivant que p sera de la forme $4n+1$, ou de la forme $4n+3$; donc le produit de tous les nombres $1, 2, 3, \ldots p-1$ sera résidu dans le premier cas et non-résidu dans le second (n° 99). Or ce produit $\equiv -1 \pmod{p}$; donc enfin -1 est résidu dans le premier cas et non-résidu dans le second.

111. Si donc r est résidu d'un nombre premier de la forme $4n+1$, $-r$ le sera aussi, et tous les non-résidus seront encore non-résidus en changeant les signes (*). Le contraire arrive pour les nombres premiers de la forme $4n+3$, dont les résidus deviennent non-résidus, et réciproquement, quand on change le signe (n° 98).

Au reste on déduit facilement de ce qui précède cette règle générale: -1 est résidu de tous les nombres qui ne sont divisibles ni par 4, ni par aucun nombre de la forme $4n+3$. Il est non-résidu de tous les autres. (N°s 103 et 105).

112. Passons aux résidus $+2$ et -2.

Si dans la table II on prend tous les nombres premiers dont le module est $+2$, on trouvera 7, 17, 23, 31, 41, 47, 71, 73, 79, 89, 97. Or on remarque facilement qu'aucun d'eux n'est de la forme $8n+3$ ou $8n+5$.

Voyons donc si cette induction peut devenir une certitude.

Observons d'abord que tout nombre composé de la forme $8n+3$ ou $8n+5$ renferme nécessairement un facteur premier de l'une ou l'autre

(*) Ainsi quand nous parlerons d'un nombre, en tant qu'il sera résidu ou non-résidu d'un nombre de la forme $4n+1$, nous pouvons ne faire aucune attention à son signe, ou lui donner le signe $\pm$.

forme; en effet les nombres premiers de la forme $8n+1$ et $8n+7$ ne peuvent former que des nombres de la forme $8n+1$ ou $8n+7$. Si donc notre induction est généralement vraie, il n'y aura aucun nombre de la forme $8n+3$, $8n+5$, dont le résidu soit $+2$. Or il est bien certain qu'il n'existe aucun nombre de cette forme et au-dessous de 100, dont le résidu soit $+2$; mais s'il y en avait au-dessus de cette limite, supposons que t soit le plus petit de tous; t sera de la forme $8n+3$ ou $8n+5$, et $+2$ sera son résidu; mais il sera non-résidu de tous les nombres semblables plus petits. Soit $a^2 \equiv 2 \pmod{t}$, on pourra toujours prendre a impair et $< t$, car a a au moins deux valeurs positives plus petites que t, dont la somme $= t$, et dont par-conséquent l'une est paire et l'autre impaire (nos 104, 105). Cela posé, soit $a^2 = 2 + ut$ ou $ut = a^2 - 2$, a^2 sera de la forme $8n+1$, et par-conséquent ut de la forme $8n-1$; donc u sera de la forme $8n+3$ ou $8n+5$ suivant que t sera de la forme $8n+5$ ou $8n+3$; mais de l'équation $a^2 = 2 + tu$, on tire la congruence $a^2 \equiv 2 \pmod{u}$, c'est-à-dire que $+2$ serait aussi résidu de u. Il est aisé de voir qu'on a $u < t$; il s'ensuivrait que t ne serait pas le plus petit nombre qui eût $+2$ pour résidu, ce qui est contre l'hypothèse; d'où suit enfin une démonstration rigoureuse de cette proposition, que nous avions déduite de l'induction.

En combinant cette proposition avec celles du n° 111, on en déduit les théorèmes suivans :

I. *$+2$ est non-résidu, et -2 est résidu de tous les nombres premiers de la forme* $8n+3$.

II. *$+2$ et -2 sont non-résidus de tous les nombres premiers de la forme* $8n+5$.

113. Par une semblable induction on tirera de la table II, pour les nombres premiers dont le résidu est -2, ceux-ci : 3, 11, 17, 19, 41, 43, 59, 67, 73, 83, 89, 97 (*). Parmi ces nombres il ne s'en trouve aucun de la forme $8n+5$ ou $8n+7$; cherchons donc si de cette induction nous pouvons tirer un théorème général. On fera voir de la même manière que dans l'article précédent, qu'un nombre composé de la forme $8n+5$ ou $8n+7$, doit renfermer un facteur premier de la forme $8n+5$ ou de la forme $8n+7$; desorte que si notre induction est

(*) En considérant -2 comme le produit de $+2$ par -1; voyez n° 111.

générale ment vraie, -2 ne peut être résidu d'aucun nombre de la forme $8n+5$ ou $8n+7$; or s'il peut y en avoir de tels, soit t le plus petit de tous, et qu'on ait $-2=a^2-tu$. Si l'on prend, comme plus haut, a impair et $<t$, u sera de la forme $8n+5$ ou $8n+7$, suivant que t sera de la forme $8n+7$ ou $8n+5$; mais de ce qu'on a $a<t$ et $ut=a^2+2$, il est facile de déduire que u est $<t$; et comme -2 serait aussi résidu de u, il s'ensuivrait que t ne serait pas le plus petit nombre dont -2 est le résidu, ce qui est contre l'hypothèse. Donc -2 sera nécessairement non-résidu de tous les nombres de la forme $8n+5$ ou $8n+7$.

En combinant cette proposition avec celles du n° 111, on en déduit les théorèmes suivans :

I. -2 *et* $+2$ *sont non-résidus de tous les nombres premiers de la forme* $8n+5$; comme nous l'avons déjà trouvé.

II. -2 *est non-résidu et* $+2$ *résidu de tous les nombres premiers de la forme* $8n+7$.

Au reste, nous aurions pu prendre a pair dans les deux démonstrations; mais alors il eût fallu distinguer le cas où a est de la forme $4n+2$, de celui où il est de la forme $4n$; d'ailleurs la marche est absolument la même et n'est sujette à aucune difficulté.

114. Il nous reste encore à traiter le cas où le nombre premier est de la forme $8n+1$; mais il échappe à la méthode précédente et demande des artifices tout-à-fait particuliers.

Soit, pour le module premier $8n+1$, une racine primitive quelconque a, on aura (n° 62) $a^{4n}\equiv -1 \pmod{8n+1}$; cette congruence peut se mettre sous la forme $(a^{2n}+1)^2\equiv 2a^{2n} \pmod{8n+1}$, ou $(a^{2n}-1)^2\equiv -2a^{2n}$; d'où il suit que $2a^{2n}$ et $-2a^{2n}$ sont résidus de $8n+1$; mais comme a^{2n} est un quarré non-divisible par le module, $+2$ et -2 seront aussi résidus (n° 98).

115. Il ne sera pas inutile d'ajouter encore une autre démonstration de ce théorème, qui a le même rapport avec celle que nous venons de donner, que la seconde démonstration du théorème du n° 108, a avec la première. Les gens instruits s'appercevront facilement que ces deux démonstrations ne sont pas aussi différentes qu'elles le paraissent au premier aspect, tant dans le premier cas que dans le second.

1°. Pour un module premier quelconque de la forme $4m+1$; parmi les nombres $1, 2, 3, \ldots 4m$, on en trouvera m qui peuvent être congrus à un biquarré, et les $3m$ autres ne pourront pas l'être.

On peut le conclure facilement des principes de la section précédente; mais on peut aussi s'en passer sans difficulté. En effet nous avons démontré que pour un pareil module, -1 était toujours résidu quadratique. Soit donc $f^2 \equiv -1$, il est clair que si z est un nombre quelconque non divisible par le module, les biquarrés des quatre nombres $+z, -z, +fz, -fz$ (qu'on voit facilement être incongrus) seront congrus entre eux. Or il est évident que le biquarré de tel nombre qu'on voudra, qui ne serait congru à aucun de ces nombres, ne pourrait pas être congru à leurs biquarrés; autrement la congruence $x^4 \equiv z^4$ aurait plus de quatre racines (n° 43). On déduit facilement de là que les nombres $1, 2, 3, \ldots 4m$ fournissent seulement m biquarrés incongrus, pour lesquels, parmi les mêmes nombres, on en trouvera m qui leur sont congrus; les autres ne pourront être congrus à aucun biquarré.

2°. Suivant un module premier de la forme $8n+1$, -1 peut être rendu congru à un biquarré; c'est-à-dire que -1 sera *résidu biquadratique* de ce nombre premier.

En effet le nombre des résidus biquadratiques moindres que $8n+1$ (zéro excepté), sera $= 2n$, c'est-à-dire, pair. Or on prouve facilement que, si r est résidu biquadratique de $8n+1$, la valeur de l'expression $\frac{1}{r}$ (mod. $8n+1$) est un pareil résidu. Donc on peut distribuer les résidus biquadratiques par classes, comme nous l'avons fait, au n° 109, pour les résidus quadratiques, et le reste de la démonstration est exactement le même qu'à l'article cité.

3° Soit maintenant $g^4 \equiv -1$ et h la valeur de l'expression $\frac{1}{g}$ (mod. $8n+1$). On aura alors $(g \pm h)^2 = g^2 + h^2 \pm 2gh \equiv g^2 + h^2 \pm 2$, puisque $gh \equiv 1$; mais $g^4 \equiv -1$; donc $g^4h^2 \equiv -h^2$: d'ailleurs... $g^4h^2 = g^2 . g^2h^2 \equiv g^2$, donc $g^2 \equiv -h^2$ ou $g^2 + h^2 \equiv 0$, et $(g \pm h)^2 \equiv \pm 2$; c'est-à-dire que $+2$ et -2 sont des résidus quadratiques de $8n+1$.

116. Au reste on tire facilement de ce qui précède la règle générale suivante: $+2$ *est résidu de tout nombre qui n'est divisible ni par* 4 *ni par aucun nombre premier de la forme* $8n+3$ *ou* $8n+5$,

et non-résidu de tous les autres, par exemple, de tous ceux de la forme $8n+3$, $8n+5$, tant premiers que composés.

-2 *est résidu de tout nombre qui n'est divisible ni par* 4 *ni par aucun nombre premier de la forme* $8n+5$ *ou* $8n+7$, *et non-résidu de tous les autres.*

Ces théorèmes élégans étaient connus de *Fermat* (*Op. mathém.*, *p.* 168); mais il n'en a point donné la démonstration, qu'il a dit avoir trouvée. Depuis, *Euler* l'a toujours cherchée en vain; mais *Lagrange* en a publié le premier une démonstration rigoureuse (*Nouv. Mém. de l'Ac. de Berlin.* 1775, p. 349, 351); et il paraît qu'*Euler* ne la connaissait pas encore quand il a écrit la dissertation que renferme le T. 1 des *Opuscula analyt.*, p. 259.

117. Passons aux résidus $+3$ et -3, et commençons par le dernier.

On trouve par la table II que les nombres premiers dont -3 est résidu, sont 3, 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97, parmi lesquels il n'y en a aucun de la forme $6n+5$. On démontre comme il suit qu'au-delà des tables il n'y a pas de nombres de cette forme dont -3 soit résidu: il est d'abord évident que tout nombre composé de la forme $6n+5$ renferme un facteur premier de la même forme; ainsi, quand il sera démontré qu'il n'y a pas de nombres premiers de la forme $6n+5$ dont -3 soit résidu, il demeurera prouvé qu'il n'y a pas non plus de nombres composés. Si donc au-delà des limites de la table il y avait de tels nombres, soit t le plus petit de tous, et qu'on ait $a^2 = -3+tu$; alors en prenant a pair et moindre que t, on aura $u<t$ et -3 résidu de u; or si a était de la forme $6n\pm 2$, tu serait de la forme $6n+1$, et partant u de la forme $6n+5$, ce qui est absurde, puisque nous avons supposé que t était le plus petit nombre contraire à notre induction; en second lieu, si a était de la forme $6n$, tu serait de la forme $36n+3$, et partant $\frac{1}{3}tu$ de la forme $12n+1$; donc $\frac{1}{3}u$ serait de la forme $6n+5$; or il est clair que -3 serait aussi résidu de $\frac{1}{3}u$, ce qui est absurde, puisque $\frac{1}{3}u<t$; donc -3 ne sera résidu d'aucun nombre de la forme $6n+5$.

Comme tout nombre de la forme $6n+5$ est contenu sous la forme

$12n+5$, ou $12n+11$, et que la première revient à $4n+1$ et la seconde à $4n+3$, on a les théorèmes suivans:

I. -3 *et* $+3$ *sont non-résidus de tout nombre premier de la forme* $12n+5$.

II. -3 *est non-résidu, et* $+3$ *résidu de tout nombre premier de la forme* $12n+11$.

118. On trouve dans la table II, que les nombres dont 3 est résidu sont 3, 11, 13, 23, 37, 47, 59, 61, 71, 73, 83, 97, parmi lesquels aucun n'est de la forme $12n+5$ ou $12n+7$; or on démontrera, comme dans les nos 112, 113, 117, qu'il n'y a absolument aucuns nombres de cette forme dont le résidu soit $+3$; ainsi nous ne nous y arrêterons pas. Nous en conclurons donc à l'aide du n° 111, les théorèmes suivans:

I. $+3$ *et* -3 *sont non-résidus d'un nombre premier quelconque de la forme* $12n+5$.

II. $+3$ *est non-résidu,* -3 *résidu de tout nombre premier de la forme* $12n+7$.

119. Cette méthode n'apprend rien pour les nombres de la forme $12n+1$, qui demandent des artifices particuliers. L'induction fait voir aisément que $+3$ et -3 sont résidus de tous les nombres premiers de cette forme. Or il suffit de démontrer que -3 l'est effectivement, puisqu'alors $+3$ le sera aussi (n° 111); mais nous allons faire voir plus généralement que -3 est résidu de tout nombre premier de la forme $3n+1$.

Soit p un de ces nombres premiers, et a un nombre appartenant à l'exposant 3, suivant le module p: et il est évident qu'il existe de tels nombres, puisque 3 divise $p-1$ (n° 55). On aura ainsi $a^3-1\equiv 0 \pmod{p}$, c'est-à-dire $a^3-1=(a-1)(a^2+a+1)$ divisible par p; mais on ne peut pas avoir $a\equiv 1 \pmod{p}$, parceque 1 appartient à l'exposant 1; donc $a-1$ n'est pas divisible par p, et partant a^2+a+1 le sera. D'où il s'ensuit que $4a^2+4a+4$ le sera aussi, c'est-à-dire qu'on aura $(2a+1)^2\equiv -3 \pmod{p}$, ou que -3 sera résidu de p.

Au reste il est clair que cette démonstration, qui est indépendante des précédentes, renferme aussi les nombres premiers de la forme $12n+7$, cas que nous avons résolu dans le n° précédent.

Nous observerons encore qu'on pourrait employer la méthode des nos 109 et 115; mais pour abréger nous ne nous y arrêterons pas.

120. On déduit facilement de ce qui précède les théorèmes suivans (nos 102, 103, 105):

I. -3 *est résidu de tous les nombres qui ne sont divisibles ni par* 8, *ni par* 9, *ni par aucun nombre premier de la forme* $6n+5$, *et non-résidu de tous les autres.*

II. $+3$ *est résidu de tous les nombres qui ne sont divisibles ni par* 4, *ni par* 9, *ni par aucun nombre premier de la forme* $12n+5$ *ou* $12n+7$, *et non-résidu de tous les autres.*

On doit remarquer surtout ce cas particulier:

-3 est *résidu* de tous les nombres premiers de la forme $3n+1$, ou, ce qui est la même chose, *de tous ceux qui sont résidus de* 3; et il est *non-résidu* de tous les nombres premiers de la forme $6n+5$, ou de tous ceux de la forme $3n+2$ (2 excepté), c'est-à-dire *de tous ceux qui sont non-résidus de* 3, et l'on voit facilement que tous les autres cas suivent naturellement de celui-là.

Les propositions relatives aux résidus $+3$ et -3, étaient connues de *Fermat* (*Opera Wallisii*, *T. II*, *p.* 857); mais *Euler* est le premier qui les ait démontrées (*Comment. nov. Petrop. T. VIII*, *p.* 105), c'est pourquoi il est encore plus étonnant que la démonstration des propositions relatives aux résidus $+2$ et -2 aient toujours échappé à sa sagacité, puisqu'elles sont appuyées sur les mêmes principes. On peut voir aussi les Recherches de *Lagrange* (Nouv. Mém. de l'Ac. de Berlin. 1775, *p.* 357).

121. L'induction fait voir que $+5$ n'est résidu d'aucun nombre impair de la forme $5n+2$, ou $5n+3$, c'est-à-dire d'aucun nombre impair qui soit non-résidu de 5 lui-même. Or nous allons démontrer que cette règle ne souffre aucune exception. Soit, s'il est possible, t le plus petit nombre à en excepter, 5 sera résidu de t, et t non-résidu de 5. Soit $a^2=5+tu$, desorte que a soit pair et $<t$; u sera impair et $<t$, et $+5$ sera résidu de u. Si a n'est pas divisible par 5, u ne le sera pas non plus; mais il est évident que tu est résidu de 5; donc comme t est non-résidu de 5, u le sera aussi, c'est-à-dire qu'il y a un nombre impair $\leq t$ qui est non-résidu de 5 et dont 5 est résidu; mais si a est

divisible par 5, soit $a=5b$ et $u=5v$, il en résultera $tv \equiv -1 \equiv 4$ (mod. 5), c'est-à-dire que tv sera résidu de 5. La marche de la démonstration est pour le reste la même que dans le cas précédent.

122. Donc $+5$ et -5 sont non-résidus de tous les nombres premiers qui sont à-la-fois non-résidus de 5 et de la forme $4n+1$, c'est-à-dire de tous les nombres premiers de la forme $20n+13$ ou $20n+17$; mais 5 sera non-résidu, et -5 résidu de tous les nombres premiers de la forme $20n+3$ ou $20n+7$.

Or on démontrera absolument de la même manière que -5 est non-résidu de tous les nombres premiers des formes $20n+11$, $20n+13$, $20n+17$, $20n+19$, et l'on voit facilement qu'il suit de là que $+5$ est résidu de tous les nombres premiers de la forme $20n+11$, ou $20n+19$; enfin non-résidu de tous ceux de la forme $20n+13$, ou $20n+17$; et comme tout nombre premier, excepté 2, et 5 dont ± 5 est résidu, est contenu dans l'une des formes : $20n+1, +3, +7, +9, +11, +13, +17, +19$, il est clair que l'on peut juger de tous, excepté de ceux qui sont de la forme $20n+1$, ou $20n+9$.

123. Par induction, on trouve facilement que $+5$ et -5 sont résidus de tous les nombres premiers de la forme $20n+1$ et $20n+9$; et si cette proposition est généralement vraie, on aura cette loi élégante que $+5$ *est résidu de tous les nombres premiers qui sont résidus de* 5 *lui-même*, (car ces nombres sont contenus dans les formes $5n+1$, ou $5n+4$, ou ce qui revient au même dans les formes $20n+1, +9, +11, +19$, parmi lesquelles la troisième et la quatrième ont déjà été traitées), *et non-résidu de tous les nombres premiers impairs, qui sont résidus de* 5, comme nous l'avons déjà démontré plus haut. Or il est clair que ce théorème suffit pour juger si $+5$ et partant -5, qui n'est autre que $+5\times-1$, sont résidus ou non-résidus d'un nombre donné quelconque. On peut observer aussi l'analogie de ce théorème avec celui du n° 120 sur le résidu -3.

Mais la vérification de cette induction n'est pas facile. Quand le nombre proposé est de la forme $20n+1$, ou plus généralement de la forme $5n+1$, on peut employer une méthode semblable à celles des n°s 114, 119. Soit en effet a un nombre quelconque appartenant

appartenant à l'exposant 5, suivant le module $5n+1$, nombre qu'on a appris à trouver dans la section précédente, on aura $a^5 \equiv 1$, ou $(a-1)(a^4+a^3+a^2+a+1) \equiv 0 \pmod{5n+1}$. Mais comme on ne peut avoir $a \equiv 1$, il s'ensuit qu'on aura $a^4+a^3+a^2+a+1 \equiv 0$; donc $4(a^4+a^3+a^2+a+1) = (2a^2+a+2)^2 - 5a^2 \equiv 0$; c'est-à-dire, que $5a^2$ est résidu de $5n+1$; et partant 5 lui-même, puisque a^2 est un résidu non-divisible par $5n+1$; car, à cause de $a^5 \equiv 1$, a n'est pas divisible par $5n+1$.

Comme le cas où il est question d'un nombre premier de la forme $5n+4$ demande des artifices particuliers de calculs, et comme nous traiterons par la suite, d'une manière générale, les propositions au moyen desquelles on peut résoudre ce problême, nous nous contenterons d'en parler ici en passant.

1°. Si p est un nombre premier, et b un nombre aussi donné non-résidu de p, la valeur de l'expression $\frac{(x+\sqrt{b})^{p+1} - (x-\sqrt{b})^{p+1}}{\sqrt{b}} = A$, dont le développement ne contiendra pas d'irrationnelles, sera toujours divisible par p, quelque valeur que l'on attribue à x. En effet il est clair, par l'inspection des coefficiens qui naissent de ce développement, que tous les termes, depuis le second jusqu'à l'avant-dernier inclusivement, sont divisibles par p, et que partant $A \equiv 2(p+1)\left(x^p + xb^{\frac{p-1}{2}}\right) \pmod{p}$; mais parceque b est non-résidu de p, on aura $b^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, (n° 106); or on a toujours $x^p \equiv x$ (section précédente), d'où s'ensuit $A \equiv 0$.

2°. Dans la congruence $A \equiv 0$, l'indéterminée x aura p dimensions, et tous les nombres $0, 1, 2, 3 \ldots p-1$, seront racines de cette congruence. Soit e un diviseur de $p+1$, l'expression... $\frac{(x+\sqrt{b})^e - (x-\sqrt{b})^e}{\sqrt{b}}$, que nous représenterons par B, sera rationnelle, x y aura $e-1$ dimensions, et il est constant par les premiers élémens d'analyse, que A est divisible par B. Or je dis qu'il y a $e-1$ valeurs, qui rendent B divisible par p. En effet, soit $A = BC$, x aura dans C, $p-e+1$ dimensions, et partant la congruence $C \equiv 0 \pmod{p}$, ne pourra avoir plus de $p-e+1$ racines, d'où il suit

que les $e-1$ autres nombres pris dans la série $0, 1, 2, \ldots p-1$, seront racines de la congruence $B \equiv 0$.

3°. Supposons maintenant p de la forme $5n+4$, $e=5$, b un non-résidu de p, et le nombre a déterminé de manière à rendre $\frac{(a+\sqrt{b})^5-(a-\sqrt{b})^5}{\sqrt{b}}$ divisible par p. Cette expression devient $=10a^4+20a^2b+2b^2=2\{(b+5a^2)^2-20a^4\}$; donc $(b+5a^2)^2-20a^4 \equiv 0 \pmod{p}$; c'est-à-dire que $20a^4$ est résidu de p; mais comme $4a^4$ est un résidu non-divisible par p, (car on voit facilement que a ne peut être divisible par p), 5 sera lui-même résidu de p.

Il est clair par là que le théorème énoncé au commencement de cet article est généralement vrai.

Observons encore que les démonstrations des deux cas sont dues à *Lagrange*. (*Mémoires de l'Académie de Berlin*, 1775, p. 352).

124. On démontre par une méthode semblable que -7 *est non-résidu de tout nombre premier qui est non-résidu de* 7, et l'on peut conclure par induction, que -7 *est résidu de tout nombre qui est résidu de* 7; mais personne n'a encore démontré rigoureusement cette seconde partie. Pour les nombres qui sont résidus de 7 et de la forme $4n-1$, la démonstration est facile, car on peut démontrer par la méthode précédente qui est maintenant assez connue, que $+7$ est toujours non-résidu de ces nombres, et partant -7 résidu. Mais nous sommes peu avancés par là, car les autres cas ne peuvent être traités par cette méthode. Il y a cependant un cas qui peut être résolu de la même manière qu'aux nos 119, 123. Soit p un nombre de la forme $7n+1$, et a un nombre appartenant à l'exposant 7; on voit facilement que $\frac{4(a^7-1)}{a-1} = (2a^3+a^2-a-2)^2+7(a^2+a)^2 \equiv 0$, et que partant $-7(a^2+a)^2$ est résidu de p. Mais $(a^2+a)^2$ comme quarré, est résidu de p; de plus il est non divisible par p. En effet a n'est ni $\equiv 0$, ni $\equiv -1 \pmod{p}$, c'est-à-dire que ni a, ni $a+1$ ne sont divisibles par p, et partant le quarré $(a-1)^2a^2$ ne l'est pas non plus. Donc 7 lui-même est résidu de p. Mais les nombres de la forme $7n+2$, ou $7n+4$ échappent à toutes les méthodes que nous avons fait connaître jusqu'à présent. Au reste, cette démonstration est encore due à *Lagrange*, (*ibidem*). Nous montrerons plus bas gé-

néralement, section VII, que l'expression $\frac{4(x^p-1)}{x-1}$ peut toujours être ramenée à la forme $X^2 \mp pY^2$, X et Y étant des fonctions rationnelles et entières de x, et où l'on doit prendre le signe supérieur, quand p est un nombre premier de la forme $4n+1$, et le signe inférieur, quand p est de la forme $4n+3$. *Lagrange* n'a pas poussé cette analyse au-delà du cas où $p=7$ (*Voyez ibidem*).

125. Puisque les méthodes précédentes ne suffisent pas pour établir des démonstrations générales, il est temps d'en exposer une autre exempte de ce défaut. Commençons par un théorème dont la démonstration nous a long-temps échappé, quoique au premier aspect il paraisse si facile, que plusieurs auteurs n'ont pas même cru qu'il fût nécessaire de le démontrer. C'est celui-ci : *Tout nombre, si l'on en excepte les quarrés pris positivement, est toujours non-résidu de quelques nombres premiers.* Mais comme ce théorème ne nous servira que d'auxiliaire pour d'autres démonstrations, nous ne présenterons que les cas dont nous pourrons avoir besoin; les autres se trouveront démontrés par la suite. Nous allons donc faire voir *que tout nombre premier de la forme* $4n+1$ *soit positif, soit négatif, est non-résidu de quelques nombres premiers, et même de nombres premiers plus petits que lui* (*).

Quand le nombre premier p de la forme $4n+1$ est pris négativement, soit $2a$ le nombre pair immédiatement plus grand que $\sqrt{p}$. On voit facilement que $4a^2$ est toujours $<2p$ (**) ou que $4a^2-p<p$.

(*) Il est évident qu'il faut excepter $+1$.

(**) L'assertion de l'auteur est vraie, excepté pour les valeurs $p=5$ et $p=17$. Soit en effet $p=m^2+k$, m^2 étant le plus grand quarré contenu dans p; on aura $2a=m+1$ ou $=m+2$, suivant que m sera impair ou pair, donc $4a^2$ sera m^2+2m+1 ou m^2+4m+4; d'où il suit

$4a^2-2p=1-2k+2m-m^2=2(1-k)-(m-1)^2$ ou $4a^2-2p=2(4-k)-(m-2)^2$

or dans le premier cas on a évidemment $4a^2-2p<0$, puisque k ne peut pas être plus petit que 4.

Dans le second cas, l'assertion est en défaut pour tous les nombres dans lesquels $k<4$ (ce qui exige qu'on ait $k=1$, puisque k est de la forme $4n+1$), et $(m-2)^2<6$, c'est-à-dire, pour les nombres pour lesquels $m=2$ ou $m=4$; ces nombres sont donc $2^2+1=5$ et $4^2+1=17$; mais pour tout autre on aura $4a^2-2p<0$.

On peut substituer la démonstration suivante qui n'offre aucune exception.

Mais $4a^2-p$ est de la forme $4n+3$ et $+p$ est résidu quadratique de $4a^2-p$, puisque $4a^2 \equiv p \pmod{4a^2-p}$. Si donc $4a^2-p$ est un nombre premier, $-p$ sera non-résidu; dans le cas contraire $4a^2-p$ renfermera un facteur de cette forme; donc $+p$ sera résidu, et partant $-p$ non-résidu.

Quand le nombre premier est pris positivement, il est nécessaire de distinguer deux cas; celui où p est de la forme $8n+5$, et celui où il est de la forme $8n+1$.

Soit d'abord p de la forme $8n+5$, prenons un nombre positif quelconque $a < \sqrt{\frac{1}{2}p}$; alors $8n+5-2a^2$ sera un nombre positif de la forme $8n+5$ ou $8n+3$, suivant que a sera pair ou impair, et nécessairement divisible par un nombre premier de la forme $8n+3$ ou $8n+5$, car le produit des nombres de la forme $8n+1$ et $8n+7$ ne peut avoir ni la forme $8n+3$, ni la forme $8n+5$. Soit cette différence égale à q, on aura $8n+5 \equiv 2a^2 \pmod{q}$. Mais (n° 112) 2 est non-résidu de q, et partant $2a^2$ et $8n+5$ (n° 98). a^2 en effet n'est pas divisible par q, car sans cela le nombre premier p serait divisible par q.

126. La démonstration n'est pas aussi simple dans le cas où le nombre premier positif est de la forme $8n+1$. Mais comme cette vérité est d'une grande importance, nous ne pouvons omettre la démonstration, quoiqu'un peu longue.

LEMME. *Si l'on a deux suites de nombres* A, B, C, D, etc. (I), A′, B′, C′, D′, *etc.* (II), (dans lesquelles il est indifférent que les termes soient ou non en même nombre) *telles que* p *étant un nombre premier quelconque ou une puissance d'un nombre premier qui divise un ou plusieurs termes de la seconde, il y ait au moins autant de termes de la première qui soient divisibles par* p; *alors je dis que le produit de tous les nombres de* (I) *est divisible par le produit de tous les nombres de* (II).

Soit $p = (m+1)^2 - k$, m étant la racine du plus grand quarré contenu dans p; il en résulte $(m+1)^2 \equiv p \pmod{k}$. Or si $m+1$ est pair, k sera de la forme $4n+3$ et parconséquent $-p$ sera non-résidu de k; si $m+1$ est impair, k sera de la forme $4n$, et comme les nombres de cette forme n'ont d'autres résidus que ceux qui sont de la forme $4n+1$ ou $8n+1$ (n° 103), il s'ensuit que $-p$ est non-résidu de k; or k est $< p$. (*Note du Traducteur*).

Exemple. Soit (I) composé des nombres 12, 18, 45, et (II) composé des nombres 3, 4, 5, 6, 9; alors en faisant successivement $p=2, 4, 3, 9, 5$, on trouvera dans (I) 2, 1, 3, 1, 1, termes divisibles, et 2 1, 3, 1, 1 dans (II) respectivement; or le produit de tous les termes de (I)=9720 qui est divisible par 3240, produit des termes de (II).

Démonstration. Soit Q le produit de tous les termes de (I), et Q' le produit de tous les termes de (II), il est évident que tout nombre premier diviseur de Q' le sera aussi de Q. Prouvons maintenant que tout facteur premier de Q' est au moins élevé à la même puissance dans Q. Soit p ce diviseur, et supposons qu'il y ait dans la suite (I) a termes divisibles par p et non par p^2, b par p^2 et non par p^3, c par p^3 et non par p^4, etc.; a', b', c', etc. ayant la même signification dans la suite (II). On verra facilement que $a+2b+3c+$ etc., est l'exposant de p dans Q, et $a'+2b'+3c'+$ etc., l'exposant de p dans Q'; mais a' n'est certainement pas $>a$, ni $b'>b$, etc. par hypothèse; donc aussi $a'+2b'+3c'+$ etc., ne sera pas $>a+2b+3c+$ etc., ainsi, comme aucun nombre premier ne peut avoir un exposant plus grand dans Q' que dans Q, Q est divisible par Q' (n° 17).

127. LEMME. *Dans la progression* 1, 2, 3, 4.... n, *il ne peut y avoir plus de termes divisibles par un nombre quelconque* h, *que dans la progression* a, a+1, a+2, ... a+n—1, *qui a le même nombre de termes.*

En effet on voit sans peine que si n est divisible par h, il y a dans chaque progression $\frac{n}{h}$ termes divisibles par h; sinon soit $n=he+f$, f étant $<h$; il y aura dans la première série e termes, et dans la seconde e ou $e+1$ termes divisibles par h.

Il suit de là, comme corollaire, que $\frac{a(a+1)(a+2)(a+3)\ldots(a+n-1)}{1 \quad 2 \quad 3 \quad\quad n}$ est toujours un nombre entier : proposition connue par la théorie des nombres figurés, mais qui, si je ne me trompe, n'a encore été démontrée directement par personne.

Enfin on aurait pu présenter plus généralement ce lemme comme il suit :

Dans la progression a, $a+1$, $a+2\ldots a+n-1$, il y a au moins autant de termes congrus suivant le module h à un nombre

donné quelconque, qu'il y a de termes divisibles par h dans la progression 1, 2, 3.... n.

128. Théorème. *Soit* a *un nombre quelconque de la forme* $8n+1$, p *un nombre quelconque premier avec* a *et dont* $+$a *soit résidu, et* m *un nombre arbitraire; je dis que dans la suite*, a, $\frac{1}{2}(a-1)$, $2(a-4)$, $\frac{1}{2}(a-9)$, $2(a-16)$, ... $2(a-m^2)$ *ou* $\frac{1}{2}(a-m^2)$ *suivant que* m *est pair ou impair, il y a au moins autant de termes divisibles par* p *que dans la suite* 1, 2, 3...2m$+$1. Désignons la première par (I), la seconde par (II).

1°. Quand $p=2$, tous les termes de (I), le premier excepté, c'est-à-dire m termes, seront divisibles par 2, et il y en aura autant dans (II).

2°. Si p est un nombre impair, ou le double ou le quadruple d'un nombre impair, et que $a\equiv r^2 \pmod{p}$, alors dans la progression $-m, -(m-1), -(m-2)\ldots 0, 1, 2\ldots m$ (III), qui a le même nombre de termes que (II), il y aura au moins autant de termes congrus à r suivant le module p, qu'il y en a dans (II) de divisibles par p (n° précéd.); mais on ne pourra pas en trouver deux qui ne diffèrent que par le signe; en effet si $r\equiv -f\equiv +f \pmod{p}$, on aura $2f\equiv 0$; donc aussi $2a\equiv 0$, puisque par hypothèse $f^2\equiv a$; mais comme a est premier avec p, on ne peut avoir $2a\equiv 0 \pmod{p}$ à moins que $p=2$, et nous avons déjà parlé de ce cas. Enfin chacun de ces nombres aura, dans la série (I), son correspondant qui sera divisible par p; savoir, si $\pm b$ est un terme de la série (III) congru à r suivant p, on aura $a-b^2\equiv 0 \pmod{p}$. Si donc b est pair, le terme $2(a-b^2)$ sera divisible par p; si b est impair, le terme $\frac{1}{2}(a-b^2)$ sera divisible par p; car $\frac{a-b^2}{p}$ sera entier et pair, puisque (hyp.) a est de la forme $8n+1$, et b^2 l'est aussi comme quarré d'un nombre impair, tandis que p est au plus divisible par 4. On conclut enfin de là qu'il y a dans la série (I) autant de termes divisibles par p, qu'il y en a dans la série (III) de congrus avec r suivant le module p, c'est-à-dire autant ou plus qu'il y en a de divisibles par p dans la série (II).

3°. Soit p de la forme $8n$, et $a\equiv r^2 \pmod{2p}$; car on voit facilement que a étant résidu de p, le sera aussi de $2p$. Alors dans la

série (III), il y aura au moins autant de termes congrus à r suivant p, qu'il y en a dans (II) de divisibles par p, et ils seront tous inégaux; mais à chacun d'eux, il en correspondra un dans la série (I) qui sera divisible par p. Si en effet $\pm b \equiv r \pmod{p}$, on aura $b^2 \equiv r^2 \pmod{2p}$ (*), et partant $\frac{1}{2}(a-b^2)$, et à plus forte raison $2(a-b^2)$ seront divisibles par p. Donc il y aura au moins autant de termes divisibles par p dans (I) que dans (II).

129. THÉORÈME. *Si* a *est un nombre premier de la forme* $8n+1$, *il y aura nécessairement au-dessous de* $2\sqrt{a}$ *un nombre premier dont* a *est non résidu.*

En effet, soit s'il se peut a résidu de tous les nombres premiers plus petits que $\sqrt{2a}$, il est clair que a serait aussi résidu de tous les nombres composés plus petits que $2\sqrt{a}$ (n° 105). Soit m le nombre immédiatement plus petit que $\sqrt{a}$. Alors dans la série (I) il y aura au moins autant de termes divisibles par un nombre quelconque $< 2\sqrt{a}$ que dans la série (II) du n°. précéd.; d'où il suit que le produit Q de tous les termes de (I) est divisible par le produit Q' de tous ceux de (III) (n° 126); mais le premier est $a(a-1)(a-4)\ldots(a-m^2)$ ou la moitié de ce produit, suivant que m est pair ou impair. Or puisque Q est divisible par Q' et que tous les facteurs de (II) sont premiers avec a, il s'ensuit que $\frac{Q}{a}$ est divisible par Q'. Or Q' peut être mis sous la forme..... $(m+1).(\overline{m+1}^2-1)(\overline{m+1}^2-4)\ldots.(\overline{m+1}^2-m^2)$, et l'on aurait $\frac{1}{m+1}\cdot\frac{a-1}{\overline{m+1}^2-1}\cdot\frac{a-4}{\overline{m+1}^2-4}\cdot\ldots\cdot\frac{a-m^2}{\overline{m+1}^2-m^2}$ = un nombre entier, quoique ce soit le produit de plusieurs fractions plus petites que l'unité, puisque $\sqrt{a}$ étant irrationnel, on a $m+1>\sqrt{a}$ et partant $(m+1)^2>a$. Il suit de là que notre supposition ne peut avoir lieu.

Or comme $a>4$, on aura $2\sqrt{a}<a$, et il existera un nombre premier $<a$ dont a est non-résidu.

130. Maintenant que nous avons démontré que tout nombre

(*) En effet $b^2-r^2=(b+r)(b-r)$; l'un de ces facteurs est divisible par p; l'autre est divisible par 2, puisqu'ils sont tous deux pairs; donc $b^2-r^2 \equiv 0 \pmod{2p}$.

premier de la forme $4n+1$ positif ou négatif, est toujours non-résidu d'un nombre premier au moins plus petit que lui, nous allons passer à l'examen exact et général de la condition nécessaire pour qu'un nombre premier soit résidu ou non-résidu d'un autre.

Nous avons démontré plus haut que -3 et $+5$ sont résidus ou non-résidus de tous les nombres premiers qui sont respectivement résidus ou non-résidus des nombres 3 et 5.

On trouve par induction, relativement aux nombres suivans, que, -7, -11, $+13$, $+17$, -19, -23, $+29$, -31, $+37$, $+41$, -43, -47, $+53$, -59, etc., sont résidus ou non-résidus de tous les nombres premiers qui, pris positivement, sont résidus ou non-résidus de ces nombres premiers. Cette induction s'établit facilement au moyen de la Table II.

Une légère attention suffit pour remarquer que parmi ces nombres premiers, ceux de la forme $4n+1$ sont affectés du signe $+$, et ceux de la forme $4n+3$, du signe $-$.

131. Nous démontrerons bientôt généralement ce que l'induction nous a fait découvrir; mais avant de l'entreprendre, il est nécessaire de faire voir toutes les conséquences de ce théorème supposé vrai et que nous énoncerons ainsi:

Tout nombre qui, pris positivement, est résidu ou non-résidu de p, *aura, pour résidu ou non-résidu,* $+$p *ou* $-$p, *selon que* p *sera de la forme* $4n+1$ *ou* $4n+3$.

Comme presque tout ce qu'on peut dire sur les résidus quadratiques est une suite de ce théorème, la dénomination du *théorème fondamental* dont nous nous servirons dorénavant, ne sera pas déplacée.

Pour exposer nos raisonnemens de la manière la plus courte, nous désignerons par a, a', a'', etc. les nombres premiers de la forme $4n+1$, par b, b', b'', etc. les nombres premiers de la forme $4n+3$, par A, A', A'', etc. les nombres quelconques de la forme $4n+1$, par B, B', B'', etc. les nombres quelconques de la forme $4n+3$. Enfin la lettre R placée entre deux quantités, indiquera que la première est résidu de la seconde, et la lettre N indiquera le contraire. Par exemple, $5R11$, $2N5$, indiqueront que 5 est résidu de 11, et que 2 est non-résidu de 5.

Maintenant,

Maintenant, à l'aide des théorèmes du n° 111, on déduira du théorème fondamental les propositions suivantes :

	Si	on aura
1..	$\pm aRa'$	$\pm a'Ra$
2..	$\pm aNa'$	$\pm a'Na$
3..	$\left\{\begin{matrix}+aRb\\-aNb\end{matrix}\right\}$	$\pm bRa$
4..	$\left\{\begin{matrix}+aNb\\-aRb\end{matrix}\right\}$	$\pm bNa$
5..	$\pm bRa$	$\left\{\begin{matrix}+aRb\\-aNb\end{matrix}\right.$
6..	$\pm bNa$	$\left\{\begin{matrix}+aNb\\-aRb\end{matrix}\right.$
7..	$\left\{\begin{matrix}+bRb'\\-bNb'\end{matrix}\right\}$	$\left\{\begin{matrix}+b'Nb'\\-b'Rb'\end{matrix}\right.$
8..	$\left\{\begin{matrix}+bNb'\\-bRb'\end{matrix}\right\}$	$\left\{\begin{matrix}+b'Rb\\-b'Nb\end{matrix}\right.$

132. Ce tableau renferme tous les cas qui peuvent se présenter quand on compare deux nombres premiers; le tableau suivant renferme ceux qui conviennent à la comparaison des nombres quelconques.

	Si	on aura
9.	$\pm aRA$	$\pm AR'a$
10.	$\pm bRA$	$\left\{\begin{matrix}+ARb\\-ANb\end{matrix}\right.$
11.	$+aRB$	$\pm BRa$
12.	$-aRB$	$\pm BNa$
13.	$+bRB$	$\left\{\begin{matrix}-BRb\\+BNb\end{matrix}\right.$
14.	$-bRB$	$\left\{\begin{matrix}+BRb\\-BNb.\end{matrix}\right.$

Comme les mêmes principes conduisent aux démonstrations de ces propositions, il n'est pas nécessaire de les développer toutes; la démonstration de la proposition 9 que nous plaçons ici, peut servir de modèle; mais, avant tout, il faut observer que tout nombre de la forme $4n+1$ ne renfermera aucun facteur de la forme $4n+3$, ou en renfermera un nombre pair parmi lesquels il pourra y en avoir d'égaux; tandis que tout nombre de la forme $4n+3$ doit en renfermer un nombre impair. Le nombre des facteurs de la forme $4n+1$ reste indéterminé.

Passons à la démonstration de la proposition 9. Soit A le produit des facteurs premiers a', a'', a''', etc. b, b', b'', etc.; le nombre de ces derniers sera nul ou pair. Or si a est résidu de A, il sera résidu de tous les facteurs a', a'', a''', etc. b, b', b'', etc.; donc, par les propositions 1 et 3 du n° précédent, chacun de ces facteurs sera résidu de a, et partant leur produit A; donc (n° 111) $-A$ le sera aussi; mais si $-a$ est résidu de A, il le sera de tous les facteurs de A, et chacun des nombres a', a'', etc. sera résidu de a, tandis que chacun des nombres b, b', etc. sera non-résidu; mais comme ces derniers sont en nombres pair, le produit total A sera résidu de a, et par conséquent aussi $-A$.

133. Donnons encore plus de généralité à nos recherches. Considérons deux nombres quelconques P et Q impairs et premiers entre eux, affectés de signes quelconques. Concevons P, abstraction faite du signe, décomposé en facteurs premiers, et désignons par p le nombre de ceux dont Q est non-résidu, en comptant plusieurs fois les facteurs qui entrent plusieurs fois dans P et dont Q est non-résidu. Soit de même q le nombre des facteurs de Q dont P est non-résidu. Les nombres p et q auront entre eux une certaine relation dépendante de la nature des nombres P et Q; savoir, si l'un des nombres pq est pair ou impair, la forme des nombres P et Q apprendra si l'autre est pair ou impair. Cette relation est présentée dans la table suivante:

p et q seront à-la-fois pairs ou impairs quand les nombres P et Q seront des formes:

$$1+A \text{ et } +A' \ldots . 2+A \text{ et } -A' \ldots . 3+A \text{ et } +B$$
$$4+A \text{ et } -B \ldots . 5-A \text{ et } -A' \ldots . 6+B \text{ et } -B'.$$

Au contraire, l'un sera pair et l'autre impair quand P et Q au-

ront une des formes

$7 - A$ et $+B$..... $8 - A$ et $-B$..... $9 + B$ et $+B'$ ..... $10 - B$ et $- B'$.

Exemple. Soient les nombres proposés -55 et $+1197$ qui doivent être rapportés au 4e cas. 1197 est non-résidu d'un seul facteur premier de 55 savoir, 5; mais -55 est résidu de trois facteurs premiers de 1197, savoir, 3, 3, 19.

Si P et Q désignent des nombres premiers, ces propositions reviennent à celles du n° 131. En effet, dans ce cas p et q ne peuvent être plus grands que 1; parconséquent lorsqu'on suppose p pair; il est nécessairement $=0$, c'est-à-dire que Q est résidu de P; mais quand p est impair, Q est non-résidu de P, et *vice versâ*. Ainsi en mettant a et b au lieu de A et B, il suit de la 8e que si $-a$ est résidu ou non-résidu de b, $-b$ sera non-résidu ou résidu de a, ce qui s'accorde avec la 3e et la 4e du n° 131.

En général il est clair que Q ne peut être résidu de P, à moins qu'on n'ait $p=0$; si donc p est impair, Q est certainement non-résidu de P.

On peut déduire sans peine de là les propositions du n° précédent.

Au reste on verra bientôt que ces relations générales ne sont pas une spéculation stérile, puisque sans leur secours il serait presqu'impossible de donner une démonstration complète du théorème fondamental.

134. Voyons maintenant la manière de déduire ces propositions.

1°. Soit, comme ci-dessus, P décomposé en facteurs premiers, et Q en facteurs quelconques, ayant toutefois égard au signe de Q. On pourra combiner chaque facteur de P avec chaque facteur de Q, et si l'on représente par s le nombre de toutes les combinaisons dans lesquelles le facteur de Q est non-résidu du facteur de P, p et s seront tous les deux pairs ou tous les deux impairs. Soient en effet f, f', f'', etc. les facteurs premiers de p, et supposons que parmi les facteurs de Q, il y en ait m non-résidus de f, m' non-résidus de f', m'' non-résidus de f'', etc. On voit facilement que l'on aura $s = m + m' + m'' +$ etc., et que p exprimera combien il y a de nombres impairs parmi m, m', m'' etc.; d'où il suit que s est pair quand p est pair, et impair quand p est impair.

2°. Ce que nous venons de dire a lieu de quelque manière qu'on décompose Q en facteurs. Passons aux cas particuliers. Considérons d'abord le cas où l'un des nombres P est positif, et l'autre Q, de la forme $+A$ ou $-B$; décomposons P et Q en facteurs premiers, en donnant à tous les facteurs de P le signe $+$, et le signe $+$ ou le signe $-$ à chacun de ceux de Q, suivant qu'ils seront de la forme a ou b, et Q sera alors de la forme $+A$ ou $-B$, comme l'hypothèse l'exige. Combinons chacun des facteurs de P avec chacun des facteurs de Q, et désignons comme ci-dessus par s le nombre des combinaisons dans lesquelles le facteur de Q est non-résidu du facteur de P, et semblablement par t le nombre de celles où le facteur de P est non-résidu du facteur de Q. Il suit du théorème fondamental que ces combinaisons doivent être identiques; donc $s=t$. Enfin de ce que nous avons démontré tout-à-l'heure, il suit que $p\equiv s \pmod 2$ et $q\equiv t \pmod 2$, d'où $p\equiv q \pmod 2$. Les propositions 1, 3, 4, 6 du n° 133 se trouvent démontrées par là.

On peut démontrer les autres propositions directement de la même manière; mais elles exigent une considération nouvelle, et il est plus aisé de les déduire, comme il suit, des précédentes.

3°. Désignons de nouveau par P et Q des nombres quelconques impairs et premiers entre eux, par p et q le nombre de facteurs premiers de P et Q, nombres dont Q et P sont respectivement non-résidus. Soit enfin p' le nombre de facteurs de P dont $-Q$ est non-résidu: quand Q sera négatif par lui-même, il est évident que $-Q$ indiquera un nombre positif. Distribuons maintenant les facteurs de P en quatre classes.

(1) En facteurs de la forme a, dont Q est résidu.

(2) En facteurs de la forme b, dont Q est résidu; soit leur nombre χ.

(3) En facteurs de la forme a, dont Q est non-résidu; soit leur nombre ψ.

(4) En facteurs de la forme b, dont Q est non-résidu; soit leur nombre ω.

On voit facilement que $p=\psi+\omega$, et $p'=\chi+\psi$; d'où $p'-p=\chi-\omega$.

Quand P sera de la forme $\pm A$, on aura $\chi+\omega\equiv 0 \pmod 2$, (n° 132), et parconséquent $\chi-\omega\equiv 2\omega$, ou $\chi-\omega\equiv 0 \pmod 2$; donc $p'-p\equiv 0 \pmod 2$. Quand P est de la forme $\pm B$ on trouve par un raisonnement semblable que p et p' sont incongrus suivant le module 2.

4°. Appliquons cela aux différens cas. Soient d'abord P et Q de la forme $+A$, on aura (prop. 1) $p\equiv q \pmod 2$; mais (3°.) $p'\equiv p$; donc $p'\equiv q \pmod 2$, ce qui s'accorde avec la proposition 2. De même si P est de la forme $-A$ et Q de la forme $+A$, on aura $p\equiv q \pmod 2$, par la proposition 2 que nous venons de démontrer; donc, comme $p'\equiv p$, on aura $p'\equiv q$; ainsi la prop. 5 est démontrée.

On déduira de la même manière la prop. 7 de la prop. 3, la 8e de la 4e ou de la 7e, la 9e et la 10e de la 6e.

135. Les propositions du n° 133 ne sont à la vérité pas démontrées par le n° précédent; mais nous avons fait voir que leur vérité dépend de la vérité du théorème fondamental que nous avons supposé; et par la méthode que nous avons suivie pour les déduire, il est évident qu'elles ont lieu pour les nombres P et Q, si le théorème fondamental a lieu pour tous les facteurs premiers de ces nombres comparés entre eux, quand même il ne serait pas généralement vrai. Passons maintenant à la démonstration du théorème fondamental. Pour rendre plus clair ce qui suivra, il est bon de prévenir d'avance que lorsque nous dirons que le théorème fondamental est vrai jusqu'à un nombre M, nous entendrons par là qu'il a lieu pour deux nombres premiers quelconques dont aucun n'est plus grand que M.

On doit entendre la même chose, lorsque nous dirons que les théorèmes des nos 131, 132, 133 sont vrais jusqu'à une certaine limite. Au reste, on voit que si la vérité du théorème fondamental est constatée jusqu'à une certaine limite, ces propositions auront aussi lieu jusqu'à la même limite.

136. La vérité du théorème fondamental pour de petits nombres, se découvre facilement par l'induction; ainsi on aura une limite jusqu'à laquelle il aura lieu. Nous supposons cette induction établie, et il est absolument indifférent jusqu'à quel point on la pousse. Ainsi il suffirait de la continuer jusqu'au nombre 5, ce qui se fait par une seule observation, puisqu'on a $\pm 5N3$ et $\pm 3N5$.

Or si le théorème fondamental n'est pas généralement vrai, il existera une limite T jusqu'à laquelle il le sera; desorte qu'il n'ait pas lieu pour le nombre immédiatement plus grand $T+1$: ce qui revient au même que si nous disions qu'il y a deux nombres premiers dont le plus grand est $T+1$, qui sont contraires au théorème, quoique deux autres nombres quelconques s'accordent avec lui, pourvu qu'ils soient plus petits que $T+1$. D'où il suit que les propositions des n°s 131, 132, 133 auront lieu jusqu'à T. Nous allons voir que cette supposition ne peut subsister. Il y a plusieurs cas à distinguer, suivant la forme qu'affectent $T+1$ et le nombre premier plus petit que lui qui, comparé à $T+1$, contrarie le théorème. Désignons ce nombre par p.

Quand $T+1$ et p sont de la forme $4n+1$, le théorème fondamental pourrait être faux de deux manières, savoir, si l'on avait à-la-fois, ou $\pm pR(T+1)$ et $\pm(T+1)Np$, ou $\pm pN(T+1)$ et $\pm(T+1)Rp$.

Quand $T+1$ et p sont de la forme $4n+3$, le théorème fondamental est faux, si l'on a en même temps ou $pR(T+1)$ et $-(T+1)Np$, (ou, ce qui revient au même, $-pN(T+1)$ et $+(T+1)Rp$, ou $+pN(T+1)$ et $-(T+1)Rp$, ou $-pR(T+1)$ et $+(T+1)Np$.

Quand $T+1$ est de la forme $4n+1$, et p de la forme $4n+3$, le théorème fondamental est faux, si l'on a à-la-fois ou $\pm pR(T+1)$ et $+(T+1)Np$; ou $-(T+1)Rp$ ou $\pm pN(T+1)$ et $-(T+1)Np$ ou $+(T+1)Rp$.

Quand $T+1$ est de la forme $4n+3$, et p de la forme $4n+1$, le théorème fondamental est faux, si l'on a ou $pR(T+1)$, ou $-pN(T+1)$ et $\pm(T+1)Np$; ou $+pN(T+1)$, ou $-pR(T+1)$ et $\pm(T+1)Rp$.

Si l'on peut démontrer qu'aucun de ces cas n'a lieu, il sera certain que la vérité du théorème fondamental n'est limitée par aucun terme. Entreprenons donc cette tâche; mais comme plusieurs de ces cas dépendent des autres, nous ne pourrons conserver l'ordre dans lequel nous les avons présentés.

137. Premier cas. *Quand* $T+1$ *est de la forme* $4n+1(=a)$,

et p *de la même forme, et que l'on a* ±pRa, *on ne peut pas avoir* ±aNp. C'est le premier cas du n° 131.

Soit $+p \equiv e^2 \pmod{a}$ et e pair et $< a$, ce qui est toujours possible. Il y a deux cas à distinguer :

1°. Quand e n'est pas divisible par p. Soit $e^2 = p + af$, f sera positif et de la forme $4n+3$, (ou de la forme B), $< a$ et non divisible par p. On aura donc $e^2 \equiv p \pmod{f}$, c'est-à-dire, pRf, d'où, par la proposition 11 du n° 132, $\pm fRp$; (car les propositions ont lieu pour les nombres p et $f < a$); mais on a aussi $afRp$, donc $\pm aRp$ (n° 98).

2°. Quand e est divisible par p. Soit $e = gp$ et $e^2 = p + aph$, ou $pg^2 = 1 + ah$. Alors h sera de la forme $4n+3$ (c'est-à-dire B), et premier avec p et g. Or on aura pg^2Rh, donc aussi pRh, donc (proposition 11, n° 132) $\pm hRp$; mais on a aussi $-ahRp$, à cause de $-ah \equiv 1 \pmod{p}$, donc aussi $\mp aRp$.

138. Second cas. *Quand* T+1 *est de la forme* 4n+1(=a), p *de la forme* 4n+3, *et que* ±pR(T+1), *on ne peut pas avoir* +(T+1)Np, *ou* −(T+1)Rp. C'est le cinquième cas du n° 131.

Soit, comme ci-dessus, $e^2 = p + fa$, e pair et $< a$:

1°. Quand e n'est pas divisible par p, f ne le sera pas non plus; d'ailleurs f sera positif, de la forme $4n+1$ (ou A) et $< a$; or on a $+pRf$, et partant $+fRp$ (prop. 10, n° 132); mais on a aussi $+faRp$, donc aRp, ou $-aNp$.

2°. Quand e est divisible par p. Soit $e = pg$ et $f = ph$, on aura ainsi $g^2p = 1 + ah$; alors h sera positif, de la forme $4n+3 (= B)$ et premier à p et à g^2. Or $+g^2pRh$, et parconséquent pRh; donc (prop. 13, n° 132) $-hRp$; mais on a $-ahRp$, d'où il résulte aRp et $-aNp$.

139. Troisième cas. *Quand* T+1 *est de la forme* 4n+1(=a), p *de la même forme, et que* ±pNa, *on ne peut pas avoir* ±aRp. C'est le deuxième cas du n° 131.

Soit pris un nombre premier moindre que a, dont $+a$ ne soit pas résidu (125—129); il faut considérer séparément deux cas, suivant que ce nombre premier sera de la forme $4n+1$ ou $4n+3$;

car il n'a pas été démontré qu'il en existe de tels sous l'une ou l'autre forme.

I. Soit ce nombre premier de la forme $4n+1$ et $=a'$, alors on aura $\pm a'Na$ (n° 137), d'où $\pm a'pRa$. Soit donc $e^2 \equiv a'p \pmod{a}$. Il y aura encore quatre cas à distinguer :

1°. Quand e n'est pas divisible ni par p, ni par a'. Soit $e^2 = a'p \pm af$, en prenant les signes de telle manière que f soit positif. Alors on aura $f < a$ premier avec a' et p : pour le signe supérieur, il sera de la forme $4n+3$; pour le signe inférieur, de la forme $4n+1$. Désignons, pour abréger, par $[x, y]$ le nombre de facteurs premiers de y, dont x est non-résidu ; comme on a évidemment $a'pRf$, il s'ensuit $[a'p, f]=0$; donc $[f, a'p]$ sera un nombre pair (prop. 1, 3, n° 133), c'est-à-dire ou $=0$, ou $=2$; donc f sera résidu des deux nombres a' et p, ou ne le sera d'aucun des deux ; mais la première supposition est inadmissible, puisque $\pm af$ est résidu de a' et que $\pm aNa'$ (hyp.), d'où il résulte $\pm fNa'$. Donc f est non-résidu des deux nombres a' et p ; mais puisque $\pm afRp$, on aura $\pm aNp$.

2°. Quand e est divisible par p et non par a'. Soit $e=gp$ et $g^2p = a' \pm ah$, le signe étant pris de manière à ce que h soit positif. On aura $h < a$ et premier avec a', g et p, pour le signe supérieur de la forme $4n+3$, et pour le signe inférieur de la forme $4n+1$. En multipliant tantôt par p et tantôt par a' l'équation $g^2p = a' \pm ah$, on en tire sans peine

$$pa'Rh \ldots (\alpha), \qquad \pm ahpRa' \ldots (\beta), \qquad aa'hRp \ldots (\gamma).$$

De (α) il suit que $[pa', h]=0$, et partant (prop. 1 et 3, n° 133) $[h, pa']$ pair, c'est-à-dire que h sera résidu ou non-résidu de p et de a'. Dans le dernier cas, il suit de (β) que $\pm apNa'$ et comme par hypothèse $\pm aNa'$, on aura $\pm pRa'$; donc, par le théorème fondamental qui a lieu pour les nombres p et a' moindres que $T+1$, $\pm a'Rp$. De là et de ce que hNp on tire, au moyen de (γ), $\pm aNp$. Dans le premier cas, de (β) on tire $\pm apRa'$, d'où $\pm pNa'$, $\pm a'Np$; de là enfin et de hRp on déduit, au moyen de γ, $\pm aNp$.

3°. Quand e est divisible par a' et non par p, la démonstration

tion procède presque de la même manière que dans l'hypothèse précédente, et ne pourra pas arrêter celui qui l'a bien conçue.

4°. Quand e sera divisible à-la-fois par a' et par p, il le sera aussi par le produit $a'p$; (en effet nous supposons les nombres a' et p inégaux, sans cela l'hypothèse aNa' contiendrait la relation aNp, qu'il s'agit de démontrer). Soit $e=ga'p$ et $g^2a'p=1\pm ah$, h sera $<a$ et premier avec p et a'; il sera pour le signe supérieur de la forme $4n+3$, et pour le signe inférieur de la forme $4n+1$. Or on voit facilement que de cette équation on peut déduire

$$a'pRh, \qquad \pm ahpRa', \qquad \pm aa'hRp,$$

relations qui s'accordent avec celles trouvées (2°.). Quant au reste, la démonstration est la même.

II. Quand le nombre premier est de la forme $4n+3$, la démonstration est si conforme à la précédente, qu'il nous a paru superflu de la placer ici. Nous observerons seulement, en faveur de ceux qui veulent la faire eux-mêmes (ce que nous recommandons), qu'il est avantageux, lorsqu'on est arrivé à l'équation $e^2=bp\pm af$, dans laquelle b représente le nombre premier de considérer séparément les deux signes.

140. Quatrième cas. *Quand* T+1 *est de la forme* 4n+1 (=a), p *de la forme* 4n+3 *et* ±pNa, *on ne peut avoir* +aRp, *ou* —aNp. Sixième cas du n° 131.

Nous omettons la démonstration de ce cas, parcequ'elle est absolument semblable à celle du troisième.

141. Cinquième cas. *Quand* T+1 *est de la forme* 4n+3(=b), *et* p *de la même forme, et que l'on a* pRb, *ou* —pNb, *on ne peut avoir* +bRp, *ou* —bNp. Troisième cas du n° 132.

Soit $p\equiv e^2 \pmod{b}$, e étant pair et $<b$.

I. Quand e n'est pas divisible par p; soit $e^2=p+bf$, f sera positif, $<b$, de la forme $4n+3$ et premier avec p. Or on a pRf, et partant (prop. 13, n° 132) $-fRp$; mais comme $bfRp$, il s'ensuit que $-bRp$, d'où $+bNp$.

II. Quand e est divisible par p; soit $e=pg$ et $g^2p=1+bh$. Alors h sera de la forme $4n+1$ et premier avec p, $p\equiv b^2p^2$

(mod. h), parconséquent pRh; d'où il résulte (prop. 10, n° 132) $+hRp$; mais on a $-bhRp$, donc $-bRp$ ou $+bNp$.

142. Sixième cas. *Quand* T$+1$ *est de la forme* 4n$+3$(=b), p *de la forme* 4n$+1$ *et* pRb, *on ne peut pas avoir* $\pm$bNp. Septième cas du n° 131.

Nous omettons la démonstration, qui est semblable à la précédente.

143. Septième cas. *Quand* T$+1$ *est de la forme* 4n$+3$(=b), p *de la même forme et qu'on a* $+$pNb, *ou* $-$pRb, *on ne pourra avoir* $+$bNp, *ou* $-$bRp. Quatrième cas du n° 131.

Soit $-p \equiv e^2$ (mod. b), et e pair $< b$.

I. Quand e n'est pas divisible par p, soit $-p = e^2 - bf$; f sera positif, de la forme $4n+1$, premier avec p et moindre que b; car de ce que e n'est pas plus grand que $b-1$, et que $p < b-1$, il s'ensuit que $bf = p + e^2 < b^2 - b$, ou $f < b-1$. Or on a $-pRf$, donc (prop. 10 n° 132) $+fRp$; d'ailleurs $bfRp$, donc bRp, ou $-bNp$.

II. Quand e est divisible par p, soit $e = pg$ et $g^2 p = -1 + bh$, h sera positif, de la forme $4n+3$, premier à p et $< b$; or on a $-pRh$, donc (prop. 14, n° 132) hRp; d'ailleurs $bhRp$, donc $+bRp$ et $-bNp$.

144. Huitième cas. *Quand* T$+1$ *est de la forme* 4n$+3$(=b), p *de la forme* 4n$+1$, *et que* $+$pNb, *ou* $-$pRb, *on ne pourra avoir* $\pm$bRp. Dernier cas du n° 131.

La démonstration est la même que dans le cas précédent.

145. Dans la démonstration du théorème fondamental, nous avons toujours pris pour e une valeur paire; on aurait pu également employer une valeur impaire; mais alors il aurait fallu distinguer différens cas. Ceux qui aiment ces recherches ne perdront pas leur temps, s'ils s'exercent à les développer: il est alors nécessaire de supposer les théorèmes relatifs aux résidus $+2$ et -2; mais comme notre démonstration a été achevée sans y avoir recours, nous en tirons une nouvelle manière de les démontrer; elle est d'autant moins à dédaigner, que les méthodes dont nous nous sommes servis pour démontrer que ± 2 est résidu de tout nombre premier de la forme $8n+1$ peuvent ne pas sembler assez

directes. Nous supposerons les autres cas démontrés par les méthodes exposées précédemment, et que celui où le nombre premier est de la forme $8n+1$ n'est trouvé que par induction. Nous le démontrerons rigoureusement de la manière suivante.

Si ± 2 n'était pas résidu de tous les nombres premiers de la forme $8n+1$, soit a le plus petit nombre de cette forme, dont ± 2 soit non-résidu, ensorte que le théorème ait lieu pour tous les nombres plus petits que a. On prendra un nombre premier $< \frac{1}{2}a$, dont a ne soit pas résidu, ce qui est toujours possible, puisque par le n° 129 on en trouvera un $< 2\sqrt{a}$, et qu'on a $2\sqrt{a} < \frac{1}{2}a$, car cette condition se réduit à $4 < \sqrt{a}$, ou $a > 16$, et le plus petit nombre premier de la forme $8n+1$ (1 excepté) est 17. Soit ce nombre $= p$, on aura, par le théorème fondamental, pNa; d'ailleurs $\pm 2Na$, donc $\pm 2pRa$. Soit donc $e^2 \equiv 2p \pmod{a}$, e étant impair et $< a$; alors il y a deux cas à distinguer.

I. Quand e n'est pas divisible par p. Soit $e^2 = 2p + aq$, q sera positif, $< a$, non-divisible par p; il sera de la forme $8n+7$, ou $8n+3$, suivant que p sera de la forme $4n+1$ ou $4n+3$. On distribuera tous les facteurs premiers de q en quatre classes, et supposons qu'il y en ait f de la forme $8n+1$, g de la forme $8n+3$, h de la forme $8n+5$, et l de la forme $8n+7$. Soient F, G, H, L les produits des facteurs de ces quatre classes; on observera que, si les facteurs d'une certaine classe manquaient, il faudrait mettre 1 à la place de leur produit. Cela posé, commençons par le cas où p est de la forme $4n+1$, et conséquemment q de la forme $8n+7$. q étant $< a$, le théorème a lieu pour ses diviseurs de la forme $8n+1$, donc $2RF$; mais il est démontré que 2 est résidu de tout nombre de la forme $8n+7$, donc aussi $2RL$. Or l'équation $e^2 = 2p + aq$ donne $2pRq$ et partant $2pRF$ et $2pRL$, donc pRF et pRL; d'où s'ensuit enfin, en vertu du même théorème fondamental (prop. 9 et 11, n° 132), FRp et LRp. Mais 2 est non-résidu de tout facteur de la forme $8n+3$ ou $8n+5$, donc il est résidu ou non-résidu de GH, suivant que $g+h$ est pair ou impair, et il est aisé de voir que p est aussi résidu ou non-résidu dans les mêmes circonstances; mais $g+h$ ne saurait être impair, car en examinant les différens cas, il s'ensuivrait que $FGHL$ ou q serait de la forme $8n+3$ ou $8n+5$, contre l'hypothèse. On

aura donc $pR\,GH$, d'où $GH\,Rp$, et comme nous avons déjà $FLRp$, il s'ensuit $FG\,HL\,Rp$ ou qRp; d'ailleurs l'équation $e^2 = 2p + aq$ donne encore $aq\,Rp$, donc aRp, contre l'hypothèse. Dans le cas où p est de la forme $4n+3$ et q de la forme $8n+3$, on peut faire voir de la même manière que pRF, et partant FRp, $-pRG$, donc GRp; enfin, que $h+l$ est pair, et parconséquent, $HL\,Rp$, d'où il suit qRp et aRp, contre l'hypothèse.

II. Quand e est divisible par p, la démonstration peut s'établir d'une manière semblable: nous laissons au lecteur le soin de la trouver.

146. Au moyen du théorème fondamental et des propositions relatives à -1 et ± 2, on peut toujours déterminer si un nombre donné quelconque est résidu ou non-résidu d'un nombre premier donné. Mais il ne sera pas inutile de reprendre ici ce que nous avons fait voir plus haut, afin de réunir tout ce qui est nécessaire pour la solution de ce problême-ci :

Étant donnés deux nombres quelconques P *et* Q, *trouver si l'un d'eux est résidu ou non-résidu de l'autre.*

I. Soit $P = a^\alpha b^\beta c^\gamma$ etc., a, b, c, etc. désignant des nombres premiers inégaux pris positivement; car il est évident que P doit être toujours regardé comme positif. Pour abréger, dans ce numéro nous appellerons simplement *relation* de deux nombres x, y, celle qui existe entre ces deux nombres, en tant que le premier x est résidu ou non-résidu du second y. La relation des nombres Q et P dépend ainsi de la relation des nombres Q et a^α, Q et b^β, etc. (n° 105).

II. Cherchons la relation des nombres Q et a^α; et ce que nous allons dire s'appliquera également aux relations de Q et b^β, etc.

1°. Quand Q est divisible par a, soit $Q = Q'a^e$, Q' n'étant pas divisible par a; alors si $e = \alpha$ ou $> \alpha$, on aura QRa^α, mais si $e < \alpha$ et impair, on aura QNa^α; enfin si $e < \alpha$ et pair, la relation de Q à a^α sera la même que celle de Q à $a^{\alpha-e}$. Ainsi ce cas est ramené au suivant. (Voyez n° 102).

2°. Quand Q n'est pas divisible par a, nous ferons encore ici deux sous-divisions :

(A). Quand $a=2$, on a toujours QRa^{α} si $\alpha=1$; mais si $\alpha=2$, il faut que Q soit de la forme $4n+1$, et quand $\alpha=3$ ou >3, Q doit être de la forme $8n+1$; si cette condition a lieu, ou aura QRa^{α}. (Voyez n° 103).

(B). Quand a est différent de 2, la relation de Q à a^{α} est la même que celle de Q à a. (Voyez n° 101).

III. On cherchera de la manière suivante la relation d'un nombre quelconque Q à un nombre premier a impair : quand $Q>a$, on substituera à Q son *résidu minimum positif* suivant le module a, ou, ce qui est quelquefois avantageux, son *résidu minimum absolu*, qui aura avec a la même relation que Q.

Or si l'on résout Q, ou le nombre pris à sa place, en facteurs premiers p, p', p'', etc., auxquels il faut joindre le facteur -1, quand Q est négatif, il est évident que la relation de Q à a dépendra de la relation des facteurs p, p', p'', etc. à a : ensorte que, si parmi eux il y en a $2m$ non-résidus de a, on aura QRa ; mais s'il y en a $2m+1$, on aura QNa. Au reste, on voit facilement que si parmi les facteurs p, p', p'', etc., il y en a un nombre pair d'égaux entre eux, on peut les rejeter, puisqu'ils n'influent en rien sur la relation de Q à a.

IV. Si -1 et 2 sont facteurs de Q, leur relation à a se trouve par les n°s 108, 112, 113, 114, mais la relation des autres nombres à a dépend de la relation de a à ces nombres. (Théorème fondam. et n° 131). Soit p l'un d'eux ; en traitant a et p comme nous avons traité Q et a, qui étaient des nombres plus grands, on trouvera que la relation de a à p peut être déterminée par les n^{os} (108—114), (si, par exemple, le résidu *minimum* de a (mod. p) n'est divisible par aucun nombre impair), ou que cette relation dépend de celle de p à des nombres premiers plus petits que lui. Il en est de même des autres facteurs p', p'', etc. Or on voit facilement qu'en continuant ces opérations, on arrivera né-

cessairement à des nombres dont les relations seront déterminées par les numéros précités. Un exemple éclaircira cette méthode.

Soit proposé de trouver la relation de 453 à 1236; $1236 = 3.4.103$, et $453 R 4$ (II. 2.) (A), $453 R 3$ (II. 1.); il reste donc à trouver la relation de 453 à 103; or elle sera la même que celle de 41 à 103, puisque $453 \equiv 41 \pmod{103}$, ou (Théor. fond.) que celle de 103 à 41, ou encore que celle de -20 à 41, puisque $-20 \equiv 103 \pmod{41}$; mais $-20 = -1.2.2.5$; or $-1 R 41$ (n° 108); $5 R 41$, car $41 \equiv 1 \pmod{5}$ et est parconséquent résidu de 5 (théor. fond.); il suit de là que $+453 \; R \; 103$, ou enfin $+453 \; R \; 1236$.

147. Étant proposé un nombre quelconque A, on peut trouver de certaines formules qui contiennent tous les nombres premiers à A dont A est résidu, ou tous ceux qui sont diviseurs des nombres de la forme $x^2 - A$, x^2 étant un quarré indéterminé. Nous appellerons simplement ces nombres *diviseurs* de $x^2 - A$; l'on voit facilement ce que sont les *non-diviseurs*. Mais pour abréger nous ne considérerons que les diviseurs qui sont impairs et premiers à A, les autres cas se ramenant sans peine à celui-là.

Soit d'abord A un nombre premier positif de la forme $4n+1$, ou négatif de la forme $4n-1$. Suivant le théorème fondamental, tous les nombres premiers qui, pris positivement, sont résidus de A, seront diviseurs de $x^2 - A$; mais tous les nombres premiers non-résidus de A seront non-diviseurs de $x^2 - A$, si pourtant on en excepte 2, qui est toujours diviseur. Soient r, r', r'', etc., tous les résidus de A qui sont plus petits que lui, et n, n', n'', etc., tous les non-résidus; alors tout nombre premier contenu dans une des formes $Ak+r$, $Ak+r'$, $Ak+r''$, etc. sera diviseur de $x^2 - A$; mais tout nombre premier contenu dans une des formes $Ak+n$, $Ak+n'$, etc. sera non-diviseur de $x^2 - A$, k étant un nombre entier indéterminé. Nous appellerons les premières *formes des diviseurs* de $x^2 - A$, et les dernières *formes des non-diviseurs*. Le nombre de chacune d'elles sera égal au nombre de résidus r, r', etc. ou de non-résidus n, n', etc., et partant, (n° 96) $= \frac{1}{2}(A-1)$. Or si B est un nombre composé impair et que l'on ait ARB, tous les facteurs premiers de B seront contenus dans une des premières formes, et parconséquent, B lui-même; donc tout nombre com-

posé impair qui sera contenu dans la forme des non-diviseurs sera non-diviseur de $x^2 - A$; mais on ne peut pas dire que les non-diviseurs de $x^2 - A$ sont tous compris dans la forme des non-diviseurs, car en supposant B non-diviseur de $x^2 - A$, quelques-uns de ses facteurs premiers seront non-diviseurs de $x^2 - A$, et si le nombre de ces facteurs est pair, B sera compris dans quelque forme de diviseurs (n° 93).

Ainsi, soit $A = -11$; on trouvera que les formes des diviseurs de $x^2 + 11$ sont $11k+1$, 2, 3, 4, 5, 9, et que celles des non-diviseurs sont $11k+2$, 6, 7, 8, 10. Ainsi -11 sera résidu de tous les nombres premiers contenus dans une des premières formes, et non-résidu de ceux qui sont contenus dans une des dernières.

On peut trouver des formes semblables pour les diviseurs et les non-diviseurs de $x^2 - A$, quel que soit A; mais on voit aisément qu'on n'a à considérer que les valeurs de A qui ne sont divisibles par aucun quarré; car si $A = a^2 A'$, tous les diviseurs de $x^2 - A$ premiers avec A, seront diviseurs de $x^2 - A'$, et de même pour les non-diviseurs. Or nous distinguerons trois cas : 1°. quand A est de la forme $4n+1$ ou $-(4n-1)$; 2°. quand A est de la forme $4n-1$ ou $-(4n+1)$; 3°. quand A est pair ou de la forme $\pm(4n+2)$.

148. *Premier cas.* Quand A est de la forme $4n+1$ ou $-(4n-1)$. On résoudra A en facteurs premiers, a, b, c, d, etc., en affectant du signe $+$ ceux de la forme $4n+1$, et du signe $-$ ceux de la forme $4n-1$ qui seront en nombre pair ou impair, suivant que A sera de la forme $4n+1$ ou $-(4n-1)$ (n° 132). On distribuera en deux classes les nombres plus petits que A et premiers avec lui; en mettant dans la première ceux qui ne sont non-résidus d'aucun diviseur de A, ou qui sont non-résidus d'un nombre pair de ces diviseurs, et dans la seconde ceux qui sont non-résidus d'un nombre impair des mêmes diviseurs. Désignons les premiers par r, r', r'', etc. et les secondes par n, n', n'', etc.; alors $Ak+r$, $Ak+r'$, etc., sont les formes des diviseurs de $x^2 - A$, et $Ak+n$, $Ak+n'$, etc. celles des non-diviseurs. C'est-à-dire que *tout nombre premier, excepté* 2, *sera diviseur ou non-diviseur de* $x^2 - A$, *suivant qu'il sera contenu dans l'une des premières ou l'une des dernières formes.*

En effet, si p est un nombre premier résidu ou non-résidu

d'un des facteurs de A, ce facteur sera résidu ou non-résidu de p (théor. fond.); donc si parmi les facteurs de A, il y en a m dont p soit non-résidu, il y en aura autant qui seront non-résidus de p, et partant, lorsque p sera contenu dans l'une des premières formes, m sera pair et ARp, et lorsque p sera contenu dans une des dernières, m sera impair et ANp.

Exemple. Soit $A=+105=-3\times+5\times-7$; les nombres r, r', r'', etc. sont:

1, 4, 16, 46, 64, 79, qui ne sont non-résidus d'aucun fact.;
2, 8, 23, 32, 53, 92, qui sont non-résidus de 3 et 5;
26, 41, 59, 89, 101, 104, ... 3 et 7;
23, 52, 73, 82, 97, 103, ... 5 et 7;

les nombres n, n', n'', etc. sont:

11, 29, 44, 71, 74, 86, non-résidus de 3;
22, 37, 43, 58, 67, 88, ... de 5;
19, 31, 34, 61, 76, 94, ... de 7;
17, 38, 47, 62, 68, 83, ... de 3, 5 et 7.

On déduit facilement de la théorie des combinaisons et des n^{os} (32, 96) que la multitude des nombres r, r', etc. sera

$$t\left(1+\frac{l(l-1)}{1.2}+\frac{l(l-1)(l-2)(l-3)}{1.2.3.4}+\text{etc.}\right),$$

et celle des nombres n, n', etc.

$$t\left(l+\frac{l(l-1)(l-2)}{1.2.3}+\frac{l(l-1)(l-2)(l-3)(l-4)}{1.2.3.4.5}+\text{etc.}\right),$$

l désignant le nombre des facteurs a, b, c, d, etc., t étant $=2^{-l}(a-1)(b-1)(c-1)$ etc., et chaque série devant être continuée jusqu'à ce qu'elle s'arrête d'elle-même. (En effet il y a t nombres résidus de a, b, c, d, etc., $t.\frac{l.(l-1)}{1.2}$ non-résidus de deux de ces facteurs, etc. Mais pour abréger, nous sommes forcés de ne pas donner plus de développement à la démonstration). Or chacune des séries a pour somme $t.2^{l-1}$; car la première

mière provient de $1 + \frac{l-1}{1} + \frac{(l-1)(l-2)}{1.2} + \frac{(l-1)(l-2)(l-3)}{1.2.3} +$ etc. en prenant le premier terme, puis la somme du second et du troisième, puis la somme du quatrième et du cinquième, etc. : la seconde provient aussi de la même série, en joignant le premier terme au second, le troisième au quatrième, etc. Il y a donc autant de formes de diviseurs de $x^2 - A$, que de formes de non-diviseurs; et ils sont en nombre $2^{i-1}.t$ de chaque espèce, ou $\frac{1}{2}(a-1)(b-1)(c-1)(d-1)$ etc.

149. Nous pouvons traiter ensemble le second et le troisième cas. En effet on pourra toujours poser $A = (-1).Q$, ou $= (+2)Q$, ou $= (-2)Q$, Q étant un nombre de la forme $+4n+1$ ou $-(4n-1)$. Soit généralement $A = \alpha Q$, ensorte que α soit ou -1 ou ± 2. Alors A sera résidu de tout nombre dont α et Q seront tous deux résidus, ou tous deux non-résidus : au contraire il sera non-résidu de tout nombre dont l'un d'eux seulement sera non-résidu. De là on déduit sans peine les formes des diviseurs et des non-diviseurs de $x^2 - A$. Si $\alpha = -1$; nous partagerons tous les nombres plus petits que $4A$ et premiers avec lui, en deux classes. La première renfermera ceux qui sont dans quelque forme des diviseurs de $x^2 - Q$, et en même temps de la forme $4n+1$, et aussi ceux qui sont dans quelque forme des non-diviseurs de $x^2 - Q$ et en même temps de la forme $4n-1$: la seconde renfermera tous les autres. Soient r, r', r'', etc. les premiers, et n, n', n'', etc. les derniers; A sera résidu de tous les nombres premiers contenus dans une des formes $4Ak+r$, $4Ak+r'$, $4Ak+r''$, etc., et non-résidu de tous les nombres premiers contenus dans une des formes $4Ak+n$, $4Ak+n'$, $4Ak+n''$, etc. Si $\alpha = \pm 2$, nous distribuerons tous les nombres plus petits que $8Q$ et premiers avec lui en deux classes : la première renfermera tous ceux qui sont contenus dans quelque forme des diviseurs de $x^2 - Q$, et qui sont de la forme $8n+1$ ou $8n+7$, pour le signe supérieur, et de la forme $8n+1$ ou $8n+3$ pour le signe inférieur; cette classe comprendra aussi tous ceux qui sont contenus dans quelque forme de non-diviseurs de $x^2 - Q$ et qui sont, pour le signe supérieur, de la forme $8n+3$, $8n+5$, et pour le signe inférieur, de la forme $8n+5$, $8n+7$, et la seconde tous les autres. Alors désignant les nombres de la première classe par r, r', r'', etc., ceux de la seconde par n, n', n'', etc., $\pm 2Q$ sera résidu de tous les nombres

premiers contenus dans les formes $8Qk+r, 8Qk+r', 8Qk+r''$, etc., et non-résidu de tous ceux contenus dans les formes $8Qk+n, 8Qk+n', 8Qk+n''$, etc. Au reste, on peut démontrer facilement qu'il y a autant de formes de diviseurs qu'il y en a de non-diviseurs.

Exemple. On trouve ainsi que 10 est résidu de tous les nombres premiers contenus dans les formes $40K+1, +3, +9, +13, +27, +31, +37, +39$, et non-résidu de tous les nombres premiers contenus dans les formes $40K+7, +11, +17, +19, +21, +23, +29, +33$.

150. Ces formes ont plusieurs propriétés assez remarquables; nous n'en citerons cependant qu'une seule. Si B est un nombre composé premier avec A, tel qu'un nombre $2m$ de ses facteurs premiers soient compris dans quelque forme de non-diviseurs de x^2-A, B sera contenu dans quelque forme de diviseurs de x^2-A; mais si le nombre de facteurs premiers de B contenus dans quelque forme de non-diviseurs de x^2-A est impair, B sera aussi contenu dans quelque forme de non-diviseurs. Nous omettons la démonstration, qui n'a rien de difficile. Il suit de là que non-seulement tout nombre premier, mais aussi tout nombre composé impair et premier avec A est non-diviseur dès qu'il est contenu dans une des formes de non-diviseur; car nécessairement quelque facteur premier de ce nombre sera non-diviseur.

151. Le théorème fondamental que nous avons présenté d'une manière très-simple et qui le met au nombre des théorèmes les plus élégans dans ce genre, n'a été jusqu'ici démontré par personne; ce qui doit d'autant plus étonner, qu'*Euler* connaissait quelques propositions qui en dérivent et desquelles il était facile de revenir à ce théorème. Il avait en effet découvert qu'il existait de certaines formes sous lesquelles se présentaient tous les diviseurs premiers de x^2-A, et d'autres qui comprenaient tous les non-diviseurs, de manière à s'exclure réciproquement; il avait même donné le moyen de les trouver. Mais il avait envain cherché à démontrer sa méthode, et ses efforts n'avaient eu d'autre fruit que de donner un plus grand degré de vraisemblance à cette proposition, qu'il avait trouvée par induction. A la vérité, dans un Mémoire lu à l'Académie de Pétersb. le 20 novembre 1775, intitulé : *Novæ*

Demonstrationes circa divisores numerorum formæ x^2+ny^2, et imprimé (*T.* 1. *nov. act. Ac. Peterb., p.* 47), il paraît croire qu'il a atteint son but; mais il s'y est glissé une erreur; car il suppose tacitement l'existence de ces formes de diviseurs et de non-diviseurs (149) : et de cette supposition il n'était pas difficile de déduire quelles devaient être ces formes; mais la méthode qu'il a employée pour démontrer cette supposition ne paraît pas convenable. Dans un autre écrit intitulé : *De Criteriis æquationis* $fx^2+gy^2=hz$ *utrumque resolutionem admittat necne* (Opusc. anal. T. 1), dans laquelle équation f, g, h sont donnés et x, y, z indéterminés; il trouve que si l'équation est résoluble pour une valeur de $h=s$, elle le sera pour tout nombre premier congru avec s, suivant le module $4fg$, proposition de laquelle on pouvait aisément déduire la supposition dont nous avons parlé. Mais la démonstration de ce théorème a toujours échappé aux recherches de ce grand géomètre (*), ce qui n'est pas étonnant, puisqu'à notre avis il fallait partir du théorème fondamental. Au reste, la vérité de cette proposition résultera naturellement de ce que nous exposerons dans la section suivante.

Après *Euler*, *Legendre* s'est livré à la même recherche, dans un excellent Traité intitulé : *Recherches d'Analyse indéterminée* (Hist. de l'Acad. des Sciences, 1785, p. 465). Il y est parvenu à un théorème qui, dans le fond, revient au théorème fondamental; savoir, que si p et q sont deux nombres premiers positifs, les résidus *minima* absolus des puissances $p^{\frac{q-1}{2}}$, $q^{\frac{p-1}{2}}$, suivant les modules q, p, respectivement, seront tous les deux $+1$ ou -1, quand l'un des deux est de la forme $4n+1$; mais que

(*) Comme il l'avoue lui-même, p. 216. « *Hujus elegantissimi theorematis demonstratio ad huc desideratur, postquàm à pluribus jamdudùm frustrà est investigata..... Quocirca plurimùm in præstitisse censendus erit, cui successerit demonstrationem hujus theorematis invenire* ». On peut voir dans les Opusc. anal. (*T.* 1, *Additamentum ad dissert.* VIII, *et T.* II, *dissert.* XIII), et dans plusieurs Dissertations des Comment. de Pétersb., avec quelle ardeur cet homme immortel a cherché la démonstration de ce théorème, et de quelques autres qui ne sont que des cas particuliers de notre théorème fondamental.

si p et q sont de la forme $4n+3$, l'un des résidus *minima* sera $+1$ et l'autre -1 (p. 516); d'où, au moyen du n° 106, il s'ensuit que la *relation* de p à q est la même que celle de q à p, quand p ou q est de la forme $4n+1$, et qu'elle est *inverse* quand p et q sont de la forme $4n+3$ (*). Cette proposition est contenue parmi celles du n° 131; elle suit aussi des propositions 1, 3, 9 du n° 133; réciproquement, le théorème fondamental peut se déduire de la proposition de *Legendre*. Ce célèbre auteur en a donné la démonstration, et comme elle est très-ingénieuse, nous en parlerons plus amplement dans la section suivante. Comme il y suppose plusieurs choses sans démonstration (ainsi qu'il en convient lui-même, p. 520 : *Nous avons supposé seulement*, etc.) dont jusqu'à présent une partie n'a été démontrée par personne, et dont l'autre partie ne peut, selon nous, l'être que par le théorème fondamental. Il nous semble que la route qu'il a prise ne peut pas lui faire éviter la difficulté, et notre démonstration peut être regardée comme la première.

Au reste, nous donnerons plus bas deux autres démonstrations de cet important théorème, absolument différentes entre elles, et de la précédente.

152. Jusqu'à présent nous n'avons traité que la congruence simple $x^n \equiv A \pmod{m}$, et nous avons appris à reconnaître les cas où elle est résoluble. Par le n° 105, la recherche des racines elles-mêmes est ramenée au cas où m est un nombre premier, ou une puissance d'un nombre premier; et par le n° 101, ce dernier cas est ramené à celui où m est un nombre premier. Quant à celui-ci, en comparant ce que nous avons dit (n°s 61 et suiv.) avec ce que nous enseignerons sect. V et VIII, on aura presque tout ce qui peut se faire par les méthodes générales. Mais dans les cas où elles sont applicables, elles sont infiniment plus longues que les méthodes indirectes que nous exposerons dans la section VI, et partant elles sont moins remarquables par leur utilité dans la pratique que par leur beauté.

(*) Le mot *relation* reçoit ici le sens que nous lui avons donné n° 146.

Les congruences complètes du second degré peuvent être ramenées facilement à des congruences simples.

Soit la congruence $ax^2+bx+c\equiv 0 \pmod{m}$; elle sera équivalente à celle-ci : $4a^2x^2+4abx+4ac\equiv 0 \pmod{4am}$. Celle-ci peut se mettre sous la forme $(2ax+b)^2\equiv b^2-4ac \pmod{4am}$, et donnera, si elle est résoluble, toutes les valeurs de $2ax+b$ moindres que $4am$. Désignant une quelconque d'entre elles par r, les solutions de la congruence proposée se déduiront de la solution de la congruence $2x\equiv r-b \pmod{4am}$, que nous avons exposée sect. II. Au reste nous observerons que le plus souvent la solution peut se simplifier par divers artifices; par exemple, on peut, au lieu de la congruence proposée, en trouver une autre, $a'x^2+2b'x+c'\equiv 0$, qui lui soit équivalente et dans laquelle a' soit divisible par m. Mais comme ces considérations, sur lesquelles on peut consulter la section VIII, alongeraient trop cette section, nous la supprimons ici.

SECTION CINQUIÈME.

Des Formes, et des Équations indéterminées du second degré.

153. Nous parlerons surtout dans cette section des fonctions de deux indéterminées de la forme $ax^2+2bxy+cy^2$, où a, b, c sont des nombres entiers donnés, fonctions que nous appellerons *formes du second degré*, ou simplement *formes*. Ces recherches nous conduiront à trouver toutes les solutions d'une équation indéterminée quelconque du second degré à deux inconnues, soit qu'on puisse en obtenir la solution en nombres entiers, ou seulement en nombres rationnels. Quoique ce problême ait déjà été résolu dans toute sa généralité par *Lagrange*, et qu'il ait trouvé plusieurs propriétés des *formes*, auxquelles il faut encore joindre celles découvertes par *Euler*, ou démontrées par lui et annoncées par *Fermat*: cependant un examen plus approfondi des *formes* nous a fait voir tant de choses nouvelles, que nous avons cru utile de reprendre ce sujet en entier, avec d'autant plus de raison que nous avons remarqué que les découvertes de ces hommes illustres, répandues dans divers ouvrages, étaient connues de peu de personnes. D'ailleurs la méthode que nous avons employée nous appartient presque en entier, et les choses que nous pouvions ajouter n'auraient pas été entendues sans une nouvelle exposition. Au reste nous placerons en temps et lieu ce qui a rapport à l'histoire des vérités remarquables.

Nous représenterons la forme $ax^2+2bxy+cy^2$ par le symbole (a, b, c), quand il ne s'agira pas des indéterminées x et y. Ainsi cette expression désignera d'une manière indéfinie la somme de trois parties, dont la première est le produit d'un nombre donné a

par le quarré d'une indéterminée quelconque, la seconde le double du produit de b et de cette indéterminée multipliée par une autre, et la troisième le produit de c par le quarré de cette seconde indéterminée. Par exemple, (1, 0, 2) exprimera la somme d'un quarré et du double d'un quarré. Au reste, quoique les formes (a, b, c) et (c, b, a) soient les mêmes, quant à leurs parties, elles diffèrent cependant si l'on fait attention à l'ordre de ces parties; aussi nous les distinguerons avec soin, et la suite fera voir l'avantage qui en résultera.

154. Nous dirons qu'un nombre donné est *représenté* par une forme donnée, si l'on peut trouver pour les indéterminées de cette forme des valeurs qui la rendent égale au nombre donné.

THÉORÈME. *Si un nombre* M *peut être représenté par la forme* (a, b, c), *de manière que les valeurs des indéterminées soient premières entre elles;* $b^2 - ac$ *sera résidu quadratique de* M.

Soit m et n les valeurs des indéterminées, et qu'on ait $am^2 + 2bmn + cn^2 = M$, et prenons les nombres μ et ν tels qu'on ait $\mu m + \nu n = 1$ (n° 40). On prouvera facilement par la multiplication, que

$$(am^2+2bmn+cn^2)(a\mu^2-2b\mu\nu+c\nu^2)=\{\mu(mb+nc)-\nu(ma+nb)\}^2-(b^2-ac)(m\mu+n\nu)^2,$$

ou

$$M(a\mu^2-2b\mu\nu+c\nu^2)=\{\mu(mb+nc)-\nu(ma+nb)\}^2-(b^2-ac);$$

donc

$$b^2-ac\equiv\{\mu(mb+nc)-\nu(ma+nb)\}^2 \pmod{M},$$

c'est-à-dire que $b^2 - ac$ est résidu quadratique de M.

Nous appellerons par la suite *déterminant* de la forme (a, b, c) le nombre $b^2 - ac$, dont nous verrons que dépendent en grande partie les propriétés de cette forme.

155. Il suit de ce qu'on vient de voir que $\mu(mb+nc)-\nu(ma+nb)$ est la valeur de l'expression $\sqrt{(b^2-ac)}$ (mod. M). Or μ et ν peuvent être déterminés d'une infinité de manières pour satisfaire à l'équation $m\mu + n\nu = 1$; il en résultera donc différentes valeurs pour cette expression; examinons quelles relations elles ont entre elles.

Soient

$$m\mu+n\nu=1,\quad m\mu'+n\nu'=1;$$
$$\mu(mb+nc)-\nu(ma+nb)=V,\quad \mu'(mb+nc)-\nu'(ma+nb)=V'$$

Si l'on multiplie la première équation par μ', la seconde par μ, et qu'on retranche l'un des résultats de l'autre, il vient $\mu'-\mu=n(\mu'\nu-\mu\nu')$; en multipliant par ν' et ν, on tirera de même $\nu'-\nu=m(\mu\nu'-\mu'\nu)$. Mais les deux dernières donnent alors

$$V'-V=(\mu'-\mu)(mb+nc)-(\nu'-\nu)(ma+nb)$$

et substituant pour $\mu'-\mu$, $\nu'-\nu$ leurs valeurs

$$V'-V=(\mu\nu'-\mu'\nu)(am^2+2bmn+cn^2)=(\mu\nu'-\mu'\nu)M\ldots \text{ ou } V'\equiv V \text{ (mod. } M).$$

Ainsi, de quelque manière que μ et ν soient déterminés, la formule $\mu(mb+nc)-\nu(ma+nb)$ ne peut donner des valeurs différentes, c'est-à-dire incongrues, de l'expression $\sqrt{(b^2-ac)}$ (mod. M). Si donc ν est une valeur quelconque de cette formule, nous dirons que la représentation du nombre M par la forme $ax^2+2bxy+cy$, dans laquelle $x=m$ et $y=n$, *appartient à la valeur* V *de l'expression* $\sqrt{(b^2-ac)}$ (*mod.* M). Au reste on peut faire voir facilement que si V est une valeur de cette formule, et que $V'\equiv V$ (mod. M), on pourra prendre à la place de μ et ν d'autres nombres μ' et ν' qui donnent V'. Il suffit de faire $\mu'=\mu+\frac{n(V'-V)}{M}$, $\nu'=\nu-\frac{m(V'-V)}{M}$, et l'on aura $\mu'm+\nu'n=\mu m+\nu n=1$; mais la valeur de la formule résultante de μ' et ν' surpassera celle qui résulte de μ et ν de la quantité $(\mu'\nu-\mu\nu')M$ qui devient $=(\mu m+\nu n)(V'-V)=V'-V$; donc cette valeur sera V'.

156. Si l'on a deux représentations du même nombre par la même forme (a, b, c), et que les valeurs des indéterminées soient premières entre elles, elles peuvent appartenir à la même valeur de l'expression $\sqrt{(b^2-ac)}$ (mod. M), ou à des valeurs différentes.

Soit

$$M=am^2+2bmn+cn^2=am'^2+2bm'n'+cn'^2,\quad \text{et}\quad \mu m+\nu n=1,\quad \mu'n'+\nu'm'=1;$$

il est clair que si l'on a

$$\mu(mb+nc)-\nu(ma+nb)\equiv\mu'(m'b+n'c)-\nu'(m'a+n'b)\ \text{(mod. } M),$$

la congruence aura toujours lieu quelques valeurs convenables que l'on prenne pour μ et ν, μ' et ν', auquel cas nous dirons que la représentation

représentation du nombre M appartient à la même valeur de l'expression $\sqrt{(b^2-ac)}$ (mod. M).

Mais si pour quelques valeurs de μ et ν, μ' et ν', cette congruence n'a pas lieu, elle n'aura lieu pour aucune, et les représentations appartiendront à des valeurs *différentes*. Et, si l'on avait

$$\mu(mb+nc)-\nu(ma+nb)\equiv-\{\mu'(m'b+n'c)-\nu'(m'a+n'b)\},$$

nous dirions que les représentations appartiennent à des valeurs *opposées*. Nous nous servirons de toutes ces dénominations lorsqu'il s'agit de plusieurs représentations du même nombre par des formes différentes, mais qui ont le même déterminant.

Exemple. Soit $(3, 7, -8)$ la forme proposée dont le déterminant $=73$. Elle donne pour le nombre 57 les représentations suivantes : $3.13^2+14.13.25-8.25^2$; $3.5^2+14.5.9-8.9^2$. Pour la première on peut prendre $\mu=2$, $\nu=-1$, d'où résulte la valeur de $\sqrt{73}$ (mod. 57), à laquelle la représentation appartient $=2(13.7+25.8)+(13.3+25.7)=-4$. De la même manière, en faisant $\mu=2$, $\nu=-1$, on trouve que la seconde représentation appartient à la valeur $+4$. Donc les deux représentations appartiennent à des valeurs opposées.

Avant d'aller plus loin, nous observerons que les formes dont le déterminant est zéro doivent être exclues des considérations suivantes, parcequ'elles nuiraient à l'élégance des théorèmes, et qu'elles exigent qu'on les traite en particulier.

157. Si la forme F, dont les indéterminées sont x, y, peut être changée en une autre F', dont les indéterminées soient x', y', en y substituant $x=\alpha x'+\beta y'$, $y=\gamma x'+\delta y'$, α, β, γ, δ étant des nombres entiers, nous dirons que la première *renferme* la seconde, ou que la seconde est *contenue dans la première*.

Soient $F=ax^2+2bxy+cy^2$, $F'=a'x'^2+2b'x'y'+c'y'^2$.

On aura les trois équations suivantes :

$$a'=a\alpha^2+2b\alpha\gamma+c\gamma^2,\quad b'=a\alpha\beta+b(\alpha\delta+\beta\gamma)+c\gamma\delta,\quad c'=a\beta^2+2b\beta\delta+c\delta^2.$$

Multipliant la seconde par elle-même, la première par la troisième, et retranchant, il vient

$$b'^2-a'c'=(b^2-ac)(\alpha\delta-\beta\gamma)^2;$$

d'où il suit que le déterminant de la forme F' est divisible par celui de la forme F, et que le quotient est un quarré; ainsi ces déterminans seront de même signe. Si, de plus, la forme F' pouvait être changée en la forme F par une transformation semblable, c'est-à-dire, si F' était contenue sous F et F sous F', les déterminans seraient égaux et $(\alpha\delta - \beta\gamma)^2 = 1$. Dans ce cas, nous les appellerons formes *équivalentes*. L'égalité des déterminans est une condition nécessaire pour l'équivalence des formes, mais il s'en faut bien qu'elle soit suffisante.

L'analyse précédente fait voir clairement que la même chose aura lieu pour les formes dont le déterminant est $= 0$; mais l'équation $(\alpha\delta - \beta\gamma)^2 = 1$ ne peut pas s'étendre à ce cas-là.

Nous nommerons la substitution *transformation propre*, quand $\alpha\delta - \beta\gamma > 0$, et *transformation impropre*, quand $\alpha\delta - \beta\gamma < 0$, et la forme F sera dite contenue *proprement* ou *improprement* dans la forme F' selon que F pourra être transformée en F' par une transformation *propre* ou *impropre*. Si donc F et F' sont équivalentes, la transformation sera propre ou impropre, suivant que $\alpha\delta - \beta\gamma = \pm 1$. Si plusieurs transformations sont toutes propres ou toutes impropres, elles seront *semblables;* mais une forme propre et une formee impropre seront *dissemblables*.

158. *Si les déterminans de deux formes* F *et* F′ *sont égaux, et que* F′ *soit contenue sous* F, F *sera aussi contenue sous* F′ *et le sera proprement ou improprement, suivant que* F′ *sera contenue sous* F *proprement ou improprement.*

Supposons que F devienne F' en posant $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$; F' deviendra F en posant $x' = \delta x - \beta y$, $y' = -\gamma x + \alpha y$. Car on déduira par là de F' le même résultat qu'en substituant dans F, à la place de x et de y, $\alpha(\delta x - \beta y) + \beta(+\alpha y - \gamma x)$ et $\gamma(\delta x - \beta y) + \delta(+\alpha y - \gamma x)$, qui reviennent à $(\alpha\delta - \beta\gamma)x$ et $(\alpha\delta - \beta\gamma)y$. Or ce résultat serait évidemment $(\alpha\delta - \beta\gamma)^2 F = F$, puisque par hypothèse $(\alpha\delta - \beta\gamma)^2 = 1$. Or il est aisé de voir que la seconde transformation est propre ou impropre en même temps que la première.

Si F' est contenu proprement dans F, et F proprement dans F', nous dirons que ces formes sont *proprement équivalentes;* et si elles

se contiennent improprement, nous dirons qu'elles sont *improprement équivalentes*. On verra bientôt l'utilité de ces distinctions.

Exemple. Par la substitution $x=2x'+y'$, $y=3x'+2y'$, la forme $2x^2-8xy+3y^2$ devient $-13x'^2-12x'y'-2y'^2$; et celle-ci se change en la première, par la substitution $x'=2x-y$, $y'=-3x+2y$. Donc les formes $(2, -4, +3)$ et $(-13, -6, -2)$ sont proprement équivalentes.

Nous allons maintenant nous occuper des problèmes suivans :

1°. Étant données deux formes quelconques qui ont le même déterminant, chercher si elles sont équivalentes ou non, si elles le sont proprement ou improprement, ou des deux manières à-la-fois, ce qui est possible. Quand elles ont des déterminans inégaux, chercher si l'une ne renferme pas l'autre, proprement, improprement, ou des deux manières. Enfin trouver toutes les transformations tant propres qu'impropres de l'une dans l'autre.

2°. Étant donnée une forme quelconque, trouver si un nombre donné peut être représenté par elle, et assigner toutes les représentations.

Mais comme les formes dont le déterminant est négatif exigent une autre méthode que celles dont le déterminant est positif, nous présenterons d'abord ce qu'il y a de commun aux deux cas, que nous considérerons ensuite séparément.

159. *Si la forme* F *renferme la forme* F', *et que la forme* F' *renferme la forme* F'', F *renfermera* F''.

Soient x, y; x', y'; x'', y'' les indéterminées des formes F, F', F'' respectivement, que F devienne F' en posant $x=\alpha x'+\beta x'$, $y=\gamma x'+\delta y'$, et que F devienne F'' en posant $x'=\alpha' x''+\beta' y''$, $y'=\gamma' x''+\delta' x''$. Il est clair que F se changera en F'', en faisant $x=\alpha(\alpha' x''+\beta' y'')+\beta(\gamma' x''+\delta' y'')=(\alpha\alpha'+\beta\gamma')x''+(\alpha\beta'+\beta\delta')y''$, et $y=\gamma(\alpha' x''+\beta' y'')+\delta(\gamma' x''+\delta' y'')=(\alpha'\gamma+\delta\gamma')x''+(\beta'\gamma+\delta\delta')y''$: donc F renfermera F''.

Comme $(\alpha\alpha'+\beta\gamma')(\beta'\gamma+\delta\delta')-(\alpha\beta'+\beta\delta')(\alpha'\gamma+\gamma'\delta)\ldots$ $=(\alpha\delta-\beta\gamma)(\alpha'\delta'-\beta'\gamma')$, qui sera positif si les deux facteurs sont de même signe, et négatif dans le cas contraire, la forme F

renfermera donc F'' *proprement*, si F renferme F', et F', F'' de la même manière, soit *proprement* ou non, et la forme F renfermera F'' *improprement*, dans le cas contraire.

Il suit de là que si l'on a tant de formes F, F', F'', F''', etc. qu'on voudra, telles que chacune renferme la suivante, la première renfermera la dernière, et la renfermera *proprement* ou *improprement*, suivant que le nombre des formes qui renferment la suivante improprement sera pair ou impair.

Si la forme F *est équivalente à la forme* F', *et la forme* F' *à la forme* F'', *la forme* F *sera équivalente à la forme* F'', *et le sera proprement ou improprement, suivant que* F *et* F', F' *et* F'' *seront équivalentes de la même manière ou d'une manière différente.*

En effet, puisque F, F' sont équivalentes aux formes F', F'' respectivement, les premières renferment les dernières, et partant F renferme F''; mais les dernières renferment aussi les premières, donc F et F'' sont équivalentes. Or, de ce que nous avons vu tout-à-l'heure, il suit que F renferme F'' proprement ou improprement, suivant que F et F', F' et F'' sont équivalentes de même ou de différente manière, et il en est de même de F'' et F; donc, dans le premier cas, F et F'' sont proprement équivalentes, et dans le second, improprement.

Les formes (a, —b, c), (c, b, a), (c, —b, a) *sont équivalentes à la forme* (a, b, c), *savoir, les deux premières improprement et la dernière proprement.*

En effet $ax^2+2bxy+cy^2$ se change en $ax'^2-2bx'y'+cy'^2$, en faisant $x=x'+0.y'$ et $y=0.x'-y'$, ce qui donne $\alpha\delta-\beta\gamma=-1$, et partant, la transformation est impropre; elle se change en $cx'^2+2bx'y'+ay'^2$ par la transformation impropre $x=0.x'+y'$, $y=x'+0.y'$, et en $cx'^2-2bx'y+ay'^2$ par la transformation propre $x=0.x'-y'$, $y=x'+0.y$.

Il suit de là qu'une forme quelconque équivalente à (a, b, c) est proprement équivalente à cette forme ou à la forme $(a, -b, c)$. De même, si une certaine forme renferme la forme (a, b, c), où y est contenue, elle renferme proprement l'une des deux formes

(a, b, c), $(a, -b, c)$, ou bien elle est renfermée proprement dans l'une des deux. Les formes (a, b, c), $(a, -b, c)$ s'appelleront formes *opposées*.

160. Si les formes (a, b, c), (a', b', c') ont le même déterminant, et qu'on ait $c = a'$ et $b + b' \equiv 0 \pmod{c}$, nous dirons qu'elles sont *contiguës*, et quand une désignation plus exacte sera nécessaire, nous dirons que la première est contiguë à la seconde *par la première partie*, et que la seconde est contiguë à la première *par la dernière partie*.

Ainsi la forme $(7, 3, 2)$ est contiguë à la forme $(3, 4, 7)$ par la dernière partie, la forme $(3, 1, 3)$ est contiguë par les deux parties à son opposée $(3, -1, 3)$.

Les formes contiguës sont toujours proprement équivalentes.

Car la forme $ax^2 + 2bxy + cy^2$ se change en la forme contiguë $cx'^2 + 2b'x'y' + c'y'^2$ en faisant $x = -y'$ et $y = x' + \frac{b+b'}{c} y'$ (où, par hypothèse, $\frac{b+b'}{c}$ est un entier), comme on s'en assurera par le développement. Or $o \cdot \frac{b+b'}{c} - 1 \cdot (-1) = 1$; donc la transformation est propre. Au reste, ces définitions et ces conclusions n'auraient plus lieu si $c = a' = 0$; mais ce cas n'arrive que lorsque le déterminant des formes est un quarré.

Il suit de là que les formes (a, b, c), (a', b', c') sont proprement équivalentes, si $a = a'$ et $b \equiv b' \pmod{a}$, car la première est proprement équivalente à $(c, -b, a)$ (n° précéd.); or celle-ci est contiguë par la première partie à la forme (a', b', c').

161. *Si la forme* (a, b, c) *renferme la forme* (a', b', c'), *tout diviseur commun des nombres* a, b, c, *le sera aussi des nombres* a', b', c', *et tout diviseur commun de* a, 2b, c, *le sera aussi de* a', 2b', c'.

L'inspection des trois équations du n° 157 suffit pour le démontrer, en ayant soin de multiplier la seconde par 2 pour la seconde partie de la proposition.

Il suit de là que le plus grand commun diviseur des nombres a, b, $(2b)$, c doit diviser celui des nombres a', b', $(2b')$, c'.

Si donc les formes sont équivalentes, ces deux plus grands communs diviseurs sont égaux, puisqu'ils doivent se diviser mutuellement, et si dans ce cas l'un des deux groupes n'a pas de commun diviseur, l'autre n'en aura pas non plus.

162. PROBLÈME. *Si la forme* $AX^2+2BXY+CY^2\ldots F$ *renferme la forme* $ax^2+2bxy+cy^2\ldots f$, *et qu'on connaisse une quelconque des transformations, déduire de celle-là toutes les transformations qui lui sont semblables.*

Soit la transformation donnée, $X=\alpha x+\beta y$, $Y=\gamma x+\delta y$; supposons d'abord qu'on en connaisse encore une autre semblable, $X=\alpha' x+\beta' y$, $Y=\gamma' x+\delta' y$, et examinons ce qui doit en résulter. Nommons D, d les déterminans des formes F, f, faisons $\alpha\delta-\beta\gamma=e$, $\alpha'\delta'-\beta'\gamma'=e'$, on aura (n° 157) $d=De^2=De'^2$, et partant $e=e'$, puisque e et e' sont de même signe par hypothèse.

Or on aura les six équations suivantes :

$$A\alpha^2+2B\alpha\gamma+C\gamma^2=a\ldots\ldots(1) \qquad A\alpha'^2+2B\alpha'\gamma'+C\gamma'^2=a\ldots\ldots(2)$$
$$A\alpha\beta+B(\alpha\delta+\beta\gamma)+C\gamma\delta=b\ldots(3) \qquad A\alpha'\beta'+B(\alpha'\delta'+\beta'\gamma')C\gamma'\delta'=b\ldots(4)$$
$$A\beta^2+2B\beta\delta+C\delta^2=c\ldots\ldots(5) \qquad A\beta'^2+2B\beta'\delta'+C\delta'^2=c\ldots\ldots(6).$$

Si l'on multiplie la première par la seconde, on en déduira

$$(A\alpha\alpha'+B(\alpha\gamma'+\alpha'\gamma)+C\gamma\gamma')^2-D(\alpha'\gamma-\alpha\gamma')^2=a^2,$$

ou si l'on fait $A\alpha\alpha'+B(\alpha\gamma'+\alpha'\gamma)+C\gamma\gamma'=a'\ldots$

$$a'^2-D(\alpha'\gamma-\alpha\gamma')^2=a^2\ldots(7).$$

Si l'on multiplie la première par la quatrième, et la seconde par la troisième, et qu'on ajoute, on trouvera

$$a'\{A(\alpha\beta'+\alpha'\beta)+B(\alpha\delta'+\alpha'\delta+\beta\gamma'+\beta'\gamma)+C(\gamma\delta'+\delta'\gamma)\}$$
$$-D(\alpha\gamma'+\alpha'\gamma)(\alpha\delta'-\alpha'\delta+\beta\gamma'-\beta'\gamma)=2ab,$$

ou en représentant $A(\alpha\beta'+\alpha'\beta)+B(\alpha\delta'+\alpha'\delta+\beta\gamma'+\beta'\gamma)\ldots$ $+C(\gamma\delta'+\delta'\gamma)$ par $2b'$,

$$2a'b'-D(\alpha\gamma'-\alpha'\gamma)(\alpha\delta'-\alpha'\delta+\beta\gamma'-\beta'\gamma)=2ab\ldots\ldots(8).$$

Si l'on multiplie la première par la sixième, la seconde par la cinquième, la troisième par la quatrième, et qu'on ajoute les deux premiers produits et le double du troisième, on trouve

$$4b'^2-D\{(\alpha\delta'-\alpha'\delta+\beta\gamma'-\beta'\gamma)^2+ee'\}=2b^2+2ac,$$

ou bien comme $2Dee' = 2d = 2b^2 - ac$.....

$$4b'^2 - D(\alpha\delta' - \alpha'\delta + \beta\gamma' - \beta'\gamma)^2 = 4b^2 \text{.....(9).}$$

Si l'on multiplie la troisième par la quatrième, il vient

$$a'(A\beta\beta' + B(\beta\delta' + \beta'\delta) + C\delta\delta') - D(\alpha\delta' - \gamma\beta')(\beta\gamma' - \alpha'\delta) = b^2,$$

et comme $D(\alpha\delta' - \gamma\beta')(\beta\gamma' - \alpha'\delta) = D(\alpha\gamma' - \alpha'\gamma)(\beta\delta' - \beta'\delta) - D(\alpha\delta - \beta\gamma)(\alpha'\delta' - \beta'\gamma) = D(\alpha\gamma' - \alpha'\gamma)(\beta\delta' - \beta'\delta) - b^2 + ac$, si l'on fait d'ailleurs $A\beta\beta' + B(\beta\delta' + \beta'\delta) + C\delta\delta' = c'$, on aura

$$a'c' - D(\alpha\gamma' - \alpha'\gamma)(\beta\delta' - \beta'\delta) = ac \text{.....(10);}$$

en ajoutant le produit de la troisième par la sixième à celui de la quatrième et de la cinquième, on aura

$$2b'c' - D(\alpha\delta' - \alpha'\delta + \beta\gamma' - \beta'\gamma)(\beta\delta' - \beta'\delta) = 2bc \text{.....(11);}$$

en multipliant la cinquième par la sixième, on trouvera

$$c'^2 - D(\beta\delta' - \beta'\delta)^2 = e^2 \text{.....(12).}$$

Supposons maintenant que m soit le plus grand commun diviseur des nombres a, $2b$, c, et que les nombres A', B', C' soient déterminés de manière qu'on ait $A'a + 2B'b + C'c = m$ (n° 40). Multiplions les équations (7), (8), (9), (10), (11), (12), respectivement par A'^2, $2A'B'$, B'^2, $2A'C'$, $2B'C'$, C'^2, et ajoutons les produits, en faisant pour abréger,

$$A'a' + 2B'b' + C'c' = T \text{.....(13)}$$

et $A'(\alpha\gamma' - \alpha'\gamma) + B'(\alpha\delta' - \alpha'\delta + \beta\gamma' - \beta'\gamma) + C'(\beta\delta' - \beta'\delta) = U$...(14),

on trouve $T^2 - DU^2 = m^2$, T et U étant manifestement entiers.

Nous sommes donc conduits à cette conclusion élégante, *que la solution de l'équation indéterminée* $t^2 - Du^2 = m^2$ *en nombres entiers dépend de deux transformations quelconques semblables de la forme* F *en la forme* f, en prenant $t = T$, $u = U$. Au reste, comme dans nos raisonnemens nous n'avons pas supposé que les transformations fussent différentes, une seule transformation prise deux fois doit donner une solution; mais alors $\alpha' = \alpha$, $\beta' = \beta$, etc., $a' = a$, $b' = b$, etc., et partant $T = m$ et $U = 0$, solution qui se présentait d'elle-même.

Considérons maintenant comme connue la première transformation, et la solution de l'équation indéterminée, et cherchons

comment on peut en déduire l'autre transformation, ou comment α', β', γ', δ' dépendent de α, β, γ, δ, T et U.

Pour y parvenir, multiplions d'abord l'équation (1) par $\alpha'\delta-\beta\gamma'$, l'équation (2) par $\alpha\delta'-\beta'\gamma$, l'équation (3) par $\alpha\gamma'-\alpha'\gamma$, et l'équation (4) par $\alpha'\gamma-\alpha\gamma'$, et ajoutons les produits, il en résultera

$$(e+e')a'=(\alpha\delta'+\alpha'\delta-\beta\gamma'-\beta'\gamma)a.....(15).$$

De même si nous multiplions (1)—(2) par $\beta'\delta-\beta\delta'$, (3)+(4) par $(\alpha\delta'+\alpha'\delta-\beta\gamma'-\beta'\gamma)$ et (5)—(6) par $(\alpha\gamma'-\alpha'\gamma)$, nous aurons en ajoutant,

$$2(e+e')b'=2(\alpha\delta'+\alpha'\delta-\beta\gamma'-\beta'\gamma)b.....(16).$$

Enfin si nous multiplions (3)—(4) par $\delta\beta'-\beta\delta'$, (5) par $\alpha\delta'-\beta'\gamma$, et (6) par $\alpha'\delta-\beta\gamma'$, on aura en ajoutant les produits,

$$(e+e')c'=(\alpha\delta'+\alpha'\delta-\beta\gamma'-\beta'\gamma)c.....(17).$$

Substituant ces valeurs de a', b', c' dans l'équation (13), il vient

$$(e+e')T=(\alpha\delta'+\alpha'\delta-\beta\gamma'-\beta'\gamma)(A'a+2B'b+C'c)...$$
$$\text{ou}\quad 2eT=(\alpha\delta'+\alpha'\delta-\beta\gamma'-\beta'\gamma)m.....(18);$$

d'où l'on peut tirer la valeur de T plus facilement que de l'équation (13).

Combinant cette équation avec les équations (15), (16), (17), on en tire

$$ma'=Ta,\qquad 2mb'=2Tb,\qquad mc'=Tc.$$

Ces valeurs substituées dans les équations (7), etc. (12), en y mettant d'ailleurs m^2+DU^2 pour T^2, elles deviennent

$$(\alpha\gamma'-\alpha'\gamma)^2m^2=a^2U^2$$
$$(\alpha\gamma'-\alpha'\gamma)(\alpha\delta'-\alpha'\delta+\beta\gamma'-\beta'\gamma)m^2=2abU^2$$
$$(\alpha\delta'-\alpha'\delta+\beta\gamma'-\beta'\gamma)^2m^2=4b^2U^2$$
$$(\alpha\gamma'-\alpha'\gamma)(\beta\delta'-\beta'\delta)m^2=acU^2$$
$$(\alpha\delta'-\alpha'\delta+\beta\gamma'-\beta'\gamma)(\beta\delta'-\beta'\delta)m^2=2bcU^2$$
$$(\beta\delta'-\beta'\delta)^2m^2=c^2U^2.$$

De là, à l'aide de l'équation (14) et de celle-ci $A'a+2B'b+C'c=m$, on déduit facilement, en multipliant la 1re, la 2e et la 4e; la 2e, la 3e et la 5e; la 4e, la 5e et la 6e par A', B', C' respectivement, et en

en ajoutant les produits

$(\alpha\gamma'-\alpha'\gamma)Um^2=maU^2$, $(\alpha\delta'-\alpha'\delta+\beta\gamma'-\beta'\gamma)Um^2=2mbU^2$, $(\beta\delta'-\beta'\delta)Um^2=mcU^2$,

équations qui, divisées par mU (*), deviennent

$$aU=m(\alpha\gamma'-\alpha'\gamma)\ldots\ldots\ldots\ldots\ldots\ldots(19)$$
$$2bU=m(\alpha\delta'-\alpha'\delta+\beta\gamma'-\beta'\gamma)\ldots\ldots\ldots(20)$$
$$cU=m(\beta\delta'-\beta'\delta)\ldots\ldots\ldots\ldots\ldots\ldots(21)$$

dont une quelconque peut donner la valeur de U plus facilement que l'équation (14). Il suit aussi de là que de quelque manière qu'on détermine A', B', C', et ces quantités peuvent être déterminées par plusieurs méthodes différentes, on aura toujours les mêmes valeurs, pour T et ponr U

Or en combinant l'équation (18) avec l'équation (20), on en tire par soustraction et par addition les deux suivantes

$$eT-bU=m(\alpha'\delta-\beta\gamma')\ldots\ldots\ldots\ldots(22)$$
$$eT+bU=m(\alpha\delta'-\beta'\gamma)\ldots\ldots\ldots\ldots(23),$$

et à l'aide des quatre équations (19), (21), (22), (23), qui ne sont que dupremier degré, on obtiendra sans peine les valeurs de α', β', γ', δ', au moyen des équations suivantes qui en dérivent,

$$me\alpha'=\alpha eT+(a\beta-b\alpha)U, \qquad me\beta'=\beta eT+(b\beta-c\alpha)U,$$
$$me\gamma'=\gamma eT+(a\delta-b\gamma)U, \qquad me\delta'=\delta eT+(b\delta-c\gamma)U,$$

ou, en y substituant les valeurs de a, b, c, tirées des équations (1), (3), (5),

$$m\alpha'=\alpha T-(B\alpha+C\gamma)U, \qquad m\beta'=\beta T-(B\beta+C\delta)U;$$
$$m\gamma'=\gamma T+(A\alpha+B\gamma)U, \qquad m\delta'=\delta T+(A\beta+B\delta)U.$$

Il suit de l'analyse précédente, qu'il n'y a pas de transformation de F en f, semblable à la proposée, qui ne soit contenue dans les formules

$$\left.\begin{aligned} X&=\tfrac{1}{m}\{\alpha t-(B\alpha+C\gamma u\}x+\tfrac{1}{m}\{\beta t-(B\beta+C\delta)u\}y \\ Y&=\tfrac{1}{m}\{\gamma t+(A\alpha+B\gamma)u\}x+\tfrac{1}{m}\{\delta t+(A\beta+B\delta)u\}y \end{aligned}\right\}\ldots\ldots\ldots(I),$$

(*) Cette division ne serait pas possible si l'on avait $U=0$; mais alors les équations (19), (20), (21) naîtraient immédiatement de la première, de la troisième et de la sixième des équations précédentes.

t et u désignant indéfiniment tous les nombres qui satisfont à l'équation $t^2 - Du^2 = m^2$. Nous ne pouvons pas encore conclure que toutes les valeurs de t et de u qui satisfont à cette équation donnent des transformations convenables, lorsqu'on les substitue dans les formules (I). Mais,

1°. On s'assurera par le développement, que la susbtitution de valeurs quelconques de t et de u change F en f, au moyen des équations (1), (3), (5) et $t^2 - Du^2 = m^2$. Nous omettons, ce calcul plus long que difficile.

2°. Toute transformation déduite des formules sera semblable à la proposée; car

$$\frac{1}{m}\{\alpha t-(B\alpha+C\gamma)u\}\times\frac{1}{m}\{\delta t+(A\beta+B\delta)u\}-\frac{1}{m}\{\beta t-(B\beta+C\delta)u\}$$
$$\times\frac{1}{m}\{\gamma t+(A\alpha+B\gamma)u\}=\frac{1}{m^2}(\alpha\delta-\beta\gamma)(t^2-Du^2)=\alpha\delta-\beta\gamma.$$

3°. Si les formes F et f ont des déterminans inégaux, il peut se faire que les formules (I) renferment des fractions, par la substitution de certaines valeurs de t et de u, et que partant il faille les rejeter: mais toutes les autres seront des transformations convenables, et seront les seules.

4°. Si les formes F et f ont des déterminans égaux, et que parconséquent elles soient équivalentes, les formules (I) ne pourront jamais donner de transformations qui renferment des fractions, et parconséquent elles donnent la solution complète du problême.

En effet, par le théorême du n° précédent, on sait que dans ce cas m sera aussi diviseur commun de A, $2B$, C; or puisque $t^2 - Du^2 = m^2$, on a $t^2 - B^2u^2 = m^2 - ACu^2$; donc $t^2 - B^2u^2$ sera divisible par m^2, et partant, $4t^2 - 4B^2u^2$, ou, puisque $2B$ est divisible par m, $4t^2$ sera divisible par m^2 ou $2t$ par m. Donc $\frac{2}{m}(t+Bu)$ et $\frac{2}{m}(t-Bu)$ seront entiers, et partant, comme la différence $\frac{4Bu}{m}$ de ces deux quantités est paire, elles seront ou toutes deux impaires, ou toutes deux paires; si elles étaient impaires,

leur produit $\frac{4}{m^2}(t^2-B^2u^2)$ le serait aussi; mais puisque $t^2-B^2u^2$ est divisible par m^2, ce produit est nécessairement pair; donc cette supposition ne peut subsister, et les deux quantités sont paires, donc leurs moitiés $\frac{1}{m}(t+Bu)$, $\frac{1}{m}(t-Bu)$ sont des entiers, et parconséquent $\frac{t}{m}$ et $\frac{Bu}{m}$. Il suit de là, sans difficulté, que les quatre coefficiens des formules (I) sont toujours entiers.

Concluons de ce qui précède, que si l'on connaît toutes les solutions de l'équation $t^2-Du^2=m^2$, on en déduira toutes les transformations de la forme (A, B, C) en (a, b, c), semblables à une transformation proposée. Nous donnerons plus loin le moyen de trouver les solutions de cette équation; observons seulement ici que leur nombre est fini quand D est négatif, ou positif et en même temps un quarré; mais qu'il est infini, si D est positif et non un quarré. Quand ce cas a lieu, et qu'on n'a pas $D=d$ (Voyez 3°.), il faudrait encore chercher comment on peut, *à priori*, distinguer les valeurs de t et de u qui donnent des transformations entières, et celles qui n'en donnent pas. Mais nous donnerons plus bas, pour ce cas-là, une autre méthode qui n'aura pas le même inconvénient (n° 214).

Exemple. La forme x^2+y^2 se change par la transformation propre $x=2x'+7y'$, $y=x'+5y'$, en (6, 24, 99). On demande toutes les transformations propres de (1, 0, 2) en (6, 24, 99). Ici $D=-2$, $m=3$; ainsi l'équation à résoudre est $t^2+2u^2=9$. On peut y satisfaire de six manières: $t=3\ldots u=0$, $t=-3\ldots u=0$, $t=1\ldots u=2$, $t=1\ldots u=-2$, $t=-1\ldots u=2$, $t=-1\ldots u=-2$. La 3ᵉ et la 6ᵉ donnent des résultats fractionnaires et sont parconséquent à rejeter des autres. Résultent les quatre substitutions:

$$x=\begin{cases} 2x'+7y' \\ -2x'+7y' \\ 2x'+9y' \\ -2x'+9y' \end{cases} \qquad y=\begin{cases} x'+5y' \\ -x'+5y' \\ x'+3y' \\ -x'+3y' \end{cases}$$

dont la première est la solution proposée.

163. Nous avons dit plus haut, en passant, qu'il pouvait arriver

qu'une forme F en renfermât une autre F', tant proprement qu'improprement. On voit que cela aura lieu, si l'on peut interposer une autre forme G, telle que F renferme G, et que G renferme F', et que la forme G soit de nature à être proprement équivalente à elle-même. Car si l'on suppose que F renferme G proprement ou improprement, comme G se renferme lui-même improprement, F renfermera G improprement ou proprement, selon la supposition primitive, et partant le renfermera dans les deux cas, proprement ou improprement (n° 159). On trouvera de même que de quelque manière que G renferme F', F doit toujours renfermer F' des deux manières. Or on reconnaît qu'il existe des formes improprement équivalentes à elles-mêmes par un cas très-évident, celui de la forme (a, o, c), qui se change en (a, o, c) en faisant $x = x' + o.y'$ et $y = o.x' - y'$. Plus généralement, toute forme (a, b, c) jouit de cette propriété lorsque $2b$ est divisible par a; en effet la forme (c, b, a) est contiguë à (a, b, c) par la première partie (n° 160), et partant lui est proprement équivalente, mais (c, b, a) (n° 159) équivaut improprement à (a, b, c); donc (a, b, c) équivaut improprement à elle-même. Nous nommerons formes *ambiguës* les formes (a, b, c) dans lesquelles $2b$ est divisible par a. Nous avons donc le théorème suivant:

La forme F *renfermera la forme* F′ *proprement et improprement, si on peut trouver une forme ambiguë que* F *renferme et qui renferme* F′.

La réciproque est également vraie, et c'est l'objet du numéro suivant.

164. Théorème. *Si la forme* $Ax^2 + 2Bxy + Cy^2 \ldots (F)$, *renferme tant proprement qu'improprement la forme* $A'x'^2 + 2B'x'y + C'y'^2 \ldots (F')$, *on pourra trouver une forme ambiguë que* F *renfermera et qui renfermera* F′.

Supposons que F devienne F' par la substitution $x = \alpha x' + \beta' y$, $y = \gamma x' + \delta' y$, et par la substitution dissemblable $x = \alpha' x' + \beta' y'$, $y = \gamma' x' + \delta' y'$. Soit $\alpha\delta - \beta\gamma = e$, $\alpha'\delta' - \beta'\gamma' = e$, on aura $B'^2 - AC = e^2(B^2 - AC) = e'^2(B^2 - AC)$; donc $e^2 = e'^2$, et comme e et e' sont de signe contraire $e = -e'$ ou $e + e' = 0$; or il est clair

qu'on arrivera à la même forme en substituant dans F', pour x', $\delta''x''-\beta'y''$, pour y', $-\gamma'x''+\alpha'y''$, qu'en substituant dans F

ou bien $\begin{cases}\text{pour } x\ldots\alpha(\delta''x''-\beta'y'')+\beta(-\gamma'x''+\alpha'y'')=(\alpha\delta''-\beta\gamma')x''+(\alpha'\beta-\alpha\beta')y''\\ \text{pour } y\ldots\gamma(\delta''x''-\beta'y'')+\delta(-\gamma'x''+\alpha'y'')=(\gamma\delta''-\gamma'\delta)x''+(\alpha'\delta-\beta'\gamma)y''.\end{cases}$

ou bien $\begin{cases}\text{pour } x\ldots\alpha'(\delta''x''-\beta'y'')+\beta'(-\gamma'x''+\alpha'y'')=(\alpha'\delta''-\beta'\gamma')x''=e'x''\\ \text{pour } y\ldots\gamma'(\delta''x''-\beta'y'')+\delta''(-\gamma'x''+\alpha'y'')=(\alpha'\delta''-\beta'\gamma')x''=e'y''.\end{cases}$

Ainsi en faisant

$$\alpha\delta''-\beta\gamma'=a,\ \alpha'\beta-\alpha\beta'=b,\ \gamma\delta''-\gamma'\delta=c,\ \alpha'\delta-\beta'\gamma=d,$$

la forme F se changera en une même forme par les substitutions $x=ax''+by''$, $y=cx''+dy''$ et $x=e'x''$, $y=e'y''$, ce qui donne les trois équations suivantes :

$$Aa^2+2Bac+Cc^2=Ae'^2\ldots\ldots\ldots\ldots\ldots(1),$$
$$Aab+B(ad+bc)+Ccd=Be'^2\ldots\ldots\ldots(2),$$
$$Ab^2+2Bbd+Cd^2=Ce'^2\ldots\ldots\ldots\ldots\ldots(3);$$

mais des valeurs de a, b, c, d, on tire

$$ad-bc=ee'=-e^2=-e'^2\ldots\ldots\ldots\ldots(4).$$

Si l'on multiplie l'équation (1) par d, l'équation (2) par c, et qu'on retranche, on trouve $(Aa+Bc)(ad-bc)=(Ad-Bc)e'^2$, et partant $A(a+d)=0$.

En multipliant l'équation (2) par $a+d$, et en retranchant le produit de l'équation (1) par b et de l'équation (3) par c, on trouve $(Ab+B(a+d)+Cc)(ad-bc)=(-Ab+B(a+d)-Cc)e'^2$, d'où $B(a+d)=0$.

Enfin en retranchant du produit de l'équation (3) par c celui de l'équation (2) par b, on trouve $(Bb+Cd)(ad-bc)=(-Bb+Ca)e'^2$, d'où $C(a+d)=0$. Or comme A, B, C ne peuvent dans aucun cas être nuls en même temps, il s'ensuit que

$$a+d=0\ldots\ldots\ldots\ldots\ldots(5).$$

Si l'on multiplie l'équation (2) par a, et qu'on en retranche l'équation (1) multipliée par b, il vient $(Ba+Cc)(ad+bc)=(Ba-Ab)e'^2$, d'où

$$Ab-2Ba-Cc=0\ldots\ldots\ldots(6).$$

Des équations : $e+e'=0$, $a+d=0$, ou $\alpha\delta-\beta\gamma+\alpha'\delta'-\beta'\gamma'=0$ et $\alpha\delta'+\alpha'\delta-\beta\gamma'-\beta'\gamma=0$, on déduit $(\alpha+\alpha')(\delta+\delta')=(\beta+\beta')(\gamma+\gamma')$,

ou $(\alpha+\alpha'):(\gamma+\gamma')=(\beta+\beta'):(\delta+\delta')$. Représentons par $\frac{m}{n}$ ce rapport, réduit à sa plus simple expression, de manière que m et n soient premiers entre eux (*), et soient pris μ, ν desorte qu'on ait $\mu m+\nu n=1$. Soit d'ailleurs r le plus grand commun diviseur de a, b, c, son quarré divisera $bc+a^2=bc+ad=-e^2$; donc r divisera e. Cela posé, si la forme F, par la transformation $x=mt+\frac{\nu e}{r}u$, $y=nt-\frac{\mu e}{r}u$, se change en $Mt^2+2Ntu+Pu^2\ldots(G)$, cette forme G sera ambiguë et renfermera F'.

Démonstration. I. Pour faire voir que la forme G est ambiguë, nous démontrerons que $M(b\mu^2-2a\mu\nu-c\nu^2)=2Nr$; car alors r divisant a, b, c; $\frac{1}{r}(b\mu^2-2a\mu\nu-c\nu^2$ sera entier, et partant $2N$ un multiple de M.

Or $M=Am^2+2Bmn+Cn^2$, $Nr=(Am\nu-B(m\mu-n\nu)-Cn\mu)e$; d'ailleurs il est facile de s'assurer que l'on a

$$2e+2a=e-e'+a-d=(\alpha-\alpha')(\delta+\delta')-(\beta-\beta')(\gamma+\gamma')$$
$$2b=(\alpha+\alpha')(\beta-\beta')+(\alpha-\alpha')(\beta+\beta'),$$

et comme $m(\gamma+\gamma')=n(\alpha+\alpha')$, $m(\delta+\delta')=n(\beta=\beta')$, il en résulte $(2e+2a)n+2nb=0$, ou

$$me+ma+nb=0\ldots\ldots\ldots\ldots(7).$$

De même

$$2e-2a=e-e'-a+d=(\alpha+\alpha')(\delta-\delta')-(\gamma+\gamma')(\delta-\delta')$$
$$2c=(\gamma-\gamma')(\delta+\delta')-(\gamma'+\gamma')(\delta-\delta'),$$

d'où $n(2e-2a)+2mc=0\ldots$ ou $ne-na+mc=0\ldots\ldots(8)$.

Maintenant si l'on ajoute à $m^2(b\mu^2-2a\mu\nu-c\nu^2)$ la fonction $(1-m\mu-n\nu)\{m\nu(e-a)+(m\mu+1)b\}+(me+ma+nb)(m\mu\nu+\nu)+(ne-na+me)m\nu^2$, qui se réduit à zéro, puisque $1-m\mu-n\nu=0$,

---

(*) Si l'on avait à-la-fois $\alpha+\alpha'=0$, $\gamma+\gamma'=0$, $\beta+\beta'=0$, $\delta+\delta'=0$, le rapport $\frac{m}{n}$ serait indéterminé, et partant la méthode inapplicable. Mais une légère attention suffit pour voir qu'on aurait alors $e=e'$, et comme d'ailleurs on a $e=-e'$, il s'ensuivrait $e=e'=0$; donc alors le déterminant de la forme F' serait nul, et nous excluons ici les formes de déterminant zéro.

$me+ma+nb=0$, $ne-na+mc=0$, et qu'on effectue les produits en effaçant les termes qui se détruisent, on trouvera $2mve+b$; donc

$$m^2(b\mu^2-2a\mu\nu-c\nu^2)=2mve+b \quad \ldots\ldots\ldots\ldots (9).$$

De même, si l'on ajoute à $mn(b\mu^2-2a\mu\nu-c\nu^2)$ la fonction

$$(1-m\mu-n\nu)\{(n\nu-m\mu)e-(1+m\mu+n\nu)a\}-(me+ma+nb)m\mu^2+(ne-na+mc)n\mu^2,$$

on trouve

$$mn(b\mu^2-2a\mu\nu-c\nu^2)=(n\nu-m\mu)e-a \quad \ldots\ldots\ldots (10).$$

Enfin si l'on ajoute à $n^2(b\mu^2-2a\mu\nu-c\nu^2)$ la fonction

$$(m\mu+n\nu-1)\{n\mu(e+a)+(n\nu+1)c\}-(me+ma+nb)n\mu^2-(ne-na+mc)(n\mu\nu+\mu),$$

on trouve

$$n^2(b\mu^2-2a\mu\nu-c\nu^2)=-2n\mu e-c \quad \ldots\ldots\ldots (11).$$

Donc si l'on multiplie l'équation (9) par A, (10) par $2B$ et (11) par C, il vient

$$(Am^2+2Bmn+Cn^2)(b\mu^2-2a\mu\nu-c\nu^2)=2e\{Am\nu+B(n\nu-m\mu)-Cm\mu\}+Ab-2Ba-Cc,$$

ou à cause de l'équation (6),

$$M(b\mu^2-2a\mu\nu-c\nu^2)=2Nr.$$

II. Pour prouver que la forme G renferme la forme F', nous démontrerons

1°. Que G devient F' en posant

$$t=(\mu\alpha+\nu\gamma)x'+(\mu\beta+\nu\delta)y' \ldots u=\frac{r}{e}(n\alpha-m\gamma)x'+\frac{r}{e}(n\beta-m\delta)y' \quad \ldots\ldots\ldots (S),$$

2°. Que $\frac{r}{e}(n\alpha-m\gamma)$ et $\frac{r}{e}(n\beta-m\delta)$ sont entiers.

1°. Puisque F devient G en posant $x=mt+\frac{\nu e}{r}u$, $y=nt-\frac{\mu e}{r}u$, la forme G se changera par la transformation (S) en la même forme que celle en laquelle F se changerait en posant

$$\begin{aligned} x &= m(\mu\alpha+\nu\gamma)x'+m(\mu\beta+\nu\delta)y'+\nu(n\alpha-m\gamma)x'+\nu(n\beta-m\delta)y' \\ &= (m\mu+n\nu)\alpha x'+(m\mu+n\nu)\beta y'=\alpha x'+\beta y', \\ y &= n(\mu\alpha+\nu\gamma)x'+n(\mu\beta+\nu\delta)y'-\mu(n\alpha-m\gamma)x'-\mu(n\beta-m\delta)y' \\ &= (m\mu+n\nu)\gamma x'+(m\mu+n\nu)\delta y'=\gamma x'+\delta y'. \end{aligned}$$

Mais par cette substitution, F se change en F'; donc par la substitution (S) la forme G se change en F'.

2°. On déduit facilement des valeurs de e, b, d l'équation $\alpha' e+\gamma b-\alpha d=0$, ou comme $d=-a$, $\alpha' e+\alpha a+\gamma b=0$, éliminant b au moyen de l'équation (7), il vient

$$(n\alpha-m\gamma)a=(m\gamma-n\alpha')e \ldots\ldots\ldots\ldots (12);$$

or on a $\alpha nb=-\alpha m(e+a)$, $\gamma mb=-m(\alpha' e+\alpha a)$; donc

$$(n\alpha-m\gamma)b=(\alpha'-\alpha)me \ldots\ldots\ldots\ldots (13);$$

enfin on trouvera $\gamma' e-\gamma a+\alpha c=0$, éliminant a au moyen de l'équation (8), il vient

$$(n\alpha-m\gamma)c=(\gamma-\gamma')ne \ldots\ldots\ldots\ldots (14).$$

On trouve de même $\beta' e+\delta b-\beta d=0$, ou $\beta' e+\delta b+\beta a=0$; éliminant b au moyen de l'équation (7), il vient

$$(n\beta-m\delta)a=(m\delta-n\beta')e \ldots\ldots\ldots\ldots (15):$$

or on a $\beta nb=-\beta m(e+a)$, $\delta mb=-m(\beta' e+\beta a)$; donc

$$(n\beta-m\delta)b=(\beta'-\beta)me \ldots\ldots\ldots\ldots (16):$$

enfin on trouve $\delta' e-\delta a+\beta c=0$, et en éliminant a au moyen de l'équation (8), on a

$$(n\beta-m\delta)c=(\delta-\delta')ne \ldots\ldots\ldots\ldots (17).$$

Le plus grand commun diviseur des nombres a, b, c étant r, si l'on détermine A'', B'', C'' de manière qu'on ait $A''a+B''b+C''c=r$, on trouvera au moyen des équations (12).....(17),

$$A''(m\gamma-n\alpha')+B''(\alpha-\alpha')m+C''(\gamma-\gamma')n=\frac{r}{e}(n\alpha-m\gamma)\ldots.$$

$$A''(m\delta-n\beta')+B''(\beta'-\beta)m+C''(\delta'-\delta)n=\frac{r}{e}(n\beta-m\delta),$$

et partant, $\frac{r}{e}(n\alpha-m\gamma)$ et $\frac{r}{e}(n\beta-m\delta)$ sont entiers.

165. *Exemple.* La forme $3x^2+14xy-4y^2$ se change en la forme $-12x'^2-18x'y'+39y'^2$, proprement en faisant $x=4x'+ny'$, $y=-x'-2y'$, improprement en faisant $x=-74x'+89y'$, $y=15x'-18y'$. On a donc $\alpha+\alpha'=-70$, $\beta+\beta'=100$, $\gamma+\gamma'=14$, $\delta+\delta'=-20$; et $-\frac{70}{24}=\frac{100}{-20}=\frac{5}{-1}$. Faisons donc $m=5$, $n=-1$.

Comme

Comme on doit avoir $5\mu - \nu = 1$, on satisfera évidemment à cette équation en faisant $\mu = 0$ et $\nu = -1$; d'ailleurs on trouve $e = 3$, $a = -237$, $b = -1170$, $c = 48$; leur plus grand commun diviseur $r = 3$: ce qui donne pour la transformation qui change F en G, $x = 5t - u$ et $y = -t$. La forme ambiguë G est elle-même $t^2 - 16tu + 3u^2$.

Si les formes F et F' sont équivalentes, la forme G sera aussi renfermée dans F' puisqu'elle l'est dans F; mais comme elle renferme cette même forme, elle lui sera équivalente, et partant à la forme F; ainsi dans ce cas le théorème s'énoncera ainsi:

Si F *et* F′ *sont équivalentes tant proprement qu'improprement, on pourra trouver une forme ambiguë équivalente à chacune d'elles.* Au reste, dans ce cas $e = \pm 1$, et partant r qui divise e doit être aussi $= 1$.

Ce que nous avons dit suffit pour la transformation des formes en général; passons à la représentation des nombres.

166. *Si la forme* F *renferme la forme* F′, *tout nombre qui pourra être représenté par* F′ *pourra l'être aussi par* F.

Soient x, y; x', y' les indéterminées des formes F et F' respectivement, et supposons que le nombre M puisse être représenté par F' en faisant $x' = m$ et $y' = x$, et que la forme F se change en F' par la transformation $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$, il est évident que F deviendra M en faisant $x = \alpha m + \beta n$, $y = \gamma m + \delta n$.

Si M peut être représenté de plusieurs manières par F', savoir, en faisant encore $x = m'$, $y = n'$, il pourra l'être aussi de plusieurs manières par F: en effet, si l'on avait à-la-fois $\alpha m + \beta n = \alpha m' + \beta n'$ et $\gamma m + \delta n = \gamma m' + \delta n'$, il s'ensuivrait $m(\alpha\delta - \beta\gamma) = m'(\alpha\delta - \beta\gamma)$ et $n(\alpha\delta - \beta\gamma) = n'(\alpha\delta - \beta\gamma)$, ce qui exige que $\alpha\delta - \beta\gamma = 0$, et partant, que le déterminant de la forme F' soit $= 0$, contre l'hypothèse, ou que $m = m'$ et $n = n'$, il suit de là qu'il y a au moins autant de manières de représenter M par F que par F'.

Si donc F et F' sont équivalentes, tout nombre qui pourra être représenté par l'une pourra l'être par l'autre et d'autant de manières.

Observons enfin que dans ce cas le plus grand diviseur commun des nombres m et n est égal au plus grand diviseur commun des nombres $\alpha m+\beta n$, $\gamma m+\delta n$. Soit en effet Δ ce diviseur, prenons les nombres μ et ν tels qu'on ait $\mu m+\nu n=\Delta$, on aura $(\delta\mu-\gamma\nu)(\alpha m+\beta n)-(\beta\mu-\alpha\nu)(\gamma m+\delta n)=(\alpha\delta-\beta\gamma)(\mu m+\nu n)=\pm\Delta$. Donc le plus grand diviseur commun des nombres $\alpha m+\beta n$, $\gamma m+\delta n$ divisera Δ; mais Δ le divise, puisqu'il divise évidemment $\alpha m+\beta n$, $\gamma m+\delta n$; donc ce plus grand commun diviseur est égal à Δ. Il suit de là que si m et n sont premiers entre eux, $\alpha m+\beta n$ et $\gamma m+\delta n$ le seront aussi.

167. THÉORÈME. *Si les formes* $ax^2+2bxy+cx^2\ldots.(F)$, $a'x'^2+2b'x'y'+c'y'^2\ldots.(F')$ *sont équivalentes, que leur déterminant soit* D, *que la dernière se change en la première en faisant* $x'=\alpha x+\beta y$, $y'=\gamma x+\delta y$, *que d'ailleurs le nombre* M *soit représenté par la forme* F *en faisant* $x=m$, $y=n$, *et partant, par la forme* F' *en faisant* $x'=\alpha m+\beta n=m'$, $y'=\gamma m+\delta n=n'$, m *et* n *et parconséquent* m' *et* n' *étant premiers entre eux, les deux représentations appartiendront à la même valeur de l'expression* $\sqrt{D}$ (*mod.* M), *ou à des valeurs opposées, suivant que la transformation de* F' *en* F *sera propre ou impropre.*

Soient déterminés les nombres μ, ν de manière qu'on ait $\mu m+\nu n=1$, et soient faits $\frac{\delta\mu-\gamma\nu}{\alpha\delta-\beta\gamma}=\mu'$, $-\frac{\beta\mu+\alpha\nu}{\alpha\delta-\beta\gamma}=\nu'$(*). On aura (n° précéd.) $\mu'm'+\nu'n'=1$. Soit d'ailleurs

$$\mu(bm+cn)-\nu(am+bn)=V\ldots\mu'(b'm'+c'n')-\nu'(a'm'+b'n')=V'.$$

V et V' sont les valeurs de l'expression $\sqrt{D}$ (mod. M) auxquelles appartiennent la première et la seconde représentation. Cela posé, si dans V' on met pour m', n', μ', ν' leurs valeurs, et dans V pour $a\ldots a'\alpha^2+2b'\alpha\gamma+c'\gamma^2$, pour $b\ldots a'\alpha\beta+b'(\alpha\delta+\beta\gamma)+c'\gamma\delta$, pour $c\ldots a'\beta^2+2b'\beta\delta+c'\delta^2$, on trouve, toutes réductions faites, $V=V'(\alpha\delta-\beta\gamma)$, et partant $V=V'$ ou $V=-V'$, suivant que $\alpha\delta-\beta\gamma$ sera $=+1$ ou $=-1$. Donc, etc.

Si donc on a plusieurs représentations d'un nombre M par la forme (a, b, c) au moyen des valeurs de x, y premières entre elles et qui appartiennent à des valeurs différentes de l'expres-

(*) μ' et ν' sont des nombres entiers puisque $\delta-\beta\gamma=\pm 1$

sion $\sqrt{D}$ (mod. M); les représentations par la forme (a', b', c') appartiendront aux mêmes valeurs, et s'il n'y a aucune représentation du nombre M par une certaine forme, qui appartienne à une certaine valeur donnée, il n'y en aura aucune non plus qui appartienne à cette valeur pour une forme équivalente.

168. THÉORÈME. *Si le nombre* M *peut être représenté par la forme* $ax^2+2bxy+cy^2$ *en donnant à* x *et* y *des valeurs* m *et* n *premières entre elles, et que* N *soit la valeur de l'expression* $\sqrt{D}$ (*mod.* M) *à laquelle cette représentation appartienne, les formes* (a, b, c) *et* $\left(M, N, \frac{N^2-D}{M}\right)$ *seront proprement équivalentes.*

Il suit du n° 155 qu'on peut trouver des nombres entiers μ et ν qui satisfassent aux équations

$$m\mu+n\nu=1 \ldots . \mu(bm+cn)-\nu(am+bn)=N.$$

Cela fait, la forme (a, b, c) se change, au moyen de la substitution $x=mx'-\nu y'$, $y=nx'+\mu y'$, en une forme dont le déterminant $=D(m\mu+n\nu)^2=D$, c'est-à-dire en une forme équivalente. Si on suppose cette forme $=(A, B, C)$, on aura $C=\frac{B^2-D}{A}$, d'ailleurs

$$A=am^2+2bmn+cn^2=M, \quad B=-m\nu a+(m\mu-n\nu)b+n\mu c=N;$$

donc la forme (A, B, C) revient à $\left(M, N, \frac{N^2-D}{M}\right)$.

Au reste, des équations

$$m\mu+n\nu=1 \ldots \ldots . \mu(mb+nc)-\nu(ma+nb)=N,$$

on déduit... $\mu=\frac{ma+nb+nN}{M}$... $\nu=\frac{mb+nc-mN}{M}$,

qui seront ainsi des nombres entiers.

Il faut observer que cette proposition n'a pas lieu quand $M=0$, car dans ce cas on doit avoir $N^2-D=0$, d'où il suit que $\frac{N^2-D}{M}$ est indéterminé.

169. Si l'on a plusieurs représentations du nombre M par la forme (a, b, c) qui appartiennent à la même valeur N de l'expression $\sqrt{D}$ (mod. M), en supposant toujours les valeurs de x, y premières entre elles, on en déduira plusieurs transformations propres

de la forme $(a, b, c)\ldots(F)$ en $\left(M, N, \frac{N^2-D}{M}\right)\ldots(G)$; savoir, si une de ces représentations provient des valeurs $x=m'$, $y=n'$, F se changera en G par la substitution

$$x=m'x'+\frac{m'N-m'b-n'}{M}\ldots y=n'x'+\frac{n'N+m'a+n'b}{M}.$$

Réciproquement, une transformation propre de F en G étant donnée, on en déduira une représentation de M par la forme F, qui appartiendra à la valeur N. Si F se change en G en posant $x=mx'-\nu y'$ et $y=nx'+\mu y'$, on représentera M par la forme F en posant $x=m$, $y=n$, et comme $m\mu+n\nu=1$, la valeur de l'expression $\sqrt{D}$ (mod. M) à laquelle appartient la représentation sera $\mu(bm+cn)-\nu(am+bn)=N$. En outre de plusieurs transformations propres différentes, on déduirait autant de représentations diverses appartenantes à la valeur N ; car si l'on supposait que la même représentation pût dériver de deux transformations propres différentes, ces deux transformations étant $x=mx'-\nu y'$ et $y=nx'+\mu y'$, $x=mx'-\nu' y'$, $y=nx'+\mu' y'$; des deux équations

$$m\mu+n\nu=m\mu'+n\nu'\ldots.\mu(mb+nc)-\nu(ma+nb)=\mu'(mb+nc)-\nu'(ma+nb),$$

on déduit sans peine qu'il faudrait qu'on eût $M=0$, ou bien $\mu=\mu'$, $\nu=\nu'$; or la première condition est déjà exclue, et nous avons supposé m' et n' différens de m et n. Il résulte de là que si on avait toutes les transformations propres de F en G, elles donneraient toutes les représentations de M par F, qui appartiennent à la valeur N. La recherche des représentations d'un nombre donné par une forme donnée, dans lesquelles les valeurs des indéterminées sont premières entre elles, se réduit donc à trouver toutes les transformations propres de cette forme en une autre forme équivalente donnée.

En appliquant ici ce que nous avons dit n° 162, on conclut facilement que si une représentation du nombre M par la forme F appartenante à la valeur N, est donnée par les valeurs $x=\alpha$, $y=\gamma$, la formule générale qui comprend toutes les représentations du même nombre par la forme F, sera

$$x=\frac{\alpha t-(\alpha b+\gamma c)u}{m}\ldots\ldots y=\frac{\gamma t+(\alpha a+\gamma b)u}{m},$$

m étant le plus grand commun diviseur des nombres a, $2b$, c, et t, u tous les nombres entiers qui satisfont indéfiniment à l'équation

$$t^2 - Du^2 = m^2.$$

170. Si la forme (a, b, c) est équivalente à une certaine forme ambiguë, elle sera équivalente, tant proprement qu'improprement, à la forme $\left(M, N, \frac{N^2 - D}{M}\right)$, ou encore elle sera proprement équivalente tant à la forme $\left(M, N, \frac{N^2 - D}{M}\right)$, qu'à la forme $\left(M, -N, \frac{N^2 - D}{M}\right)$ (n° 159); on aura donc les représentations du nombre M par F appartenantes soit à la valeur $+N$, soit à la valeur $-N$. Et réciproquement, si on connaît plusieurs représentations du nombre M par la même forme F, et que ces représentations appartiennent à des valeurs opposées de l'expression $\sqrt{D}$ (mod. M), la forme F sera équivalente à la forme G tant proprement qu'improprement, et l'on pourra assigner une forme ambiguë équivalente à F.

Ces principes généraux sur la représentation des nombres nous suffisent pour ce que nous avons à dire à présent. Nous parlerons plus bas des représentations où les indéterminées ne doivent pas avoir de valeurs premières entre elles. Quant aux autres propriétés, les formes dont le déterminant est négatif, demandent à être traitées d'une manière tout-à-fait différente que celles dont le déterminant est positif. Aussi nous allons maintenant considérer séparément chacun de ces cas : nous commencerons par le premier comme étant le plus facile.

171. PROBLÈME. *Étant proposée une forme quelconque* (a, b, a′) *dont le déterminant est négatif*, ut $= -$ D, *trouver une forme* (A, B, C) *qui lui soit proprement équivalente, et dans laquelle* A *soit non* $> 2\sqrt{\frac{D}{3}}$, B *non* $> \frac{1}{2}$ A, C *non* $<$ A.

Nous supposons que ces trois conditions ne soient pas réunies dans la forme proposée, autrement il serait inutile de chercher la seconde forme. Soit b' le résidu *minimum* absolu du nombre $-b$, suivant le module a'(*) et $a'' = \frac{b'^2 + D}{a'}$, qui sera entier, puisque

$b'^2 \equiv b^2$, d'où $b'^2 + D \equiv b^2 + D \equiv aa' \pmod{a'}$. Maintenant, si $a'' < a'$, soit encore b'' résidu *minimum* de $-b'$, suivant le module a'', et $a''' = \frac{b''^2+D}{a''}$. Si $a''' < a''$, soit de même b''' résidu absolu *minimum* de $-b''$, suivant le module a''', et $a^{IV} = \frac{b'''^2+D}{a'''}$; en continuant cette opération jusqu'à ce que l'on parvienne à un terme $a^{(m+1)}$ de cette progression qui ne soit pas plus petit que le terme précédent $a^{(m)}$, ce qui arrivera nécessairement, sans quoi on aurait une suite de nombres entiers plus grands que zéro et décroissans à l'infini. Alors la forme (a^m, b^m, a^{m+1}) satisfera à toutes les conditions.

En effet, 1°. dans la suite de formes (a, b, a'), (a', b', a''), (a'', b'', a'''), etc., une quelconque est contiguë à celle qui la précède; donc la dernière est proprement équivalente à la première (n°s 159 et 160).

2°. Comme $b^{(m)}$ est le résidu *minimum* absolu de $-b^{(m-1)}$, suivant le module $a^{(m)}$, il ne sera pas plus grand que $\frac{1}{2}a^{(m)}$ (n° 4.).

3°. Puisque $a^{(m)}.a^{(m+1)} = D + b^{(m)2}$, et que $a^{(m+1)}$ non $< a^{(m)}$, $a^{(m)2}$ ne sera $> D + b^{(m)2}$; et comme $b^{(m)}$ est non $> \frac{1}{2}a^{(m)}$, $a^{(m)2}$ ne sera pas $> D + \frac{1}{4}a^{(m)2}$, ou $\frac{3}{4}a^{(m)2}$ ne sera pas plus grand que D; donc enfin $a^{(m)}$ non $> 2\sqrt{\frac{D}{3}}$.

Exemple. Soit la forme (304, 217, 155) dont le déterminant $= -31$, on trouve la suite de formes : (304, 217, 155), (155, −62, 25), (25, 12, 7), (7, 2, 5), (5, −2, 7); et la dernière est la forme cherchée. De même, pour la forme (121,49,20) dont le déterminant est — 19, on trouve les formes équivalentes : (20, −9, 5), (5, −1, 4), (4, 1, 5); donc (4, 1, 5) est la forme cherchée.

Nous appellerons *formes réduites* les formes (A, B, C), qui sont telles que, le déterminant étant négatif, on ait A non $> 2\sqrt{\frac{D}{3}}$, B non $> \frac{1}{2}A$, et C non $< A$; ainsi on peut trouver une forme

(*) Il faut remarquer que si a ou a' étaient zéro, le déterminant serait un quarré positif, ce qui est contre l'hypothèse, par la même raison a et a' ne peuvent être de signe contraire.

réduite proprement équivalente à une forme donnée quelle qu'elle soit.

172. PROBLÈME. *Trouver les conditions nécessaires pour que deux formes réduites non identiques et de même déterminant négatif, soient proprement équivalentes.*

Soient les formes (a, b, c), (a', b', c') dont le déterminant est $-D$; supposons, ce qui est permis, que a' ne soit pas $> a$, et que la forme $ax^2+2bxy+cy^2$ se change en $a'x'^2+2b'x'y'+c'y'^2$, par la substitution propre $x=\alpha x'+\beta y'$, $y=\gamma x'+\delta y'$. On aura les équations

$a\alpha^2+2b\alpha\gamma+c\gamma^2=a'$....(1), $a\alpha\beta+b(\alpha\delta+\beta\gamma)+c\gamma\delta=b'$...(2), $\alpha\delta-\beta\gamma=1$...(3).

L'équation (1) peut se mettre sous la forme $aa'=(a\alpha+b\gamma)^2+D\gamma^2$, donc aa' est positif; et comme on a d'ailleurs $ac=D+b^2$, $a'c'=D+b'^2$, il s'ensuit que ac, $a'c'$, aa' sont positifs, et partant que a, a', c, c' sont tous de même signe. Mais a et a' sont non $> 2\sqrt{\frac{D}{3}}$; donc aa', et à plus forte raison $D\gamma^2$ ne sera pas $> \frac{4}{3}D$; mais γ doit être entier, il sera donc 0 ou ± 1.

I. Si $\gamma=0$, l'équation (3) donne $\alpha\delta=1$, et partant $\alpha=\pm 1$, et $\delta=\pm 1$: dans les deux cas, il résulte de l'équation (1), $a=a'$, et de l'équation (2) $b'-b=\pm\beta a$; mais b est non $> \frac{1}{2}a$, b' non $> \frac{1}{2}a'$, et partant non $> \frac{1}{2}a$; donc l'équation $b'-b=\pm\beta a$ ne peut avoir lieu si b est de même signe que b', à moins qu'on n'ait $b=b'$, d'où s'ensuivrait $c'=\frac{b'^2+D}{a'}=\frac{b^2+D}{a}=c$, et partant, à moins que les formes (a, b, c), (a', b', c') ne soient identiques, ce qui est contre l'hypothèse. Si b et b' sont de signe contraire, cette équation n'aura lieu non plus qu'en supposant $b=-b'\pm\frac{1}{2}a$, ce qui donne de même $c'=c$; la forme (a', b', c') sera donc $(a, -b, c)$, c'est-à-dire opposée à la forme (a, b, c). On voit d'ailleurs que ces formes sont ambiguës, puisque $2b=+a$ (n° 163).

II. Si $\gamma=\pm 1$, l'équation (1) devient $a\alpha^2+c-a'=\pm 2b\alpha$; mais c n'est pas $< a$, et par conséquent pas $< a'$; donc $2b\alpha$ n'est certainement pas $< a\alpha^2$; ainsi $2b$ n'étant pas $> a$, α ne sera pas $< \alpha^2$, ce qui exige qu'on ait $\alpha=0$, ou $\alpha=\pm 1$.

1°. Si $\alpha=0$, l'équation (1) donne $c=a'$; et comme on a à-la-fois a non $\geq a'$ et non $< c$, il s'ensuit que $a=a'=c$: or

l'équation (3) donne $\beta\gamma = -1$, et partant l'équation (2) devient $b + b' = \pm\delta c = \pm\delta a$. On pourra supposer seulement ici, comme dans le cas précédent, $b = b'$, ou $b = -b'$. Par la première supposition, les formes (a, b, c), (a', b', c') seraient identiques, par la seconde elles seront opposées.

2°. Si $\alpha = \pm 1$, l'équation (1) donne $a + c - a' = \mp 2b$; mais a et c sont tous deux non $< a'$, donc $2b$ sera non $< a$ et non $< c$; d'ailleurs on a $2b$ non $> a$ et non $> c$; donc nécessairement $a = c = \pm 2b$. L'équation $a + c - a' = \mp 2b$ donne alors $\pm 2b = a'$, ainsi l'équation (2) devient

$$a(\alpha\beta + \gamma\delta) + b(\alpha\delta + \beta\gamma) = b',$$

ou comme $\alpha\delta - \beta\gamma = 1$,

$$b' - b = a(\alpha\beta + \gamma\delta) + 2b\beta\gamma = a(\alpha\beta + \gamma\delta \mp \beta\gamma),$$

ce qui exige, comme ci-dessus, que $b = b'$, ou que $b = -b'$. Or, dans le premier cas, les formes seraient identiques contre l'hypothèse; dans le second, elles sont opposées et ambiguës.

Il résulte de cette analyse que les formes (a, b, c), (a', b', c') ne peuvent être équivalentes, à moins qu'elles ne soient opposées et en même temps ambiguës, ou telles que $a = c = a' = c'$. Il était évident, *à priori*, que dans ce cas les formes sont proprement équivalentes; car, comme opposées, elles sont improprement équivalentes, et comme ambiguës, elles le sont aussi proprement. Mais si $a = c$, la forme, $\left(\frac{D + (a-b)^2}{a}, a - b, a\right)$ sera contiguë, et partant équivalente à (a, b, c); mais comme $D + b^2 = ac = a^2$, on a $\frac{D + (a-b)^2}{a} = 2a - 2b$, et la forme $(2a - 2b, a - b, a)$ est ambiguë; donc (a, b, c) sera aussi proprement équivalente à son opposée.

On juge facilement par là si deux formes réduites (a, b, c), (a', b', c') non opposées, peuvent être improprement équivalentes. En effet, elles le seront, si (a, b, c) et $(a', -b', c')$ qui ne sont pas identiques, sont proprement équivalentes; sinon elles ne le seront pas. Il suit de là que les formes proposées, pour être improprement équivalentes, doivent être identiques, et en outre ambiguës, ou telles qu'on

qu'on ait $a = c$. Mais les formes qui ne sont ni identiques, ni opposées, ne peuvent être équivalentes ni proprement ni improprement.

173. PROBLÈME. *Étant données deux formes* F *et* F′ *de même déterminant négatif, chercher si elles sont équivalentes.*

Cherchons deux formes réduites f et f' proprement équivalentes aux formes F, F' respectivement. Si les formes f, f' sont équivalentes proprement ou improprement, ou des deux manières, F et F' le seront aussi; mais si f et f' ne sont équivalentes d'aucune manière, F et F' ne le seront pas non plus.

Par le n° précédent, il peut arriver quatre cas :

1°. Si f et f' ne sont ni identiques ni opposées, F et F' ne seront équivalentes d'aucune manière.

2°. Si f et f' sont d'abord identiques ou opposées, et ensuite ambiguës, ou telles que leurs termes extrêmes soient égaux, F et F' seront équivalentes proprement et improprement.

3°. Si f et f' sont identiques, mais qu'elles ne soient pas ambiguës, ou qu'elles n'aient pas leurs termes extrêmes égaux, F et F' ne seront que proprement équivalentes.

4°. Si f et f' sont opposées, mais qu'elles ne soient point ambiguës, ou qu'elles n'aient point leurs termes extrêmes égaux, les formes F et F' seront seulement improprement équivalentes.

Exemple. On trouve pour les formes $(41, 35, 30), (7, 18, 47)$ dont le déterminant est -5, les réduites $(1, 0, 5), (2, 1, 3)$ qui leur sont respectivement équivalentes; donc les formes proposées ne sont équivalentes en aucune manière. Mais les formes $(23, 38, 63), (15, 20, 27)$ ont la même réduite $(2, 1, 3)$, et comme elle est en même temps ambiguë, les formes proposées seront équivalentes proprement et improprement. Les formes $(37, 53, 78), (53, 73, 102)$ ont pour réduites $(9, 2, 9)$ et $(9, -2, 9)$; comme elles sont opposées et que leurs termes extrêmes sont égaux, les formes proposées sont équivalentes tant proprement qu'improprement.

174. Le nombre des formes réduites qui ont un déterminant donné $-D$, est toujours fini, et même assez petit par rapport au nombre D, et il y a deux manières de trouver ces formes

elles-mêmes; désignons indéfiniment par (a, b, c) les formes réduites dont le déterminant est $-D$, il s'agit de déterminer toutes les valeurs de a, b et c.

Première Méthode. On prendra pour a tous les nombres tant positifs que négatifs qui ne sont pas plus grands que $\sqrt{\frac{4}{3}D}$, et dont $-D$ est résidu quadratique; et pour chaque valeur de a, on prendra b successivement égal à toutes les valeurs de l'expression $\sqrt{-D}\,(\text{mod. } a)$, qui ne sont pas $> \frac{1}{2}a$, en les prenant tant positivement que négativement. Quant à c, on le fera $= \frac{D+b^2}{a}$. S'il résulte de là quelques formes dans lesquelles $c < a$, elles seront à rejeter, et les autres seront évidemment des formes réduites.

Deuxième Méthode. Soient pris pour b tous les nombres positifs ou négatifs qui ne surpassent pas $\sqrt{\frac{D}{3}}$; pour chaque valeur de b, on décomposera b^2+D de toutes les manières possibles, en deux facteurs pris positivement ou négativement, et non plus petits que $2b$, en prenant l'un des deux, le plus petit s'ils sont inégaux, pour la valeur de a, et l'autre pour la valeur de c. S'il en résulte quelques formes dans lesquelles $a > 2\sqrt{\frac{D}{3}}$, elles seront à rejeter; les autres seront visiblement des formes réduites. Il est d'ailleurs évident qu'il n'y a pas une forme réduite qui ne puisse se trouver par chacune des deux méthodes.

Exemple. Soit $D = 85$. Par la première méthode, la limite des valeurs de a est $\sqrt{\frac{340}{3}}$ qui tombe entre 10 et 11. Or les nombres compris entre 1 et 10, et dont le résidu est 85, sont: 1, 2, 5, 10, d'où résultent les douze formes suivantes:

$(1, 0, 85), (-1, 0, -85); (2, 1, 43), (2, -1, 43), (-2, +1, -43), (-2, -1, -43); (5, 0, 17), (-5, 0, -17); (10, 5, 11), (10, -5, 11), (-10, 5, -11), (-10, -5, -11)$.

Par la seconde méthode, la limite des valeurs de b est $\sqrt{\frac{85}{3}}$ qui tombe entre 5 et 6. En supposant $b = 0$, on trouve les formes: $(1, 0, 85)$, $(-1, 0, -85)$, $(5, 0, 17)$, $(-5, 0, -17)$; pour $b = \pm 1$: $(2, \pm 1, 43)$, $(-2, \pm 1, -43)$. Il n'y en a aucune pour $b = \pm 2$, parceque 89 n'est pas décomposable en deux facteurs dont chacun soit non < 4. La même chose a eu lieu pour $b = \pm 3$ et ± 4.

Enfin, pour $b = \pm 5$, il vient $(10, \pm 5, 11)$, $(-10 \pm 5, -11)$.

175. Si parmi toutes les formes déduites d'un déterminant donné, on supprime une des deux qui sans être identiques sont proprement équivalentes, celles qui resteront jouiront de cette propriété remarquable, qu'une forme quelconque de même déterminant sera proprement équivalente à quelqu'une d'entre elles, et à une seule; car, sans cela, il resterait encore des formes réduites proprement équivalentes entre elles. D'où il suit que *toutes les formes de même déterminant peuvent se distribuer en autant de classes qu'il sera resté de formes réduites*, en comprenant dans la même classe les formes qui sont proprement équivalentes à la même réduite.

Ainsi, pour $D = 85$, il reste les huit formes réduites,

$(1, 0, 85)$, $(2, 1, 43)$, $(5, 0, 17)$, $(10, 5, 11)$,

$(-1, 0, -85)$, $(-2, 1, -43)$, $(-5, 0, -17)$, $(-10, 5, -11)$.

Donc toutes les formes dont le déterminant est -85, peuvent se distribuer en huit classes, suivant qu'elles sont proprement équivalentes à la première, à la deuxième, etc.; et il est clair que les formes d'une même classe sont proprement équivalentes, tandis que deux formes prises dans deux classes différentes ne sauraient être proprement équivalentes. Mais nous traiterons ci-après, avec plus de détail, le sujet de la classification des formes; nous n'ajoutons ici qu'une observation. Nous avons déja fait voir que si le déterminant de la forme (a, b, c) est négatif, a et c sont de même signe, et on s'assurera, comme nous l'avons fait pour les formes réduites, que si (a, b, c), (a', b', c') sont deux formes équivalentes, a, a', c, c' seront de même signe (*). Il suit de là que les formes dont les termes extrêmes sont positifs, sont absolument distinctes de celles dont les termes extrêmes sont négatifs, et qu'il suffit dans les formes réduites, de considérer celles qui ont leurs termes extrêmes positifs, car les autres sont en même nombre, et

(*) En effet si l'on change la première de ces formes en la seconde, par la substitution

$$x = \alpha x' + \beta y'$$
$$y = \gamma x' + \delta y'$$

on aura $a\alpha^2 + 2\beta\alpha\gamma + c\gamma^2 = a'$, d'où $aa' = (a\alpha + b\beta)^2 + D\gamma^2$: ce produit est donc évidemment positif, et comme ni a ni a' ne sont nuls, il faut que tous deux soient de même signe.

elles naissent des premières, en changeant les signes des termes extrêmes. La même chose a lieu pour les formes réduites à rejeter et à retenir.

176. Voici en conséquence une table qui contient, pour quelques déterminans négatifs, les formes suivant lesquelles toutes celles du même déterminant peuvent se distribuer en classes; mais, suivant la remarque du n° précédent, nous n'en avons mis que la moitié, c'est-à-dire celles dont les termes extrêmes sont positifs.

Déterm.	
1...	(1, 0, 1).
2...	(1, 0, 2).
3...	(1, 0, 3), (2, 1. 2).
4...	(1, 0, 4), (2, 0, 2).
5...	(1, 0, 5), (2, 1, 3).
6...	(1, 0, 6), (2, 0, 3).
7...	(1, 0, 7), (2, 1, 4).
8...	(1, 0, 8), (2, 0, 4), (3, 1, 3).
9...	(1, 0, 9), (2, 1, 5), (3, 0, 3).
10...	(1, 0, 10), (2, 0, 5).
11...	(1, 0, 11), (2, 1, 6), (3, 1, 4), (3, —1, 4).
12...	(1, 0, 12), (2, 0, 6), (3, 0, 4), (4, 2, 4).

Il serait superflu de continuer plus loin cette table, puisque nous donnerons plus bas une bien meilleure manière de la disposer.

Il résulte de cette table que toute forme dont le déterminant est -1, équivaut proprement à la forme x^2+y^2, si les termes extrêmes sont positifs, et à la forme $-x^2-y^2$, s'ils sont négatifs; que toute forme dont le déterminant est -2, et dont les termes extrêmes sont positifs, équivaut à la forme x^2+2y^2, etc.; que toute forme dont le déterminant est -11, et dont les termes extrêmes sont positifs, équivaut à l'une des quatre : x^2+11y^2, $2x^2+2xy+6y^2$, $3x^2+2xy+4y^2$, $3x^2-2xy+4y^2$, etc.

177. PROBLÈME. *Étant donnée une suite de formes telle que chacune soit contiguë à celle qui la précède par la dernière partie, trouver une transformation propre de la première en une quelconque de la suite.*

Soient les formes $(a, b, a')=F$, $(a', b', a'')=F'$, $(a'', b'', a''')=F''$, $(a''', b''', a^{IV})=F'''$...etc. Faisons $\frac{b+b'}{a'}=h'$, $\frac{b'+b''}{a''}=h''$, $\frac{b''+b'''}{a'''}=h'''$, etc. nommons $x, y \ldots x', y' \ldots x'', y''$, etc. les indéterminées des formes F, F', F'', etc. et supposons que F se change

en F' par la substitution $x=\alpha' x'+\beta' y'$, $y=\gamma' x'+\delta' y'$

F''..... $x=\alpha'' x''+\beta'' y'' \ldots y=\gamma'' x''+\delta'' y''$

F'''..... $x=\alpha''' x'''+\beta''' y''' \ldots y=\gamma''' x'''+\delta''' y'''$.

Cela posé, comme F se change en F' en faisant $x=-y'$ et $y=x'+h'y'$, F' en F'' en faisant $x'=-y'' \ldots y'=x''+h''y''$, F'' en F''' en faisant $x''=-y'''$ et $y''=x'''+h'''y'''$, etc. on trouvera facilement les équations suivantes:

$\alpha'=0$	$\beta'=-1$	$\gamma'=1$	$\delta'=h'$
$\alpha''=\beta' \ldots\ldots$	$\beta''=h''\beta'-\alpha' \ldots$	$\gamma''=\delta' \ldots.$	$\delta''=h''\delta'-\gamma'$
$\alpha'''=\beta'' \ldots\ldots$	$\beta'''=h'''\beta''-\alpha'' \ldots$	$\gamma'''=\delta'' \ldots.$	$\delta'''=h'''\delta''-\gamma''$
$\alpha^{IV}=\beta''' \ldots\ldots$	$\beta^{IV}=h^{IV}\beta'''-\alpha''' \ldots$	$\gamma^{IV}=\delta''' \ldots.$	$\delta^{IV}=h^{IV}\delta'''-\gamma'''$
etc.	etc.	etc.	etc.

d'où l'on tire

$\alpha'=0$	$\beta'=-1$	$\gamma'=1$	$\delta'=h'$
$\alpha''=\beta' \ldots\ldots$	$\beta''=h''\beta' \ldots\ldots$	$\gamma''=\delta' \ldots.$	$\delta''=h''\delta-1$
$\alpha'''=\beta'' \ldots\ldots$	$\beta'''=h'''\beta''-\beta' \ldots$	$\gamma'''=\delta'' \ldots.$	$\delta'''=h'''\delta''-\delta'$
$\alpha^{IV}=\beta''' \ldots\ldots$	$\beta^{IV}=h^{IV}\beta'''-\beta'' \ldots$	$\gamma^{IV}=\delta''' \ldots.$	$\delta^{IV}=h^{IV}\delta'''-\delta''$
etc.	etc.	etc.	etc.

il suit du n° 159, et de la formation de ces quantités, que les différentes transformations sont propres.

Cet algorithme très-simple, et auquel on applique facilement le calcul, est analogue à celui du n° 27 (*), auquel même il

---

(*) On aurait, d'après la notation du n° 27,

$$\beta^{(n)}=\pm[-h'', h''', -h^{IV}, \ldots \ldots \pm h^{(n)}],$$

où les signes ambigus doivent être $-,-$; $-,+$; $+,-$; $+,+$, suivant que n est de la forme $4K$, $4K+1$, $4K+2$, $4K+3$,

$$\delta^{n}=\pm[h', -h'', h''', \ldots\ldots \pm h^{(n)}],$$

où les signes, dans les mêmes cas, doivent être $+,-$; $+,+$; $-,-$; $-,+$.

Mais le desir d'abréger nous empêche d'insister davantage sur ces formules, qu'au reste chacun pourra confirmer aisément.

est facile de le ramener. Au reste, cette solution n'est pas restreinte au cas des formes de déterminant négatif; elle convient à tous les cas, pourvu qu'aucun des nombres a', a'', a''', etc. ne soit égal à zéro.

178. PROBLÈME. *Étant données deux formes* F *et* f *de même déterminant négatif et proprement équivalentes, trouver une transformation propre de l'une en l'autre.*

Supposons que F soit la forme (A, B, A'); par la méthode du n° 171, on cherchera la suite des formes (A', B', A''), (A'', B'', A'''), etc. jusqu'à la réduite $(A^{(m)}, B^{(m)}, A^{(m+1)})$. Soit (a, b, a') l'autre forme f; on cherchera de même la suite (a', b', a''), (a'', b'', a'''), etc. jusqu'à $(a^{(n)}, b^{(n)}, a^{(n+1)})$, qui est la réduite. Alors il peut se présenter deux cas:

1°. Si les formes $(A^{(m)}, B^{(m)}, A^{(m+1)})$, $(a^{(n)}, b^{(n)}, a^{(n+1)})$ sont identiques, ou à-la-fois opposées et ambiguës, les formes $(A^{(m-1)}, B^{(m-1)}, A^{m})$, $(a^{(n)}, b^{n-1)}, a^{(n-1)})$ seront contiguës, $A^{(m-1)}$ désignant l'avant-dernier terme de la suite A, A', A'', etc. (il en est de même de $B^{(m-1)}$, $a^{(n-1)}$, $b^{(n-1)}$); car $A^{(n)} = a^{(n)}$, $B^{(m-1)} + B^{(m)} \equiv 0 \pmod{A^{m}}$, $b^{(n-1)} + b^{(n)} \equiv 0 \pmod{a^{(m)} = A^{(m)}}$, d'où $B^{(m-1)} - b^{(n-1)} + B^{(m)} - b^{(n)} \equiv 0$; mais si les formes réduites sont identiques, $B^{(m)} - b^{(n)} = 0$; si elles sont opposées et ambiguës, $B^{(n)} - b^{(n)} = A^{(m)}$; donc dans les deux cas $B^{(m-1)} - b^{(n-1)} \equiv 0$. Il suit de là que dans la suite de formes:

$$(A, B, A'), (A', B', A'') \ldots (A^{(m-1)}, B^{(m-1)}, A^{(m)}), (a^{(n)}, -b^{(n-1)}, a^{(n-1)}),$$
$$(a^{(n-1)}, -b^{(n-2)}, a^{(n-2)}) \ldots (a', -b, a), (a, b, a').$$

Une quelconque est contiguë à celle qui la précède, et par conséquent (n° précéd.) on pourra trouver une transformation propre de F en f.

2°. Si les formes $(A^{(m)}, B^{(m)}, A^{(m+1)})$, $(a^{(n)}, b^{(n)}, a^{(n+1)})$ n'étant pas identiques, sont opposées et que leurs termes extrêmes soient égaux, on aura $A^{(m)} = A^{(m+1)} = a^{(n)} = a^{(n+1)}$, d'où $A^{(m+1)} = a^{(n)}$, et $B^{m} - b^{(n-1)} = -(b^{(n)} + b^{(n-1)})$, et partant divisible par $a^{(n)}$; donc la forme $(A^{(m)}, B^{(m)}, A^{(m+1)})$ est contiguë à la forme $(a^{n}, -b^{n-1}, a^{n-1})$, et la suite:

$$(A, B, A'), (A', B', A'') \ldots (A^{(m)}, B^{(m)}, A^{(m+1)}), (a^{(n)}, -b^{(n-1)}, a^{(n-1)}),$$
$$(a^{(n-1)}, -b^{(n-2)}, a^{(n-2)}) \ldots (a', -b, a), (a, b, a')$$

jouit de la même propriété que la précédente. On pourra donc trouver une transformation propre de F en f.

Exemple. Soient les deux formes (23, 38, 63), (15, 20, 27); On trouvera

pour { la 1re... (23, 38, 63), (63, 25, 10), (10, 5, 3), (3, 1, 2), (2, —1, 3)
la 2e.... (15, 20, 27), (27, 7, 2), (2, 1, 3).

Les deux réduites sont opposées et ambiguës; les deux formes proposées se rapportent parconséquent au premier cas. La suite de formes contiguës sera donc

(23, 28, 63), (63, 25, 10), (10, 5, 3), (3, 1, 2),
(2, —7, 27), (27, —20, 15), (15, 20, 27).

Il en résulte $h' = \frac{38+25}{63} = 1$, $h'' = \frac{25+5}{10} = 3$, $h''' = 2$, $h^{IV} = -3$, $h^{V} = -1$, $h^{VI} = 0$, d'où l'on déduit $\alpha^{VI} = -13$, $\beta^{VI} = -18$, $\gamma^{VI} = 8$, $\delta^{VI} = 11$. Donc en faisant $x = -13t - 18u$ et $y = 8t + 11u$, la forme $23x^2 + 76xy + 63y^2$ se change en $15t^2 + 40tu + 27u^2$.

De la solution du problème précédent on déduit facilement la solution de celui-ci : F *et* f *étant deux formes improprement équivalentes, trouver une transformation impropre de* F *en* f. Soit en effet $f = at^2 + 2btu + a'u^2$, la forme $g = ap^2 - 2bpq + a'q^2$, qui est opposée à f sera proprement équivalente à F. On n'a donc qu'à chercher une transformation propre de F en g; soit $x = \alpha p + \beta q$, $y = \gamma p + \delta q$ cette transformation; il est clair (nos 158 et 159) que F deviendra f par la transformation $x = \alpha t - \beta u$, $y = \gamma t - \delta u$, qui sera impropre.

Si donc les formes F, f sont équivalentes tant proprement qu'improprement, on pourra trouver une transformation propre et une transformation impropre.

179. Problème. *Étant données deux formes équivalentes* F, f, *trouver toutes les transformations de* F *en* f.

Si les formes F et f ne sont équivalentes que d'une manière, c'est-à-dire, proprement ou improprement, on cherchera par le n° précédent une transformation de F en f, et il est clair qu'il ne peut y en avoir d'autres que celles qui sont semblables

à celle-là. Si les formes F, f sont équivalentes des deux manières, on cherchera deux transformations, l'une propre, l'autre impropre. Soit $F=(A, B, C)$, $B^2-AC=-D$ et m le plus grand commun diviseur des nombres A, $2B$, C. Alors, par le n° 162 il est constant que toutes les transformations de F en f se déduiront d'une seule dans le premier cas, et que dans le second toutes les transformations propres se déduiront d'une transformation propre, et toutes les transformations impropres, d'une transformation impropre, pourvu qu'on ait toutes les solutions de l'équation $t^2+Du^2=m^2$. Dès qu'elles seront trouvées, le problème sera résolu.

Or comme on a $D=AC-B^2$, il s'ensuit que $4D=4AC-4B^2$, ou $\frac{4D}{m^2}=\frac{4AC}{m^2}-\left(\frac{2B}{m}\right)^2$; donc $\frac{4D}{m^2}$ est un nombre entier. Cela posé,

1°. Si $\frac{4D}{m^2}>4$, on aura $D>m^2$, et partant, dans l'équation $t^2+Du^2=m^2$, on a nécessairement $u=0$ et $t=\pm m$. Donc si F et f ne sont équivalentes que d'une manière, et qu'on ait une transformation $x=\alpha x'+\beta y'$, $y=\gamma x'+\delta y'$, on n'en trouvera pas d'autres que celle-là même qui résulte de la supposition $t=m$ (n° 162), et la transformation $x=-\alpha x'-\beta y'$, $y=-\gamma x'-\delta y'$; mais si F et f sont équivalentes des deux manières, et qu'on ait une transformation propre $x=\alpha x'+\beta y'$, $y=\gamma x'+\delta y'$, et une impropre $x=\alpha' x'+\beta' y'$, $y=\gamma' x'+\delta' y'$, on n'en trouvera pas d'autres que ces deux, qui naissent de la supposition $t=m$, et les deux $x=-\alpha x'-\beta y'$, $y=-\gamma x'-\delta y'$, ... $x=-\alpha' x'-\beta' y'$, $y=-\gamma' x'-\delta' y'$, que fournit la valeur $t=-m$.

2°. Si $\frac{4D}{m^2}=4$ ou $D=m^2$, l'équation $t^2+Du^2=m^2$ admettra quatre solutions : $t=m$, $u=0$; $t=-m$, $u=0$; $t=0$, $u=1$; $t=0$, $u=-1$. Donc si F, f sont équivalentes d'une seule manière, et qu'on ait la transformation $x=\alpha x'+\beta y'$, $y=\gamma x'+\delta y'$, on en tirera en tout les quatre suivantes :

$$\left.\begin{aligned} x&=\pm\alpha x'\pm\beta y', \\ y&=\pm\gamma x'\pm\delta y', \end{aligned}\right| \quad \left.\begin{aligned} x&=\mp\frac{\alpha B+\gamma C}{m}x'\mp\frac{\beta B+\delta C}{m}y', \\ y&=\pm\frac{\alpha A+\gamma B}{m}x'\pm\frac{\beta A+\delta B}{m}y'; \end{aligned}\right.$$

mais

mais si F et f sont équivalentes des deux manières, c'est-à-dire si, outre la transformation donnée, il y en a encore une qui soit dissemblable, cette dernière en fournira encore quatre, desorte qu'il y aura huit transformations. Au reste il est aisé de démontrer que si $D=m^2$, F et f sont toujours équivalentes des deux manières. En effet, comme on a alors $m^2=AC-B^2$, B lui-même sera divisible par m, et si l'on considère la forme $\left(\frac{A}{m}, \frac{B}{m}, \frac{C}{m}\right)$, son déterminant sera -1, et partant elle sera équivalente à l'une des formes $(1, 0, 1)$, $(-1, 0, -1)$. Or on voit facilement que la même transformation qui change $\left(\frac{A}{m}, \frac{B}{m}, \frac{C}{m}\right)$ en $(\pm 1, 0, \pm 1)$, changera la forme (A, B, C) en $(\pm m, 0, \pm m)$, qui est ambiguë; donc la forme (A, B, C) étant équivalente à une forme ambiguë, sera équivalente des deux manières, à la forme (a, b, c) (nos 163 et suiv.).

3°. Si $\frac{4D}{m^2}=3$ ou $4D=3m^2$, m sera nécessairement pair, et comme dans l'équation $t^2+Du^2=m^2$, il faut que $u^2<\frac{4}{3}$, on aura six solutions : $t=m$, $u=0$; $t=-m$, $u=0$; $t=\frac{1}{2}m$, $u=1$; $t=\frac{1}{2}m$, $u=-1$; $t=-\frac{1}{2}m$, $u=1$; $t=-\frac{1}{2}m$, $u=-1$. Si donc on connaît deux transformations dissemblables,

$$x=\alpha x'+\epsilon y', \quad y=\gamma x'+\delta y';$$
$$x=\alpha' x'+\epsilon' y', \quad y=\gamma' x'+\delta' y'$$

on en déduira douze autres ; savoir, six semblables à la première, et qui sont: $x=\pm\alpha x'\pm\beta y'$, $y=\pm\gamma x'\pm\delta y'$

$$x=\left(\pm\tfrac{1}{2}\alpha-\frac{\alpha B+\gamma C}{m}\right)x'+\left(\pm\tfrac{1}{2}\beta-\frac{\beta B+\delta C}{m}\right)y'$$
$$y=\left(\pm\tfrac{1}{2}\gamma+\frac{\alpha A+\gamma B}{m}\right)x'+\left(\pm\tfrac{1}{2}\delta+\frac{\beta A+\delta B}{m}\right)y',$$
$$x=\left(\pm\tfrac{1}{2}\alpha+\frac{\alpha B+\gamma C}{m}\right)x'+\left(\pm\tfrac{1}{2}\beta+\frac{\beta B+\delta C}{m}\right)y'$$
$$y=\left(\pm\tfrac{1}{2}\gamma-\frac{\alpha A+\gamma B}{m}\right)x'+\left(\pm\tfrac{1}{2}\delta-\frac{\beta A+\delta B}{m}\right)y',$$

et six semblables à la seconde, qu'on obtiendra en mettant dans celles-ci $\alpha, \beta, \gamma, \delta$ pour $\alpha', \beta', \gamma', \delta'$. Mais on peut faire voir que dans ce cas F et f sont équivalentes des deux manières; car la forme $\left(\frac{2A}{m}, \frac{2B}{m}, \frac{2C}{m}\right)$ aura $-\frac{D}{4m^2}=-3$ pour déterminant, et sera par-

conséquent équivalente à la forme $(\pm 1, 0, \pm 3)$ ou à celle-ci $(\pm 2, \pm 1, \pm 2)$ (n° 176), d'où l'on voit facilement que la forme (A,B,C) équivaut à l'une des formes $\left(\pm\frac{m}{2}, 0, \pm\frac{3m}{2}\right)$, $(\pm m, \pm\frac{1}{2}m, \pm m)$, qui sont toutes deux ambiguës. Donc, etc.

4°. Si $\frac{4D}{m^2} = 2$, on a $\left(\frac{2B}{m}\right)^2 = 4\frac{AC}{m^2} - 2$, et partant $\left(\frac{2B}{m}\right)^2 \equiv -2$ (mod. 4). Mais comme aucun quarré ne peut être $\equiv -2$ (mod. 4) (n° 103), cette hypothèse est inadmissible.

5°. Si $\frac{4D}{m^2} = 1$, on a $\left(\frac{2B}{m}\right)^2 = 4\frac{AC}{m^2} - 1 \equiv -1$ (mod. 4), ce qui est impossible; donc cette hypothèse est encore inadmissible.

Comme d'ailleurs D ne peut être ni $= 0$, ni < 0, il n'y a pas d'autres cas que ceux que nous venons de parcourir.

180. PROBLÈME. *Trouver toutes les représentations d'un nombre donné* M *par la forme* $ax^2 + 2bxy + cy^2 \ldots . F$, *dont le déterminant est négatif, les valeurs de* x *et de* y *étant premières entre elles.*

On a vu (n° 154) que l'on ne pouvait résoudre ce problème que dans le cas où $-D$ est résidu quadratique de M; on cherchera donc d'abord toutes les valeurs différentes, c'est-à-dire, incongrues de l'expression $\sqrt{-D}$ (mod. M); soient ces valeurs $\pm N$, $\pm N'$, $\pm N''$, etc. Pour rendre le calcul plus simple, on peut prendre toutes ces valeurs telles qu'elles ne soient pas $> \frac{1}{2}M$. Cela posé, comme une quelconque de ces représentations appartient à quelqu'une de ces valeurs, nous considérerons chacune en particulier.

Si les formes F, $\left(M, N, \frac{D+N^2}{M}\right)$ ne sont pas proprement équivalentes, il n'y aura aucune représentation de M qui appartienne à la valeur N (n° 168); mais si elles le sont, on n'a qu'à chercher une transformation propre de F en $\left(M, N, \frac{D+N^2}{M}\right)$, qui soit $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$, et l'on aura $x = \alpha$, $y = \gamma$ pour la représentation du nombre M par la forme F, qui appartient à la valeur N. Soit m le plus grand diviseur commun des nombres A, $2B$, C, et nous pourrons distinguer trois cas :

1°. Si $\frac{4D}{m^2} > 4$, il n'y aura pas d'autres représentations que ces deux-ci : $x = \alpha$, $y = \gamma$; $x = -\alpha$, $y = -\gamma$ (nos 169, 180).

2°. Si $\frac{4D}{m^2}=4$, il y aura quatre représentations : $x=\pm\alpha$, $y=\pm\gamma$; $x=\pm\frac{\alpha B+\gamma C}{m}$, $y=\pm\frac{\alpha A+\gamma B}{m}$.

3°. Si $\frac{4D}{m^2}=3$, il y aura six représentations :

$$x=\pm\alpha,\ y=\pm\gamma;\quad x=\pm\tfrac{1}{2}\alpha-\frac{\alpha B+\gamma C}{m},\ y=\pm\tfrac{1}{2}\gamma+\frac{\alpha A+\gamma B}{m};$$

$$x=\pm\tfrac{1}{2}\alpha+\frac{\alpha B+\gamma C}{m},\ y=\pm\tfrac{1}{2}\gamma-\frac{\alpha A+\gamma B}{m}.$$

On cherchera de la même manière les représentations que donnent les valeurs $-N$, $+N'$, $-N'$, etc.

181. La recherche des représentations du nombre M par la forme F, dans laquelle x et y ont des valeurs quelconques, peut se ramener au premier cas. Supposons que cette représentation ait lieu en faisant $x=\mu e$, $y=\mu f$, ensorte que μ soit le plus grand diviseur commun des nombres μe, μf, ou que e et f soient premiers entre eux ; on aura $M=\mu^2(Ae^2+2Bef+Cf^2)$, et parconséquent M est divisible par μ^2; et la substitution $x=e$, $y=f$ fournira une représentation du nombre $\frac{M}{\mu^2}$ par la forme F, dans laquelle x et y ont des valeurs premières entre elles. Si donc M n'est divisible par aucun quarré, il n'y aura pas de telles représentations ; mais s'il renferme des diviseurs quarrés, que nous appellerons μ^2, ν^2, π^2, etc ; On cherchera d'abord toutes les représentations du nombre $\frac{M}{\mu^2}$ par la forme (A, B, C), dans lesquelles les valeurs de x, y sont premières entre elles; ces valeurs multipliées par μ, donneront toutes les représentations de M, dans lesquelles μ est le plus grand commun diviseur de x et de y; de la même manière on trouvera toutes les représentations dans lesquelles ν est le plus grand commun diviseur de x et de y, etc.

On peut donc, par les méthodes que nous venons d'exposer, trouver toutes les représentations d'un nombre donné, par une forme donnée de déterminant négatif.

182. Descendons maintenant à quelques cas particuliers remarquables autant à cause de leur élégance, que par l'assiduité avec laquelle *Euler* s'en est occupé.

1°. Aucun nombre, à moins que son résidu quadratique ne soit -1, ne peut être représenté par la forme x^2+y^2, dans laquelle x et y sont premiers entre eux, ou sont décomposables en deux nombres quarrés premiers entre eux; mais tous les nombres qui jouiront de cette propriété pourront se décomposer en deux quarrés. Soit M un de ces nombres, et $\pm N$, $\pm N'$, $\pm N''$, etc. les valeurs de l'expression $\sqrt{-1}$ (mod. M); alors par le n° 176 la forme $\left(M, N, \frac{N^2+1}{M}\right)$ sera proprement équivalente à la forme $(1, 0, 1)$; soit $x=\alpha x'+\beta y'$, $y=\gamma x'+\delta y'$ une transformation propre de la forme $(1, 0, 1)$ en la forme $\left(M, N, \frac{N^2+1}{M}\right)$; on aura les quatre représentations suivantes du nombre M par la forme x^2+y^2, savoir, $x=\pm\alpha, y=\pm\gamma$; $x=\mp\gamma, y=\pm\alpha$. (2°. — n° 180).

Comme la forme $(1, 0, 1)$ est ambiguë, il est évident que la forme $\left(M, -N, \frac{N^2+1}{M}\right)$ lui est aussi proprement équivalente, et que la première se change en la seconde par la transformation propre $x=\alpha x'-\beta y'$, $y=-\gamma x'+\delta y'$, d'où naissent quatre représentations de M appartenantes à $-N$, $x=\pm\alpha$, $y=\mp\gamma$; $x=\pm\gamma$, $y=\mp\alpha$. Il suit de là qu'il y a huit représentations du nombre M, dont quatre appartiennent à la valeur N, et quatre à la valeur $-N$. Mais toutes ces représentations donnent la même décomposition du nombre M en deux quarrés, $M=\alpha^2+\gamma^2$, tant qu'on ne considère que les quarrés, et non l'ordre et les signes des racines.

Si donc il n'y a pas d'autres valeurs que N et $-N$ pour l'expression $\sqrt{-1}$ (mod. M), ce qui arrive, par exemple, toutes les fois que M est un nombre premier, M ne pourra être décomposé que d'une manière en deux quarrés. Or comme -1 est résidu de tous les nombres premiers de la forme $4n+1$ (n° 108), et qu'un nombre premier ne peut évidemment se partager en deux quarrés non premiers entre eux, nous aurons le théorème suivant.

Tout nombre premier de la forme $4n+1$ *peut être décomposé en deux quarrés, et ne peut l'être que d'une seule manière.* Ainsi :

$1 = 0+1$, $5 = 1+4$, $13 = 4+9$, $17 = 1+16$,
$29 = 4+25$, $37 = 1+36$, $41 = 16+25$, $53 = 4+49$,
$61 = 25+36$, $731 = 9+64$, $89 = 25+64$, $97 = 16+81$,
etc.

Ce théorème élégant a été donné par *Fermat*, mais *Euler* est le premier qui l'ait démontré, *Comm. nov. Petr. T. V. ann.* 1754 *et* 1755. *p.* 3. Dans le *T. IV*, il existe une dissertation sur le même sujet, *p.* 8; mais alors il n'était pas parvenu à son but.

Si donc un nombre de la forme $4n+1$ ne peut pas être décomposé en deux quarrés, ou peut l'être de plusieurs manières, on sera sûr que ce n'est pas un nombre premier.

Mais réciproquement, si l'expression $\sqrt{-1}$ (mod. M) a encore d'autres valeurs que N et $-N$, il y aura d'autres représentations de M. Ainsi, dans ce cas, M peut se décomposer en deux quarrés de plusieurs manières; par exemple : $65 = 1+64 = 16+49$, $221 = 25+196 = 100+121$.

Les autres représentations dans lesquelles x et y prennent des valeurs non premières entre elles, se trouvent facilement par notre méthode. Observons seulement que si le nombre M renferme des facteurs de la forme $4n+3$, dont on ne puisse pas le délivrer en le divisant par un quarré, ce qui arrivera toutes les fois que le nombre M renfermera des puissances impaires de ces facteurs, il ne pourra en aucune manière être décomposé en deux quarrés (*).

(*) Soit le nombre $M = 2^{\mu}.S.a^{\alpha}b^{\beta}c^{\gamma}$, etc., ensorte que a, b, c, etc. soient des facteurs premiers inégaux de la forme $4m+1$, et S le produit de tous les facteurs premiers de la forme $4n+3$; cette forme donnée au nombre M convient dans tous les cas; pour M impair, il suffit de faire $\mu = 0$; si M ne renferme aucun facteur de la forme $4n+3$, on fera $S = 1$: si S n'est pas un quarré, M ne pourra en aucune manière être décomposé en deux quarrés; mais si S est un quarré, il y aura $\frac{1}{2}(\alpha+1)(\beta+1)(\gamma+1)$, etc. décompositions de M, lorsque quelqu'un des nombres α, β, γ, etc. sont impairs, et il y en aura $\frac{1}{2}(\alpha+1)(\beta+1)(\gamma+1)$, etc. $+\frac{1}{2}$, quand tous les nombres α, β, γ, etc. seront pairs, tant qu'on ne fait attention qu'aux quarrés eux-mêmes. Ceux qui ont quelque habitude du calcul des combinaisons, déduiront sans peine de notre théorie générale la démonstration de ce théorème, auquel nous ne pouvons nous arrêter, non plus qu'à d'autres particuliers. (Voyez n° 105).

2°. Pour qu'un nombre puisse être représenté par la forme x^2+2y^2, x et y étant premiers entre eux, il faut que ce nombre ait -2 pour résidu. Soit donc M un nombre qui ait -2 pour résidu, et soit N une valeur de $\sqrt{-2}\,(\text{mod. } M)$; alors (n° 176) les formes $(1, 0, 2), \left(M, N, \frac{N^2+2}{M}\right)$ seront proprement équivalentes. Supposons que la première se change en la seconde par la transformation propre $x=\alpha x'+\beta y'$, $y=\gamma x'+\delta y'$, on aura deux représentations $x=\pm\alpha, y=\pm\gamma$ du nombre M appartenantes à la valeur N, et il n'y en aura pas d'autres (n° 180 — 1°.) D'ailleurs on voit, comme ci-dessus, que les représentations qui appartiennent à $-N$, sont $x=\pm\alpha, y=\mp\gamma$. Mais ces quatre représentations ne donnent qu'une seule décomposition du nombre M en un quarré et le double d'un quarré; et si l'expression $\sqrt{-2}\,(\text{mod. } M)$ n'a pas d'autres valeurs que N et $-N$, il n'y aura pas d'autre décomposition. De là, à l'aide des propositions du n° 116, on déduit facilement le théorème suivant :

Tout nombre premier de la forme $8n+1$ *ou* $8n+3$, *peut être décomposé en un quarré et le double d'un quarré, et cela d'une seule manière; ainsi*,

$1=1+0$, $3=1+2$, $11=9+2$, $17=9+8$, $19=1+18$, $41=9+32$, $43=25+18$, $59=9+50$, $67=49+18$, $73=1+72$, $83=81+2$, $89=81+8$, $97=25+72$, etc.

Ce théorème, ainsi que plusieurs autres semblables, était connu de *Fermat*; mais *Lagrange* l'a démontré le premier (*Suite des Recherches Arithmétiques. Nouv. Mém. de l'Ac. de Berlin*, 1775, *p.* 323). Euler avait déjà trouvé beaucoup de choses qui appartenaient à ce sujet (*Specimen de usu observationum in mathesi purâ. Com. nov. Petr. T. VI.*); mais la démonstration complète lui a toujours échappé, *p.* 220. On peut voir aussi, *T. VIII*, la dissertation intitulée : *Supplementum quorumdam theorematum arithmeticorum.*

3°. Par la même méthode on démontrera que tout nombre dont -3 est résidu quad., peut être représenté par la forme x^2+3y^2, ou par la forme $2x^2+2xy+2y^2$, de manière que x et y soient

premiers entre eux. Donc, comme -3 est résidu de tous les nombres de la forme $3n+1$ (n° 119), et qu'il n'y a que des nombres pairs qui peuvent être représentés par la forme $2x^2+2xy+2y^2$, on aura, comme plus haut, le théorème suivant :

Tout nombre premier de la forme $3n+1$, *peut se décomposer en un quarré et le triple d'un quarré, et cela d'une seule manière,*

$1=1+0$, $7=4+3$, $13=1+12$, $19=16+3$, $31=4+27$, $37=25+12$, $43=16+27$, $61=49+12$, $67=64+3$, $73=25+48$, etc.

Euler a donné le premier la démonstration de ce théorème dans le mémoire déjà cité (*Comm. nov. T. VIII.*). Nous pourrions continuer de la même manière, et démontrer, par exemple, que tout nombre premier de la forme $20n+1$, $20n+8$, $20n+7$, $20n+9$ (ceux dont -5 est résidu) peuvent être représentés par l'une ou l'autre des formes x^2+5y^2 et $2x^2+2xy+3y^2$; savoir, les nombres de la forme $20n+1$, $20n+9$, par la première; ceux de la forme $20n+3$, $20n+7$, par la seconde; tandis que les nombres doubles de ceux de la forme $20n+1$, $20n+9$ seraient représentés par la forme $2x^2+2xy+3y^2$, et que les nombres doubles de ceux de la forme $20n+3$, $20n+7$, le seraient par la forme x^2+5y^2 : mais chacun déduira facilement cette proposition, et une infinité d'autres particulières, tant de ce qui précède que de ce que nous allons exposer.

Nous passerons donc aux formes de déterminant positif, et comme leur nature diffère quand le déterminant est quarré, et quand il ne l'est pas, nous commencerons par exclure ici le premier cas, que nous considérerons ensuite à part.

183. Problème. *Étant donnée une forme quelconque* (a, b, a') *dont le déterminant soit un nombre* D *positif et non quarré, trouver une forme* (A, B, C) *qui lui soit proprement équivalente, et dans laquelle* B *soit positif et* $< \sqrt{D}$, *et dans laquelle* A, *s'il est positif ou* $-A$, *si* A *est négatif, soit compris entre* $\sqrt{D}+B$ *et* $\sqrt{D}-B$.

Nous supposons que les deux conditions ne se trouvent pas réunies dans la forme proposée, autrement il serait inutile d'en chercher

une autre ; et nous observerons qu'aucun des termes extrêmes ne peut être nul, car, sans cela, le déterminant serait un quarré (n° 171). Cela posé, soit $b' \equiv -b \pmod{a'}$, et compris entre $\sqrt{D}$ et $\sqrt{D} \mp a'$ (en prenant le signe supérieur quand a' est positif, et le signe inférieur quand il est négatif) ; il est aisé de démontrer que l'opération est possible, par un raisonnement semblable à celui du n° 3. Soit ensuite $a'' = \frac{b'^2 - D}{a'}$, a'' sera un nombre entier, parceque $b'^2 - D \equiv b^2 - D \equiv aa' \equiv a \pmod{a'}$. Si $a'' < a'$, on prendra encore $b'' \equiv -b' \pmod{a''}$, et compris entre $\sqrt{D}$ et $\sqrt{D} \mp a''$ (suivant que a'' sera positif ou négatif), et $a''' = \frac{b''^2 - D}{a''}$; si l'on a $a''' < a''$, on prendra encore $b''' \equiv -b \pmod{a''}$, et compris entre $\sqrt{D}$ et $\sqrt{D} \mp a'''$, et $a^{IV} = \frac{b'''^2 - D}{a'''}$, etc. On continuera ainsi jusqu'à ce que l'on parvienne à un terme $a^{(m+1)}$ qui ne soit pas plus petit que le précédent $a^{(m)}$, ce qui doit arriver nécessairement, car autrement une progression de nombres entiers pourrait décroître à l'infini. Alors en faisant $a^{(m)} = A$, $b^{(m)} = B$, $a^{(m+1)} = C$, la forme (A, B, C) satisfera à toutes les conditions. En effet :

1°. Puisque dans la suite de formes $(a,b,a'),(a',b',a''),(a'',b'',a''')$, etc. une quelconque est contiguë à celle qui la précède ; la dernière (A, B, C) sera proprement équivalente à la première.

2°. Comme B est compris entre $\sqrt{D}$ et $\sqrt{D} \mp A$, en prenant toujours le signe supérieur quand A est positif, et le signe inférieur quand il est négatif, il est clair que si l'on fait $\sqrt{D} - B = p$ et $B - (\sqrt{D} \mp A) = q$, p et q seront des nombres positifs, quel que puisse être le signe de $\sqrt{D} \mp A$. Or on s'assurera aisément que $q^2 + 2pq + 2p\sqrt{D} = D + A^2 - B^2$; or le premier membre est essentiellement positif, donc le second l'est aussi ; et comme $D = B^2 - AC$, il s'ensuit que $A^2 - AC > 0$; mais A n'est pas plus grand que C, donc nécessairement A et C sont de signe contraire ; donc aussi, puisque $B^2 = D + AC$, on a $B^2 < D$ et $B < \sqrt{D}$.

3°. Puisque $D < B^2$ et que $-AC = D - B^2$, on a $AC < D$ (abstraction faite du signe) ; et comme A est non $> C$, on a aussi

aussi $A < \sqrt{D}$; donc $\sqrt{D} \mp A$ sera positif, et partant, B qui est compris entre $\sqrt{D}$ et $\sqrt{D} \mp A$.

4°. Donc, à plus forte raison, $\sqrt{D} + B \mp A > 0$; et comme $\sqrt{D} - B \pm A = -q$, $q < 0$, $\pm A$ sera compris entre les limites $\sqrt{D} + B$ et $\sqrt{D} - B$.

Exemple. Soit la forme (67, 97, 140) dont le déterminant est 29 ; on trouvera la suite des formes : (67, 97, 140), (140, —97, 67), (67, —37, 20), (20, — 3, — 1), (— 1, 5, 4). La dernière est la forme cherchée.

Nous appellerons *formes réduites* les formes (A, B, C), dans lesquelles A, pris positivement, est compris entre $\sqrt{D} + B$ et $\sqrt{D} - B$, B étant positif et $< \sqrt{D}$, et le déterminant D étant positif et non quarré. Ces formes réduites diffèrent un peu de celles dont le déterminant est négatif; mais à cause de leur grande analogie, nous n'avons pas voulu introduire des dénominations différentes.

184. Si l'on pouvait reconnaître l'équivalence de deux formes réduites de déterminant positif, aussi facilement que nous l'avons fait pour celles de déterminant négatif (n° 172), on reconnaîtrait sans peine l'équivalence de deux formes quelconques de déterminant négatif : mais ici la chose est bien différente, et il peut arriver qu'un grand nombre de formes réduites soient équivalentes entre elles. Ainsi, avant d'entreprendre cette recherche, il est nécessaire d'examiner plus à fond la nature des formes réduites (de déterminant positif non quarré, ce qu'on doit toujours sous-entendre dans ce que nous aurons à dire).

1°. Si (a, b, c) est une forme réduite, a et c seront de signe contraire; car en nommant D le déterminant, on aura $ac = b^2 - D$, et partant négatif, puisque $b < \sqrt{D}$.

2°. Le nombre C pris positivement, est, ainsi que a, compris entre $\sqrt{D} + b$ et $\sqrt{D} - b$; car $-c = \frac{D - b^2}{a}$; donc, abstraction faite du signe, c sera compris entre $\frac{D - b^2}{\sqrt{D} + b} = \sqrt{D} - b$ et $\frac{D - b^2}{\sqrt{D} - b} = \sqrt{D} + b$.

3°. Il suit de là que (c, b, a) est aussi une forme réduite.

4°. a et c seront $< 2\sqrt{D}$; car chacun d'eux est $< \sqrt{D} + b$, et à plus forte raison $< 2\sqrt{D}$.

5°. b est compris entre $\sqrt{D}$ et $\sqrt{D} \mp a$ (en prenant le signe supérieur lorsque a est positif, et le signe inférieur quand il est négatif). En effet, comme $\pm a$ est compris entre $\sqrt{D} + b$ et $\sqrt{D} - b$, on aura $\pm a > \sqrt{D} - b$, ou $b > \sqrt{D} \mp a$: d'ailleurs $b < \sqrt{D}$, donc b est compris entre $\sqrt{D}$ et $\sqrt{D} \mp a$. On démontrerait absolument de la même manière que b est compris entre $\sqrt{D}$ et $\sqrt{D} \mp c$ (suivant que c est positif ou négatif).

6°. *Pour toute forme réduite* (a, b, c), *on peut en trouver une également réduite qui lui soit contiguë par l'une ou l'autre partie; mais on n'en pourra trouver qu'une.*

Soit $a' = c$, $b' \equiv -b \pmod{a'}$, et compris entre $\sqrt{D}$ et $\sqrt{D} \mp a'$, $c' = \frac{b'^2 - D}{a'}$; la forme (a', b', c') sera contiguë par la dernière partie, à la forme (a, b, c); et il est clair que s'il existe une forme réduite contiguë à la forme (a, b, c) par la dernière partie, elle ne peut être autre que (a', b', c'); il reste à faire voir que cette forme est effectivement réduite.

(A). Soit fait $\sqrt{D} + b \mp a' = p$, $\pm a' - (\sqrt{D} - b) = q$; $\sqrt{D} - b = r$; il suit de la définition des formes réduites de (2°), que p, q, r sont positifs; et si l'on fait encore $b' - \sqrt{(D \mp a')} = q'$, $\sqrt{D} - b' = r'$, q' et r' seront positifs, puisque b' tombe entre $\sqrt{D}$ et $\sqrt{D} \mp a'$; soit enfin $b + b' = \pm ma'$, m sera entier. Or il est clair que $p + q' = b + b'$, d'où il suit que $\pm ma' > 0$, et partant $m > 0$, et $m - 1$ non < 0; et comme on a encore $r + q' \pm ma' = 2b' \pm a'$, d'où l'on tire $2b' = r + q' \pm a'(m - 1)$, il s'ensuit que b' est nécessairement positif, et comme $b' = \sqrt{D} - r'$, que $b' < \sqrt{D}$.

(B). Or on a $r \pm ma' = \sqrt{D} + b$, d'où $r \pm (m - 1)a' = \sqrt{D} + b \mp a'$, donc $\sqrt{D} + b > \pm a'$; d'ailleurs $q' = \pm a' - (\sqrt{D} - b')$, donc $\pm a' > \sqrt{D} - b'$; donc enfin $\pm a'$ est compris entre $\sqrt{D} + b$ et $\sqrt{D} - b$.

La forme (a', b', c') est donc une forme réduite.

On démontrera de la même manière, que si l'on fait $'a = a$,

$'b \equiv -b \pmod{'c}$, et compris entre $\sqrt{D}$ et $\sqrt{D} \mp c$, $'a = \frac{'b^2 - D}{'c}$, $('a, 'b, 'c)$ sera une forme réduite. Il est manifeste d'ailleurs qu'elle est contiguë par la première partie à la forme (a, b, c), et que nulle autre forme réduite ne peut jouir de la même propriété.

Exemple. Soit la forme réduite $(5, 11, -14)$ dont le déterminant est 191, on trouvera les réduites $(-14, 3, 13)$ $(-22, 9, 5)$, dont la première est contiguë à $(5, 11, -14)$ par la dernière partie, et la seconde par la première partie.

7°. Si la forme réduite (a', b', c') est contiguë par la dernière partie à la forme (a, b, c), la réduite (c', b', a') sera contiguë par la première partie à la réduite (c, b, a); et si la réduite $('a, 'b, 'c)$ est contiguë par la première partie à la réduite (a, b, c), la réduite $('c, 'b, 'a)$ sera contiguë par la dernière partie à la réduite (c, b, a). Or les formes $(-'a, 'b, -'c)$, $(-a, b, -c)$, $(-a', b, -c')$ seront des réduites, et la seconde sera contiguë à la première, la troisième à la seconde, par la dernière partie; ou bien, la première sera contiguë à la seconde, la seconde à la troisième, par la première partie. Il en est de même des formes $(-c', b' - a')$, $(-c, b, -a)$, $(-'c, 'b, -'a)$. Ces vérités sont si évidentes, qu'elles n'ont pas besoin d'explication.

185. Le nombre des formes réduites d'un déterminant donné D est toujours fini, et elles peuvent se trouver de deux manières. Représentons indéfiniment par (a, b, c) toutes les formes réduites dont le déterminant est D, ensorte qu'il s'agisse de trouver toutes les valeurs de a, b, c.

Première méthode. On prendra pour a tous les nombres plus petits que $2\sqrt{D}$, soit positivement, soit négativement, dont D est résidu quadratique; et pour chaque valeur de a, on fera b égal aux différentes valeurs de l'expression $\sqrt{D} \pmod{a}$ comprises entre $\sqrt{D}$ et $\sqrt{D} \mp a$, et $c = \frac{b^2 - D}{a}$. S'il en résulte quelques formes dans lesquelles $\pm a$ sorte des limites $\sqrt{D} + b$ et $\sqrt{D} - b$, il faudra les rejeter.

Deuxième méthode. On prendra pour b tous les nombres positifs $< \sqrt{D}$; pour chaque valeur de b, on décomposera $b^2 - D$ de

toutes les manières possibles en deux facteurs qui soient compris entre $\sqrt{D}+b$ et $\sqrt{D}-b$, abstraction faite du signe, et l'on fera l'un d'eux $=a$ et l'autre $=c$. Il est évident que chaque décomposition en facteurs donnera deux formes, car l'un quelconque des deux facteurs peut être pris pour a, et l'autre pour c.

Exemple. Soit $D=79$; par la première méthode, on trouve pour a vingt-deux valeurs : $\pm 1, 2, 3, 5, 6, 7, 9, 10, 13, 14, 15$, d'où résultent les 19 formes suivantes :

$(1,8,-15),(2,7,-15),(3,7,-10),(3,8,-5),(5,7,-6),$
$(5,8,-3),(6,5,-9),(6,7,-5),(7,3,-10),(7,4,-9),$
$(9,4,-7),(9,5,-6),(10,3,-7),(10,7,-3),(13,1,-6),$
$(14,3,-5),(15,2,-5),(15,7,-2),(15,8,-1).$

On en trouvera encore autant en changeant les signes des termes extrêmes, par exemple : $(-1,8,15),(-2,7,+15)$, etc., ensorte qu'on en aura trente-huit en tout. Mais comme $\pm a$ doit être compris entre les limites $\sqrt{D}+b$ et $\sqrt{D}-b$, il faut rejeter les six formes : $(\pm 13,1,\mp 6),(\pm 14,3,\mp 5),(\pm 15,2\mp 5)$; et les trente-deux qui restent, forment toutes les formes réduites.

Par la seconde méthode, on déduit les mêmes formes dans l'ordre suivant :

$(\pm 7,3,\mp 10),(\pm 10,3,\mp 7),(\pm 7,4,\mp 9),(\pm 9,4,\mp 7),$
$(\pm 6,5,\mp 9),(\pm 9,5,\mp 6),(\pm 2,7,\mp 15),(\pm 3,7,\mp 10),$
$(\pm 5,7,\mp 6),(\pm 6,7,\mp 5),(\pm 10,7,\mp 3),(\pm 15,7,\mp 2),$
$(\pm 1,8,\mp 15),(\pm 3,8,\mp 5),(\pm 5,8,\mp 3),(\pm 15,8,\mp 1).$

186. Soit F une forme réduite de déterminant D, et la forme réduite F' contiguë à F par la dernière partie; soit de même la réduite F'' contiguë à F', F''' à F'', etc., il est clair que toutes les formes F', F'', F''', etc. sont absolument déterminées, et qu'elles sont proprement équivalentes entre elles et à la forme F. Mais comme le nombre des formes réduites de déterminant donné est toujours fini, il est manifeste que toutes les formes F, F', F'', etc. ne peuvent pas être différentes. Supposons que $F^{(m)}$ et $F^{(m+n)}$ soient identiques, $F^{(m-1)}$ et $F^{(m+n-1)}$ sont réduites et contiguës par la première partie à la même forme réduite ; et partant identiques, on a de même $F^{(m-2)}=F^{(m+n-2)}$, etc., et enfin $F=F^{(n)}$. Ainsi

dans la progression F, F', F'', etc., pourvu qu'on la continue assez loin, on retrouvera enfin la forme F; et si nous supposons que $F^{(n)}$ soit la première identique avec F, c'est-à-dire que toutes les formes $F', F'', \ldots F^{(n-1)}$ soient différentes de F, il est aisé de voir que toutes les formes $F, F', \ldots F^{(n-1)}$ seront différentes entre elles. Nous appellerons l'ensemble de toutes ces formes *la période de la forme* F; si donc on continue la suite après la dernière forme de la période, les formes F', F'', etc. reparaîtront de nouveau, et la suite entière sera composée de cette période répétée à l'infini.

La progression F, F', F'', etc. peut aussi être continuée en sens inverse, en plaçant avant la forme F une forme $'F$ qui lui soit contiguë par la première partie, avant celle-ci une forme F'', etc. On aura de cette manière une suite de formes infinie dans les deux sens,

$$\ldots\ldots {}''F, {}'F, F, F', F'', F''', \ldots\ldots,$$

et l'on verra facilement que $'F$ est identique avec $F^{(n-1)}$, $''F$ avec $F^{(n-2)}$, etc. et que parconséquent la suite est aussi formée, vers la gauche, de la période de la forme F répétée à l'infini.

Si l'on attribue aux formes F, F', F'', etc. $'F, ''F$, etc. les indices 0, 1, 2, etc. $-1, -2$, etc., et généralement à la forme $F^{(m)}$ l'indice m, à la forme ${}^{(m)}F$ l'indice $-m$, il est clair *que des formes quelconques de la suite seront identiques ou différentes, selon que leurs indices sont congrus ou incongrus, suivant le module* n. Il ne faut pas confondre les indices dont il est question ici, avec ceux du n° 57. Les premiers ne sont que des accens, et les derniers de véritables exposans.

Exemple. La période de la forme $(3, 8, -5)$, dont le déterminant est 79, se trouve ainsi être :

$$(3,8,-5), (-5,7,6), (6,5,-9), (-9,4,7), (7,3,-10), (-10,7,3);$$

après la dernière, la première $(3, 8, -5)$ reparaît, et l'on a ici $n = 6$.

187. Voici encore quelques observations générales sur ces périodes.

1°. Si les formes F, F', F'', etc. $'F, ''F$, etc. sont présentées

comme il suit : $(a, b, -a')$, $(-a', b', a'')$, $(a'', b'', -a''')$, etc. $(-{}'a, {}'b, a)$, $({}''a, {}''b, -{}'a)$, $(-{}'''a, {}'''b, {}''a)$, etc. tous les nombres a, a', a'', a''', etc. ${}'a, {}''a, {}'''a$, etc. auront le même signe (n° 184—1°.), et les nombres b, b', b'', b''', etc. ${}'b, {}''b$, etc. seront nécessairement positifs.

2°. Il suit de là que le nombre n des formes de la période est toujours *pair;* car le premier terme d'une forme quelconque $F^{(m)}$ de cette période, aura évidemment le même signe que le premier terme de la forme F si m est pair, et le signe contraire si m est impair; or F et F^n sont identiques, donc n est un nombre pair.

3°. Dans le calcul indiqué (n° 184—6°.), pour trouver les différentes formes F, F', F'', etc., au lieu des expressions

$$a'' = \frac{D - b'^2}{a'}, \qquad a''' = \frac{D - b''^2}{a''}, \qquad a^{IV} = \frac{D - b'''^2}{a'''}, \quad \text{etc.}$$

on peut substituer les suivantes, qui sont plus commodes, lorsque D est un grand nombre, et qui s'en déduisent facilement :

$$a'' = \frac{(b+b')(b-b')}{a'} + a, \quad a''' = \frac{(b'+b'')(b'-b'')}{a''} + a', \quad a^{IV} = \frac{(b''+b''')(b''-b''')}{a'''} + a'', \text{ etc.}$$

4°. Une forme quelconque $F^{(m)}$ contenue dans la période de F conduit à la même période qu'elle; ensorte que la période de cette forme sera $F^{(m)}, F^{(m+1)} \ldots F^{(n-1)}, F, F' \ldots F^{(m-1)}$, dans laquelle les mêmes formes reviennent dans le même ordre, et qui ne diffère de la première que par le commencement et la fin.

5°. Il suit de là que toutes les formes réduites de même déterminant D peuvent être distribuées en périodes. On prendra une quelconque F de ces formes, et l'on cherchera sa période que nous désignerons par P. Si P ne renferme pas toutes les formes réduites dont le déterminant est D, soit G une des formes qui n'y est pas contenue, et Q sa période, il est clair que P et Q n'ont aucune forme commune, car autrement G serait contenue dans P et les périodes coïncideraient. Si P et Q n'épuisent pas encore toutes les formes réduites, une de celles qui y manquent fournira une troisième période R, qui n'aura aucune forme commune avec P et Q, et ainsi de suite, jusqu'à ce que toutes les

formes réduites soient épuisées. Ainsi, par exemple, les formes réduites dont le déterminant est 79 se distribuent en six périodes,

1....(1, 8, —15), (—15, 7, 2), (2, 7, —15), (—15, 8, 1).
2....(—1, 8, 15), (15, 7, —2), (—2, 7, 15), (15, 8, —1).
3....(3, 8, —5), (—5, 7, 6), (6, 5, —9), (—9, 4, 7), (7, 3, —10), (—10, 7, 3).
4....(—3, 8, 5), (5, 7, —6), (—6, 5, 9), (9, 4, —7), (—7, 3, 10), (10, 7, —3).
5....(5, 8, —3), (—3, 7, 10), (10, 3, —7), (—7, 4, 9), (9, 5, —6), (—6, 7, 5).
6....(—5, 8, 3), (3, 7, —10), (—10, 3, 7), (7, 4, —9), (—9, 5, 6), (6, 7, —5).

6°. Nous nommerons *formes associées*, celles qui sont composées des mêmes termes, mais placés dans un ordre inverse, comme $(a, b, -a')$, $(-a', b, a)$. On voit alors facilement (n° 184, 7°.) que si la période de la forme réduite F est F, F', F'', etc., que f soit associée à F, f' à $F^{(n-1)}$, f'' à $F^{(n-2)}$, etc. $f^{(n-2)}$ à F'', $f^{(n-1)}$ à F', la période de f sera $f, f', f''\ldots f^{(n-1)}$, et contiendra, partant, le même nombre de formes que la période de F. Nous nommerons *périodes associées* celles qui sont ainsi composées de formes associées. Les périodes 3 et 6, 4 et 5 de l'exemple précédent sont dans ce cas-là.

7°. Mais il peut arriver aussi que la forme f se trouve elle-même dans la période de son associée, comme aux périodes 1 et 2 de notre exemple, et que parconséquent la période de la forme F coïncide avec celle de la forme f, c'est-à-dire que *la période de la forme* F *soit elle-même son associée*. Toutes les fois que cette circonstance a lieu, la période renferme deux formes ambiguës. Supposons en effet que la période de la forme F contienne $2n$ formes, ou que $F = F^{(2n)}$. Soit $2m+1$ l'indice de la forme f dans la période de F (car F et f ont leurs premiers termes de signe contraire, (2°.), c'est-à-dire que $F^{(2m+1)}$ et F soient associées; il est évident qu'alors F' et $F^{(2m)}$ seront aussi associées, de même F'' et $F^{(2m-1)}$, etc., et partant $F^{(m)}$ et $F^{(m+1)}$. Soit $F^{(m)} = (a^{(m)}, b^{(m)}, -a^{(m+1)})$, $F^{(m+1)} = (-a^{(m+1)}, b^{(m+1)}, a^{(m+2)})$; on aura $b^{(m)} + b^{(m+1)} \equiv 0 \pmod{a^{(m+1)}}$; mais par la définition des formes associées $b^{(m)} = b^{(m+1)}$; donc $2b^{(m+1)} \equiv 0 \pmod{a^{(m+1)}}$, c'est-à-dire que la forme $F^{(m+1)}$ est ambiguë De même, les formes $F^{(2n)}$ et $F^{(2m+1)}$ sont associées, donc aussi $F^{(2m+2)}$ et $F^{(2n-1)}$, $F^{(2m+3)}$ et $F^{(2n-2)}$, etc. et enfin $F^{(m+n)}$ et $F^{(m+n+1)}$, dont la dernière sera ambiguë, comme on le prouvera par un raisonnement semblable. Mais comme $m+1$

et $m+n+1$ sont incongrus suivant le module $2n$, les formes $F^{(m+1)}$ et $F^{(m+n+1)}$ ne seront pas identiques (n° 186, où n représente ce que représente ici $2n$). Dans la période 1, les formes $(1, 8, -15)$, $(2, 7, -15)$; dans la période 2, les formes $(-1, 8, 15)$, $(-2, 7, 15)$ sont ambiguës.

8°. Réciproquement, *toute période qui renferme une forme ambiguë sera elle-même son associée.* En effet, on voit aisément que si $F^{(m)}$ est une forme réduite ambiguë, sa forme associée, qui est aussi réduite, lui sera en même temps contiguë par la première partie, c'est-à-dire que $F^{(m-1)}$ et $F^{(m)}$ sont associées. Mais alors toute la période sera elle-même son associée. Il suit de là que dans une période, il faut nécessairement qu'il y ait plus d'une forme ambiguë; mais il ne peut y en avoir plus de deux.

En effet, supposons que dans la période de la forme F, il se trouve trois formes ambiguës $F^{(\lambda)}$, $F^{(\mu)}$, $F^{(\nu)}$, λ, μ, ν étant $< 2n$, et inégaux. Alors les formes $F^{(\lambda-1)}$ et $F^{(\lambda)}$ seront associées; de même $F^{(\lambda-2)}$ et $F^{(\lambda+1)}$, etc. et enfin F et $F^{(2\lambda-1)}$; par la même raison, F et $F^{(2\mu-1)}$, F et $F^{(2\nu-1)}$, seront associées. Donc les formes $F^{(2\lambda-1)}$, $F^{(2\mu-1)}$, $F^{(2\nu-1)}$ seront identiques, et partant leurs indices seront congrus suivant le module $2n$; donc aussi $\lambda \equiv \mu \equiv \nu \pmod{2n}$, ce qui est absurde, puisqu'il est évident qu'il n'y a pas trois nombres différens congrus suivant le module $2n$, et plus petits que lui.

188. Comme toutes les formes de la même période sont proprement équivalentes, on est porté naturellement à chercher si deux formes prises dans des périodes différentes peuvent être équivalentes. Mais avant de prouver que la chose est impossible, il est nécessaire que nous nous occupions de la transformation des formes réduites.

Comme dans ce qui va suivre il sera souvent question de la transformation des formes, et afin d'éviter autant qu'il est possible la prolixité, nous nous servirons dorénavant de la manière suivante d'écrire. Si une forme $LY^2+2MXY+NY^2$ se change en

en la forme $lx^2+2mxy+ny^2$ par la substitution $X=\alpha x+\beta y$, $Y=\gamma x+\delta y$, nous dirons plus simplement que (L, M, N) se change en (l, m, n) par la substitution $\alpha, \beta, \gamma, \delta$. De cette manière il ne sera pas nécessaire de représenter par des caractères particuliers les indéterminées des formes dont il sera question; mais il est clair qu'il faut bien distinguer dans toutes les formes la *première* et la *seconde* indéterminée.

Soit proposée la forme réduite $(a, b, -a')=f$ et dont le déterminant est D; on formera comme au n° 186 une suite de formes réduites qui s'étende indéfiniment dans les deux sens, $\ldots .{}''f, {}'f, f, f', f''\ldots$ ensorte que l'on ait

$$f'=(-a', b', a''),\quad f''=(a'', b'', -a'''),\ \text{etc.}$$
$${}'f=(-{}'a, {}'b, a),\quad {}''f=({}''a, {}''b, -{}'a),\ \text{etc.}$$

Faisons

$$\frac{b+b'}{-a'}=h',\ \frac{b'+b''}{a''}=h'',\ \frac{b''+b'''}{-a'''}=h''',\ \text{etc.}\quad \frac{{}'b+b}{a}=h,\ \frac{{}''b+{}'b}{-{}'a}={}'h,\ \frac{{}'''b+{}''b}{{}''a}={}''h,\ \text{etc}$$

Il est clair que si l'on calcule les nombres α', α'', etc., β', β'', etc. par le moyen des relations suivantes (comme au n° 177).

$\alpha'=0\ldots\ldots$	$\beta'=-1\ldots\ldots$	$\gamma'=1\ldots\ldots$	$\delta'=h'$
$\alpha''=\beta'\ldots\ldots$	$\beta''=h''\beta'\ldots\ldots$	$\gamma''=\delta'\ldots\ldots$	$\delta''=h''\delta'-1$
$\alpha'''=\beta''\ldots\ldots$	$\beta'''=h'''\beta''-\beta'\ldots\ldots$	$\gamma'''=\delta''\ldots\ldots$	$\delta'''=h'''\delta''-\delta'$
$\alpha^{IV}=\beta'''\ldots\ldots$	$\beta^{IV}=h^{IV}\beta'''-\beta''\ldots\ldots$	$\gamma^{IV}=\delta'''\ldots\ldots$	$\delta^{IV}=h^{IV}\delta'''-\delta''$
etc.	etc.	etc.	etc.

f se changera en $\left\{\begin{matrix} f' \\ f'' \\ f''' \\ \text{etc.}\end{matrix}\right\}$ par la substitution $\left\{\begin{matrix} \alpha', \beta', \gamma', \delta' \\ \alpha'', \beta'', \gamma'', \delta'' \\ \alpha''', \beta''', \gamma''', \delta''' \\ \text{etc.}\end{matrix}\right.$

et toutes ces transformations seront propres.

Comme ${}'f$ se change en f par la substitution propre $0, 1, 1, h$ (n° 161), f se changera en ${}'f$ par la substitution propre $h, 1, -1, 0$; par la même raison ${}'f$ se changera en ${}''f$ par la substitution propre ${}'h, 1, -1, 0$, ${}''f$ en ${}'''f$ par la substitution propre ${}''h, 1, -1, 0$, etc.; de là, et au moyen du n° 159, on déduira comme au n° 177 les relations suivantes entre ${}'\alpha$, ${}''\alpha$, etc. ${}'\beta$, ${}''\beta$, etc.

$'\alpha = h$	$'\beta = 1$	$'\gamma = -1$	$'\delta = 0$
$''\alpha = 'h'\alpha - 1$	$''\beta = 'a$	$''\gamma = 'h'\gamma$	$''\delta = 'c$
$'''\alpha = ''h''\alpha - 'a$	$'''\beta = ''a$	$'''\gamma = ''h''\gamma - 'c$	$'''\delta = ''c$
$^{IV}\alpha = '''h'''\alpha - ''a$	$^{IV}\beta = '''a$	$^{IV}\gamma = '''h'''\gamma - ''c$	$^{IV}\delta = '''c$
etc.	etc.	etc.	etc.

et,

f se changera en $\left\{ \begin{matrix} 'f \\ ''f \\ '''f \\ \text{etc.} \end{matrix} \right\}$ par la substitution $\left\{ \begin{matrix} 'a, & 'b, & 'c, & 'd \\ ''a, & ''b, & ''c, & ''d \\ '''a, & '''b, & '''c, & '''d \\ \text{etc.} \end{matrix} \right.$

et toutes ces transformations seront propres.

Si l'on fait $\alpha = 1$, $\beta = 0$, $\gamma = 0$, $\delta = 1$, ces nombres auront la même relation avec la forme f que α', β', γ', δ' avec f', α'', β'', γ'', δ'' avec la forme f'', etc., $'\alpha$, $'\beta$, $'\gamma$, $'\delta$ avec $'f$, etc. C'est-à-dire, que par la substitution α, β, γ, δ, la forme f se change en f; mais alors les suites α', α'', α''', etc. $'\alpha$, $''\alpha$, $'''\alpha$, etc., par l'intercalation de α, se joindront parfaitement, et n'en feront plus qu'une seule allant à l'infini dans les deux sens, et dont tous les termes suivent la même loi : .... $'''\alpha'$, $''\alpha$, $'\alpha$, α, α', α'', α''' ..... La loi de cette suite est celle-ci :

$$'''\alpha + '\alpha = ''h''\alpha,\ \alpha'' + \alpha = 'h'\alpha,\ '\alpha + \alpha' = h\alpha,\ \alpha + \alpha'' = h'\alpha',\ \alpha' + \alpha''' = h''\alpha'', \text{ etc.}$$

ou généralement, en regardant l'accent négatif écrit à droite comme l'accent positif écrit à gauche, $\alpha^{(m-1)} + \alpha^{(m+1)} = h^{(m)}\alpha^{(m)}$.

De même la suite $''\beta$, $'\beta$, β, β', β'', etc. sera continue, et la loi de ses termes sera $\beta^{(m-1)} + \beta^{(m+1)} = h^{(m+1)}\beta^{(m)}$; cette suite est la même que la précédente, en remplaçant $'\alpha$ par β'', α par $'\beta$, α' par β, etc.

La loi de la progression $''\gamma$, $'\gamma$, γ, γ', γ'', etc. sera $\gamma^{(m-1)} + \gamma^{(m+1)} = h^{(m)}\gamma^{(m)}$, et celle de la progression : $''\delta$, $'\delta$, δ, δ', δ'', etc. sera $\delta^{(m-1)} + \delta^{(m+1)} = h^{(m+1)}\delta^{(m)}$, et en outre généralement $\delta^{(m)} = \gamma^{(m+1)}$.

Exemple. La forme $(3, 8, -5) = f$ se changera ainsi

en	par la substitution,				
$^{VIII}f = (-10, 7, 3)$.....	-805,	-152,	$+143$,	$+27$	
$^{VI}f = (3, 8, -5)$.....	-152,	$+45$,	$+27$,	-8	
$^{V}f = (-5, 7, 6)$.....	$+45$,	$+17$,	-8,	-3	
$^{IV}f = (6, 5, -9)$.....	$+17$,	-11,	-3,	$+2$	
$^{''}f = (-9, 4, 7)$.....	-11,	-6,	$+2$,	$+1$	
$^{''}f = (7, 3, -10)$.....	-6,	$+5$,	$+1$,	-1	
$^{'}f = (-10, 7, 3)$.....	$+5$,	$+1$,	-1,	0	
$f = (3, 8, -5)$.....	$+1$,	0,	0,	$+1$	
$f' = (-5, 7, 6)$.....	0,	-1,	$+1$,	-3	
$f'' = (6, 5, -9)$.....	-1,	-2,	-3,	-7	
$f''' = (-9, 4, 7)$.....	-2,	$+3$,	-7,	$+10$	
$f^{IV} = (7, 3, -10)$.....	$+3$,	$+5$,	$+10$,	$+17$	
$f^{V} = (-10, 7, 3)$.....	$+5$,	-8,	$+17$,	-27	
$f^{VI} = (3, 8, -5)$.....	-8,	-45,	-27,	-152	
$f^{VII} = (-5, 7, 6)$.....	-45,	$+143$,	-152,	$+483$	

etc.

189. A l'égard des calculs précédens, nous ferons plusieurs remarques.

1°. Tous les nombres a, a', a'', etc. $'a$, $''a$, etc. auront le même signe, tous les nombres b, b', b'', etc. $'b$, $''b$, etc. seront positifs, et les nombres $\ldots''h, 'h, h, h', h''$, etc. seront alternatifs, c'est-à-dire, que si a, a', etc. sont tous positifs, $h^{(m)}$ ou $^{(m)}h$ sera positif quand m est pair, et négatif quand m est impair; et le contraire aura lieu, si a, a', etc. sont tous négatifs.

2°. Si a est positif et partant $h' < 0$, $h'' > 0$, etc., on aura $\alpha'' = -1$, < 0; $\alpha''' = h''\alpha''$, < 0 et $>$ ou $= \alpha''$; $\alpha^{IV} = h'''\alpha''' - \alpha''$, > 0 et $> \alpha'''$, puisque $h'''\alpha''' > 0$ et $\alpha'' < 0$; $\alpha^{V} = h^{IV}\alpha^{IV} - \alpha'''$, > 0 et $> \alpha^{IV}$, puisque $h^{IV}\alpha^{IV} > 0$ et $\alpha''' < 0$, etc. On conclut de là facilement que les termes de la suite α, α', α'', α''', etc. vont toujours en augmentant, et qu'il y en a toujours deux positifs et deux négatifs alternativement, et de manière que $\alpha^{(m)}$ a le signe $+, +, -, -$, suivant que $m \equiv 0, 1, 2, 3 \pmod 4$; si a est négatif, on trouvera par un raisonnement semblable que les termes vont en augmentant, et que le signe du terme $\alpha^{(m)}$ est $+, -, -, +$, suivant que $m \equiv 0, 1, 2, 3 \pmod 4$.

3°. On trouve de même que les quatre suites infinies $\alpha', \alpha'', \alpha'''$, etc.; $\gamma, \gamma', \gamma''$, etc.; $\alpha', \alpha, {}'\alpha, {}''\alpha$, etc.; $\gamma, {}'\gamma, {}''\gamma$, etc., vont en augmentant, ainsi que les suivantes, qui leur sont équivalentes, β, β', β'', etc.; ${}'\delta, \delta, \delta'$, etc.; $\beta, {}'\beta, {}''\beta$, etc.; $\delta, {}''\delta, {}'''\delta$, etc., et suivant que $m \equiv 0, 1, 2, 3 \pmod 4$, le signe de $\alpha^{(m)}$ est: $+, \pm, -, \mp$; celui de $\beta^{(m)}$: $\pm, -, \mp, +$; celui de $\gamma^{(m)}$: $\pm, +, \mp, -$; celui de $\delta^{(m)}$: $+, \mp, -, \pm$; celui de ${}^{(m)}\alpha$: $+, \pm, -, \mp$; celui de ${}^{(m)}\beta$: $\mp, +, \pm, -$; celui de ${}^{(m)}\gamma$: $\mp, -, \pm, +$; celui de ${}^{(m)}\delta$: $+, \mp, -, \pm$; en prenant les signes supérieurs quand a est positif, et les inférieurs quand a est négatif. Il est surtout important de remarquer que m indiquant un accent positif quelconque, $\alpha^{(m)}$ et $\gamma^{(m)}$ auront les mêmes signes quand a est positif, et des signes contraires quand a est négatif; il en est de même pour $\beta^{(m)}$ et $\delta^{(m)}$, et le contraire a lieu pour ${}^{(m)}\alpha$ et ${}^{(m)}\gamma$, ${}^{(m)}\beta$ et ${}^{(m)}\delta$.

4°. On peut présenter, d'après la notation du n° 32, les valeurs de $\alpha^{(m)}$, $\beta^{(m)}$, etc. En posant $\mp h' = k'$, $\pm h'' = k''$, $\mp h''' = k'''$, etc.; $\pm h = k$, $\mp {}'h = {}'k$, $\pm {}''h = {}''k$, etc., de manière que k', k'', etc., $k, {}'k$, etc. soient positifs, on aura

$$\alpha^{(m)} = \pm [k'', k''', k^{IV} \ldots . k^{(m-1)}] \ldots . \beta^{(m)} = \pm [k'', k''', k^{IV} \ldots . k^{(m)}]$$
$$\gamma^{(m)} = \pm [k', k'', k''' \ldots . k^{(m-1)}] \ldots . \delta^{(m)} = \pm [k', k'', k''' \ldots . k^{(m)}]$$
$${}^{(m)}\alpha = \pm [k, {}'k, {}''k \ldots . {}^{(m-1)}k] \ldots . {}^{(m)}\beta = \pm [k, {}'k, {}''k \ldots {}^{(m-2)}k]$$
$${}^{(m)}\gamma = \pm [{}'k, {}''k, {}'''k \ldots . {}^{(m-1)}k] \ldots . {}^{(m)}\delta = \pm [{}'k, {}''k, {}'''k \ldots {}^{(m-2)}k].$$

Quant aux signes, ils doivent être déterminés d'après ce qui vient d'être dit (3°). Au moyen de ces formules, dont nous omettons la démonstration parcequ'elle est très-facile, le calcul devient extrêmement simple.

190. LEMME. *Si* m, μ, m', n, ν, n' *désignent des nombres entiers quelconques, mais tels qu'aucun des trois derniers ne soit* $= 0$, *que* $\frac{\mu}{\nu}$ *soit compris entre* $\frac{m}{n}$ *et* $\frac{m'}{n'}$, *et qu'on ait* $mn' - nm' = \mp 1$, *le dénominateur* ν *sera plus grand que* n *et* n'.

En effet $\mu nn'$ sera compris entre $\nu mn'$ et $\nu m'n$, et partant différera de chacune de ces limites d'une quantité plus petite que leur propre différence, ainsi $\nu mn' - \nu m'n > \mu nn' - \nu mn'$, et

$> \mu nn' - \nu m'n$; ce qui donne $\nu > n'(\mu n - \nu m)$ et $> n(\mu n' - \nu m)$, et comme $\mu n - \nu m$, ni $\mu n' - \nu m'$ ne peuvent être égaux à zéro, car il en résulterait $\frac{m}{n} = \frac{\mu}{\nu}$, ou $\frac{m'}{n'} = \frac{\mu}{\nu}$, ce qui est contre l'hypothèse, et qu'ils ne peuvent être plus petits que 1, il s'ensuit qu'on a $\nu > n'$ et $> n$.

Il est donc clair que l'on ne peut avoir $\nu = 1$; c'est-à-dire que si $mn' - m'n = \pm 1$, aucun nombre entier ne peut être compris entre les fractions $\frac{m}{n}$ et $\frac{m'}{n'}$, et qu'à plus forte raison zéro ne peut y être compris, ce qui prouve que ces fractions ne peuvent être de signes contraires.

191. THÉORÈME. *Si la forme réduite* (a, b, $-$a'), *dont le déterminant est* D, *se change en la forme réduite* (A, B, $-$A'), *de même déterminant, par la transformation* $\alpha, \beta, \gamma, \delta$: 1°. $\frac{\pm\sqrt{D} - b}{a}$ *tombera entre* $\frac{\alpha}{\gamma}$ *et* $\frac{\beta}{\delta}$, (*pourvu que l'on n'ait ni* $\gamma = 0$, *ni* $\delta = 0$, *c'est-à-dire que les deux limites soient finies*), *en prenant le signe supérieur, quand les deux limites sont de même signe que* a, *et le signe inférieur, quand elles sont toutes deux de signe contraire à celui de* a (*); 2°. $\frac{\pm\sqrt{D} + b}{a'}$ *tombera entre* $\frac{\gamma}{\alpha}$ *et* $\frac{\delta}{\beta}$, (*pourvu qu'on n'ait ni* $\alpha = 0$, *ni* $\beta = 0$), *en prenant les signes comme ci-dessus.*

On a les équations

$$a\alpha^2 + 2b\alpha\gamma - a'\gamma^2 = A \ldots (1) \qquad a\beta^2 + 2b\beta\delta - a'\delta^2 = -A' \ldots (2),$$

d'où l'on tire

$$\frac{\alpha}{\gamma} = \frac{\pm\sqrt{\left(D + \frac{aA}{\gamma^2}\right)} - b}{a} \ldots\ldots (3) \qquad \frac{\beta}{\delta} = \frac{\pm\sqrt{\left(D - \frac{aA}{\alpha^2}\right)} - b}{a} \ldots\ldots (4)$$

$$\frac{\gamma}{\alpha} = \frac{\pm\sqrt{\left(D - \frac{a'A'}{\alpha^2}\right)} + b}{a'} \ldots\ldots (5) \qquad \frac{\delta}{\beta} = \frac{\pm\sqrt{\left(D + \frac{a'A'}{\beta^2}\right)} + b}{a'} \ldots\ldots (6).$$

(*) Il n'y a pas d'autre supposition à faire, puisqu'on a $\alpha\delta - \beta\gamma = \pm 1$, et que d'après cela, par le n° précéd., les limites ne peuvent être nulles toutes deux en même temps, ni de signe contraire.

Il faudrait rejeter celle de ces quatre équations dans laquelle le dénominateur du premier membre serait nul; mais il faut déterminer ici les signes dont les radicaux doivent être affectés. Or il est évident que dans les équations (3) et (4), on doit prendre le signe supérieur quand $\frac{\alpha}{\gamma}$ et $\frac{\beta}{\delta}$ sont de même signe que a, car en prenant le signe inférieur $\frac{a\alpha}{\gamma}$ et $\frac{a\beta}{\delta}$ deviendraient négatifs; mais comme A et A' sont de même signe, $\sqrt{D}$ tombe entre $\sqrt{\left(D+\frac{aA}{\gamma^2}\right)}$ et $\sqrt{\left(D-\frac{aA'}{\delta^2}\right)}$, et parconséquent, dans ce cas, $\frac{\sqrt{D}-b}{a}$ entre $\frac{\alpha}{\gamma}$ et $\frac{\beta}{\delta}$.

On voit de même, dans les équations (5) et (6), qu'il faut prendre nécessairement les signes inférieurs quand $\frac{\gamma}{\alpha}$ et $\frac{\delta}{\beta}$ sont tous les deux de signes contraires à a' ou a, puisqu'en prenant le signe supérieur, les produits $\frac{a'\gamma}{\alpha}$, $\frac{a'\delta}{\beta}$ deviendraient positifs; d'où il suit sans difficulté que $\frac{-\sqrt{D}+b}{a'}$ tombe dans ce cas entre $\frac{\gamma}{\alpha}$ et $\frac{\delta}{\beta}$. Si l'on pouvait faire voir avec la même facilité, dans les équations (3) et (4), que l'on doit prendre les signes inférieurs quand $\frac{\alpha}{\gamma}$ et $\frac{\beta}{\delta}$ sont de signe contraire à a, et dans les équations (5) et (6), que l'on doit prendre les signes supérieurs quand $\frac{\gamma}{\alpha}$ et $\frac{\delta}{\beta}$ sont de même signe que a' ou a; il s'ensuivrait de la même manière, que dans le premier cas $\frac{-\sqrt{D}-b}{a}$ tombe entre $\frac{\alpha}{\gamma}$ et $\frac{\beta}{\delta}$, et que dans le second $\frac{\sqrt{D}+b}{a'}$ tombe entre $\frac{\gamma}{\alpha}$ et $\frac{\delta}{\beta}$, ce qui compléterait la démonstration du théorème. Mais quoique cela ne soit pas difficile, comme pour y parvenir on ne pourrait éviter certains embarras, nous préférons la méthode suivante.

Quand aucun des nombres α, β, δ, γ n'est $=0$, $\frac{\alpha}{\gamma}$ et $\frac{\beta}{\delta}$ ont les mêmes signes que $\frac{\gamma}{\alpha}$ et $\frac{\delta}{\beta}$, et l'on sait que si ces deux dernières

quantités sont de signes différens à a' ou a, $\frac{-\sqrt{D}+b}{a}$ tombe entre $\frac{\gamma}{\alpha}$ et $\frac{\delta}{\beta}$; mais alors les deux quantités $\frac{\alpha}{\gamma}$ et $\frac{\beta}{\delta}$ seront aussi de signes contraires à a, et $\frac{a'}{-\sqrt{D}+b}$ tombera entre $\frac{\alpha}{\gamma}$ et $\frac{\beta}{\delta}$. Or comme on a $D-b^2=aa'$, il en résulte $\frac{a'}{-\sqrt{D}+b}=\frac{-\sqrt{D}-b}{a}$, qui tombe parconséquent entre $\frac{\alpha}{\gamma}$ et $\frac{\beta}{\delta}$. Ainsi la première partie du théorème est démontrée pour le second cas, en supposant que l'on n'ait ni $\alpha=0$, ni $\beta=0$. De la même manière, quand aucun des nombres α, β, γ, δ n'est $=0$, et que $\frac{\alpha}{\gamma}$ et $\frac{\beta}{\delta}$ sont de même signe que a ou a', $\frac{\sqrt{D}-b}{a}$ tombe entre $\frac{\alpha}{\gamma}$ et $\frac{\beta}{\delta}$, et partant $\frac{a}{\sqrt{D}-b}$ entre $\frac{\gamma}{\alpha}$ et $\frac{\delta}{\beta}$; d'ailleurs $\frac{a}{\sqrt{D}-b}=\frac{\sqrt{D}+b}{a'}$, donc $\frac{\sqrt{D}+b}{a'}$ tombe entre $\frac{\gamma}{\alpha}$ et $\frac{\delta}{\beta}$, qui sont de même signe que a'. Ainsi la seconde partie du théorème est démontrée pour le premier cas, en supposant que l'on n'ait ni $\gamma=0$, ni $\delta=0$.

Il ne reste donc plus qu'à faire voir la vérité de la première partie pour le second cas, même en supposant $\alpha=0$ ou $\beta=0$, et celle de la seconde partie pour le premier cas, même en supposant $\gamma=0$ ou $\delta=0$; mais tous ces cas sont impossibles. Supposons en effet, pour la première partie du théorème, qu'on n'ait ni $\gamma=0$, ni $\delta=0$, que $\frac{\alpha}{\gamma}$ et $\frac{\beta}{\delta}$ soient tous deux de signe contraire à a, et qu'on ait *en premier lieu* $\alpha=0$. Alors l'équation $\alpha\delta-\gamma\beta=\pm 1$ donne $\beta=\pm 1$ et $\gamma=\pm 1$; donc l'équation (1) devient $A=-a'$; ainsi A et a' et partant a et A' sont de signes contraires, ce qui rend $\sqrt{\left(D-\frac{aA'}{\delta^2}\right)}>\sqrt{D}>b$; donc dans l'équation (4), il faut nécessairement prendre le signe inférieur, car en prenant le signe supérieur, il s'ensuivrait que $\frac{\beta}{\delta}$ aurait le même signe que a, et l'on a alors $\frac{\beta}{\delta}>\frac{-\sqrt{D}-b}{a}>1$ (puisque, par la définition de la forme réduite, $a<\sqrt{D}+b$). Or $\frac{\beta}{\delta}$ ne peut être plus grand que 1, puisque $\beta=\pm 1$ et que δ n'est

pas égal à zéro. *En second lieu*, soit $\beta = 0$; l'équation $\alpha\delta - \beta\gamma = \pm 1$ donne $\alpha = \pm 1$ et $\delta = \pm 1$; donc l'équation (2) devient $a' = A'$; ainsi a et A sont de même signe, ce qui rend $\sqrt{\left(D + \frac{aA}{a^2}\right)} > \sqrt{D} > b$. Donc dans l'équation (3) on doit prendre le signe inférieur, puisque en prenant le signe supérieur, il s'ensuivrait que $\frac{\alpha}{\gamma}$ et a seraient de même signe; on a donc $\frac{\alpha}{\gamma} > \frac{-\sqrt{D}-b}{a} > 1$, ce qui est absurde par la même raison que ci-dessus. Pour la seconde partie du théorème, si nous supposons qu'on n'ait ni $\alpha = 0$, ni $\beta = 0$; que $\frac{\gamma}{\alpha}$ et $\frac{\delta}{\beta}$ aient le même signe que a' et qu'on ait, *en premier lieu*, $\gamma = 0$, l'équation $\alpha\delta - \beta\gamma = \pm$ donne $\alpha = \pm 1$, $\delta = \pm 1$; donc l'équation (1) devient $A = a$, ainsi a' et A' sont de même signe, ce qui rend..... $\sqrt{\left(D + \frac{a'A'}{\beta^2}\right)} > \sqrt{D} > b$. Partant, dans l'équation (6), il faut prendre le signe supérieur, et l'on a $\frac{\delta}{\beta} > \frac{\sqrt{D}+b}{a'} > 1$, ce qui est absurde puisque $\delta = \pm 1$, et que β n'est $= 0$. Enfin, *en second lieu*, si l'on a $\delta = 0$, l'équation $\alpha\delta - \beta\gamma = \pm 1$ donne $\beta = \pm 1$, $\gamma = \pm 1$. Donc l'équation (2) devient $-A' = a$, ce qui rend $\sqrt{\left(D - \frac{a'A}{a^2}\right)} > \sqrt{D} > b$. Ainsi dans l'équation (5), il faut prendre le signe supérieur, et l'on a $\frac{\gamma}{\alpha} > \frac{\sqrt{D}+b}{a'} > 1$; ce qui est absurde.

Le théorème est donc maintenant démontré dans toute sa généralité.

Puisque la différence entre $\frac{\alpha}{\gamma}$ et $\frac{\beta}{\delta}$ est $\frac{1}{\gamma\delta}$, la différence entre $\frac{\pm\sqrt{D}-b}{a}$ et $\frac{\alpha}{\gamma}$ ou $\frac{\beta}{\delta}$ sera $< \frac{1}{\gamma\delta}$. D'ailleurs entre $\frac{\pm\sqrt{D}-b}{a}$ et $\frac{\alpha}{\gamma}$, ou entre cette quantité et $\frac{\beta}{\delta}$, il ne pourra tomber aucune fraction dont le dénominateur ne soit $> \gamma$ et $> \delta$ (*lemme précéd.*). De la même manière, la différence entre $\frac{\pm\sqrt{D}+b}{a'}$ et $\frac{\alpha}{\gamma}$ ou $\frac{\delta}{\beta}$ sera $< \frac{1}{\alpha\beta}$, et il ne pourra tomber entre cette quantité et l'une quelconque

quelconque de ces fractions, aucune fraction dont le dénominateur ne soit plus grand que α et β.

192. De l'application du théorème précédent à l'algorithme du n° 188, il suit que la quantité $\frac{\sqrt{D}-b}{a}$, que nous désignerons par L, tombe entre $\frac{\alpha'}{\gamma'}$ et $\frac{\beta'}{\delta'}$, entre $\frac{\alpha''}{\gamma''}$ et $\frac{\beta''}{\delta''}$, entre $\frac{\alpha'''}{\gamma'''}$ et $\frac{\beta'''}{\delta'''}$, etc. : ou entre $\frac{\alpha'}{\gamma'}$ et $\frac{\alpha''}{\gamma''}$, entre $\frac{\alpha''}{\gamma''}$ et $\frac{\alpha'''}{\gamma'''}$ etc.; et l'on déduit sans peine de ce qui a été dit n° 189 (3°. à la fin) qu'aucune de ces limites ne sera de signe contraire au signe de a, et que partant on doit prendre positivement le radical $\sqrt{D}$). Ainsi toutes les fractions dont les accens sont impairs différeront de L dans un sens, et toutes celles dont les accens sont pairs en différeront dans le sens contraire. Mais comme $\gamma' < \gamma'''$, $\frac{\alpha'}{\gamma'}$ tombera hors $\frac{\alpha'''}{\gamma'''}$ et L, et de même $\frac{\alpha''}{\gamma''}$ hors $\frac{\alpha^{IV}}{\gamma^{IV}}$ et L; $\frac{\alpha'''}{\gamma'''}$ hors L et $\frac{\alpha^{V}}{\gamma^{V}}$, etc.; ainsi ces quantités se trouveront évidemment placées dans l'ordre suivant :

$$\frac{\alpha'}{\gamma'},\ \frac{\alpha'''}{\gamma'''},\ \frac{\alpha^{V}}{\gamma^{V}} \ldots\ldots L \ldots\ldots \frac{\alpha^{VI}}{\gamma^{VI}},\ \frac{\alpha^{IV}}{\gamma^{IV}},\ \frac{\alpha''}{\gamma''};$$

d'ailleurs la différence entre $\frac{\alpha'}{\gamma'}$ et L sera plus petite que la différence entre $\frac{\alpha'}{\gamma'}$ et $\frac{\alpha''}{\gamma''}$, c'est-à-dire, $< \frac{1}{\gamma'\gamma''}$; de même la différence entre $\frac{\alpha''}{\gamma''}$ et L sera $< \frac{1}{\gamma''\gamma'''}$, etc. Ainsi les fractions $\frac{\alpha'}{\gamma'}$, $\frac{\alpha''}{\gamma''}$, $\frac{\alpha'''}{\gamma'''}$, etc. approcheront de plus en plus de la limite L, et comme γ', γ', γ'', etc. vont toujours en augmentant indéfiniment, la différence de ces fractions à L peut être rendue aussi petite qu'on le voudra.

Il suit du n° 189, qu'aucune des quantités $\frac{\gamma}{\alpha}$, $\frac{'\gamma}{'\alpha}$, $\frac{''\gamma}{''\alpha}$, $\frac{'''\gamma}{'''\alpha}$ n'aura le même signe que a; on déduit de là, par des raisonnemens absolument semblables aux précédens, que ces fractions et $\frac{-\sqrt{D}+b}{a'} = L'$ doivent être placées dans l'ordre suivant :

$$\frac{\gamma}{\alpha},\ \frac{''\gamma}{''\alpha},\ \frac{^{IV}\gamma}{^{IV}\alpha} \ldots\ldots L' \ldots\ldots \frac{^{V}\gamma}{^{V}\alpha},\ \frac{'''\gamma}{'''\alpha},\ \frac{'\gamma}{'\alpha}.$$

D'ailleurs la différence entre $\frac{\gamma}{\alpha}$ et L' est moindre que $\frac{1}{'\alpha\alpha}$, la dif-

férence entre $\frac{'\gamma}{'\alpha}$ et L' est moindre que $\frac{1}{''\alpha'\alpha}$, etc. Ainsi les fractions $\frac{\gamma}{\alpha}$, $\frac{'\gamma}{'\alpha}$, etc. approchent de L' de plus en plus et continuellement, et la différence peut être rendue plus petite qu'aucune quantité donnée.

Dans l'exemple du n° 188, on a $L=\frac{\sqrt{79}-8}{3}=0{,}2960648$, et les fractions convergentes sont: $\frac{0}{1}$, $\frac{1}{3}$, $\frac{2}{7}$, $\frac{3}{10}$, $\frac{5}{17}$, $\frac{8}{27}$, $\frac{45}{152}$, $\frac{143}{483}$, etc. Or cette dernière est égale à 0,2960662. De même ..... $L'=\frac{-\sqrt{79}+8}{5}=-0{,}1776388$, les fractions convergentes sont: $\frac{0}{1}$, $-\frac{1}{5}$, $-\frac{1}{6}$, $-\frac{2}{11}$, $-\frac{3}{17}$, $-\frac{8}{46}$, $-\frac{27}{152}$, $-\frac{143}{805}$, etc., dont la dernière est égale à 0,1776397.

193. Théorème. *Si les formes réduites* f *et* F *sont proprement équivalentes, chacune d'elles est contenue dans la période de l'autre.*

Soit $f=(a, b, -a')$, $F=(A, B, -A')$, D leur déterminant commun, et supposons que la première se change en la deuxième par la substitution propre k, l, p, q. Je dis qu'en cherchant la période de la forme f, et en calculant dans les deux sens la progression indéfinie des formes réduites et des transformations de f en ces différentes formes, comme au n° 188, *ou bien* k sera égal à un des termes de la suite $\ldots {}''\alpha, {}'\alpha, \alpha, \alpha', \alpha''\ldots$, et en le supposant $=\alpha^m$, on aura $k=\beta^m$, $p=\gamma^m$, $q=\delta^m$; *ou bien* $-k$ sera égal à un certain terme α^m, et $-l$, $-p$, $-q$ à β^m, γ^m, δ^m, respectivement. Dans l'un ou l'autre cas, F sera évidemment identique avec f^m.

I. On a quatre équations:

$$(1)\ldots ak^2+2bkp-a'p^2=A, \quad (2)\ldots akl+b(kq+kp)+a'pq=B,$$
$$(3)\ldots al^2+2blq-a'q^2=-A', \quad (4)\ldots kq-kl=1;$$

considérons d'abord le cas où quelqu'un des nombres k, l, p, q est $=0$.

1°. Si $k=0$, l'équation (4) donne $lp=-1$, et partant $l=\pm 1$, $p=\mp 1$. Donc l'équation (1) devient $-a'=A$; l'équation (2) $-b\pm a'q=B$ ou $B\equiv -b \pmod{a' \text{ ou } A}$. D'où il suit que la

forme $(A, B, -A')$ est contiguë à la forme $(a, b, -a')$ par la dernière partie; mais puisque F est une forme réduite, elle sera nécessairement identique avec f' (n° 184, 6°.). Donc $B=b'$, et partant l'équation (2) donne $b+b'=\pm a'q$; et comme d'ailleurs on a $\frac{b+b'}{-a'}=h'$, on en tire $q=\mp h'$. Il suit de là qu'on a $\mp k, \mp l, \mp p, \mp q=0, -1, +1, h'$, ou $=\alpha', \beta', \gamma', \delta^{\nu}$, respectivement.

2°. Si $l=0$, l'équation (4) donne $k=\pm 1$, $q=\pm 1$; l'équation (3) $a'=A'$; l'équation (2) $b\mp a'p=B$, ou $B\equiv b \pmod{a'}$; mais comme f et F sont des formes réduites, B et b tomberont entre $\sqrt{D}$ et $\sqrt{D}\mp a'$, suivant que a' sera positif ou négatif (n° 184, 5°.); ainsi on aura nécessairement $B=b$ et $p=0$, donc les formes f et F sont identiques, et $\pm k, \pm l, \pm p, \pm q=1, 0, 0, 1=\alpha, \beta, \gamma, \delta$, respectivement.

3°. Si $p=0$, l'équation (4) donne $k=\pm 1$, $q=\pm 1$; l'équation (1) $a=A$; l'équation (2) $\pm al+b=B$. Mais comme B et b tombent entre $\sqrt{D}$ et $\sqrt{D}\mp a$, on aura nécessairement $B=b$ $l=0$. Ainsi ce cas ne diffère pas du précédent.

4°. Si $q=0$, l'équation (4) donne $l=\pm 1$, $p=\mp 1$; l'équation (3) $a=-A'$, et l'équation (2) $\pm al-b=B$, ou $B\equiv -b \pmod{a}$. Ainsi la forme F est contiguë à la forme f par la première partie, et partant elle sera identique avec la forme $'f$: et comme on a $\frac{b+'b}{a}=h$ et $B='b$, on aura $l=h$. Il suit de là que $\pm k, \pm l, \pm p, \pm q=h, 1, -1, 0='\alpha, '\beta, '\gamma, '\delta$ respectivement.

Il reste donc le cas où aucun des nombres k, l, p, q n'est $=0$. Or par le lemme du n° 190, les quantités $\frac{k}{p}, \frac{l}{q}, \frac{p}{k}, \frac{q}{l}$ auront le même signe, et il en résulte deux cas: celui où leur signe est le même que celui de a et a', et celui où il est contraire.

II. Si $\frac{k}{l}$ et $\frac{l}{q}$ ont le même signe que a, la quantité $\frac{\sqrt{D}-b}{a}=L$ tombera entre ces fractions (n° 191). Nous allons démontrer que $\frac{k}{p}$ est égal à quelqu'une des fractions $\frac{\alpha''}{\gamma''}, \frac{\alpha'''}{\gamma'''}, \frac{\alpha^{IV}}{\gamma^{IV}}$, etc., et $\frac{l}{q}$ à

celle qui la suit immédiatement, c'est-à-dire, que si $\frac{k}{p}=\frac{\alpha^{(m)}}{\gamma^{(m)}}$, on aura $\frac{l}{q}=\frac{\alpha^{m+1}}{\gamma^{m+1}}$. Nous avons fait voir dans le n° précédent que les quantités $\frac{\alpha'}{\gamma'}$, $\frac{\alpha''}{\gamma''}$, $\frac{\alpha'''}{\gamma'''}$, etc. (que nous désignerons par φ', φ'', φ''', etc.) et L sont placées dans l'ordre suivant:

$$\varphi', \varphi''', \varphi^{v}....L....\varphi^{vi}, \varphi^{iv}, \varphi''.....(I).$$

La première de ces quantités est $=0$ (puisque $\alpha'=0$); toutes les autres ont le même signe que L ou a; mais comme par hypothèse $\frac{k}{p}$ et $\frac{l}{q}$ ont le même signe, ils tomberont, par rapport à φ', du même côté que L, et comme d'ailleurs L tombe entre ces deux mêmes quantités, elles seront l'une à droite, l'autre à gauche de L. Mais on peut faire voir aisément que $\frac{k}{p}$ ne peut tomber après φ'', autrement $\frac{l}{q}$ tomberait entre φ' et L; d'où il suivrait, 1°. que φ'' tomberait entre $\frac{k}{p}$ et $\frac{l}{q}$, et que partant le dénominateur de la fraction φ'' serait plus grand que q (n° 190); 2°. que $\frac{l}{q}$ tombe entre φ' et φ'', et que partant q est plus grand que le dénominateur de φ'', ce qui implique contradiction.

Supposons que $\frac{k}{p}$ ne soit égal à aucune des fractions φ'', φ''', φ^{iv}, etc., et voyons ce qu'il en résulterait. Alors il est évident que si $\frac{k}{p}$ est situé à gauche de L, il tombera entre φ' et φ''', ou entre φ''' et φ^{v}, ou entre φ^{v} et φ^{vii}, etc., puisque L est irrationnel et parconséquent différent de $\frac{k}{p}$, et que les fractions φ', φ''', etc. peuvent approcher de L de plus près qu'aucune quantité donnée qui ne serait pas L lui-même. De même, si $\frac{k}{p}$ est à droite de L, il tombera entre deux fractions consécutives de la suite $....\varphi^{vi}$, φ^{iv}, φ''. Supposons donc que $\frac{k}{p}$ tombe entre $\varphi^{(m)}$ et $\varphi^{(m+a)}$, les fractions $\frac{k}{p}$, $\varphi^{(m)}$, $\varphi^{(m+1)}$, $\varphi^{(m+a)}$ se trouveront dans l'ordre suivant:

$$\varphi^{(m)}, \frac{k}{p}, \varphi^{(m+2)}.....L.....\varphi^{(m+1)}.....(\text{II})\ (*);$$

alors $\frac{l}{q}$ sera nécessairement $=\varphi^{(m+1)}$; car il doit être à droite de L, et s'il était aussi à droite de $\varphi^{(m+1)}$, $\varphi^{(m+1)}$ tomberait entre $\frac{k}{p}$ et $\frac{l}{q}$ et l'on aurait $\gamma^{(m+1)} > p$; mais comme $\frac{k}{p}$ tomberait entre $\varphi^{(m)}$ et $\varphi^{(m+1)}$, il s'ensuivrait qu'on aurait en même temps $p > \gamma^{(m+1)}$, ce qui implique contradiction. Si $\frac{l}{q}$ était à gauche de $\varphi^{(m+1)}$, il tomberait entre $\varphi^{(m+2)}$ et $\varphi^{(m+1)}$, et alors on aurait $q > \gamma^{(m+2)}$; mais comme $\varphi^{(m+2)}$ tombe lui-même entre $\frac{k}{p}$ et $\frac{l}{q}$, on aurait en même temps $\gamma^{(m+2)} > q$, ce qui implique contradiction. On aura donc $\frac{l}{q} = \varphi^{(m+1)} = \frac{\alpha^{(m+1)}}{\gamma^{(m+1)}} = \frac{\beta^{(m)}}{\delta^{(m)}}$.

Puisque $kq - lp = 1$, l et q seront premiers entre eux, et par la même raison $\beta^{(m)}$ et $\delta^{(m)}$ le sont aussi; d'où l'on voit facilement que l'équation $\frac{l}{q} = \frac{\beta^{(m)}}{\delta^{(m)}}$ ne peut avoir lieu à moins qu'on n'ait $l = \beta^{(m)}$ et $q = \delta^{(m)}$, ou $l = -\beta^{(m)}$ et $q = -\delta^{(m)}$. Or comme la forme f se change par la transformation propre $\alpha^{(m)}$, $\beta^{(m)}$, $\gamma^{(m)}$, $\delta^{(m)}$, en la forme $f^{(m)} = (\pm a^{(m)}, b^{(m)}, \mp a^{(m+1)})$ on aura les équations

$$a\alpha^{(m)}\alpha^{(m)} + 2b\alpha^{(m)}\gamma^{(m)} - a'\gamma^{(m)}\gamma^{(m)} = \pm a^{(m)} \quad .....(5)$$
$$a\alpha^{(m)}\beta^{(m)} + b(\alpha^{(m)}\delta^{(m)} + \beta^{(m)}\gamma^{(m)}) - a'\gamma^{(m)}\delta^{(m)} = b^{(m)} \quad ...(6)$$
$$a\beta^{(m)}\beta^{(m)} + 2b\beta^{(m)}\delta^{(m)} - a'\delta^{(m)}\delta^{(m)} = \mp a^{(m+1)} \quad .....(7)$$
$$\alpha^{(m)}\delta^{(m)} - \beta^{(m)}\gamma^{(m)} = 1 \quad .....(8).$$

Mais en substituant $\beta^{(m)}$ et $\delta^{(m)}$ pour l et q dans l'équation (3), son premier membre devient égal à celui de l'équation (1); on a donc $\pm a^{(m+1)} = -A'$. Or (**) en multipliant l'équation (2)

(*) Peu importe que l'ordre de la suite (II) soit le même que celui de la suite (I), ou qu'il lui soit opposé, c'est-à-dire, que φ^m soit dans la première à gauche ou à droite.

(**) Il me semble que le calcul serait plus simple de la manière suivante :
En remplaçant dans l'équation (8), β^m et δ^m par $\pm l$ et $\pm q$, elle devient

par $\alpha^{(m)}\delta^{(m)} - \beta^{(m)}\gamma^{(m)}$, et l'équation (6) par $kq - lp$, et retranchant, on voit facilement par le développement qu'on a

$$B - b^{(m)} = (p\alpha^{(m)} - k\gamma^{(m)})(al\beta^{(m)} + b(q\beta^{(m)} + l\delta^{(m)}) - a'q\delta^{(m)}) + (l\delta^{(m)} - q\beta^{(m)})(ak\alpha^{(m)} + b(p\alpha^{(m)} + k\gamma^{(m)}) - a'p\gamma^{(m)}) \ldots\ldots (9),$$

ou comme $l = \pm\beta^{(m)}$ et $q = \pm\delta^{(m)}$,

$$B - b^{(m)} = \pm(p\alpha^{(m)} - k\gamma^{(m)})(al^2 + 2blq - a'q^2) = \pm(p\alpha^{(m)} - k\gamma^{(m)})A', \text{ ou } B \equiv b^{(m)} \pmod{A'};$$

mais B et $b^{(m)}$ tombent entre $\sqrt{D}$ et $\sqrt{D} \pm A'$; on aura donc nécessairement $B = b^{(m)}$, partant $p\alpha^{(m)} - k\gamma^{(m)} = 0$, ou..... $\frac{k}{p} = \frac{\alpha^{(m)}}{\gamma^{(m)}} = \varphi^{(m)}$.

Ainsi, de la supposition que $\frac{k}{p}$ n'est égal à aucune des quantités φ'', φ''', etc., on fait voir qu'il est égal à l'une d'elles. Si nous avions supposé d'abord $\frac{k}{p} = \varphi^{(m)}$, on aurait eu évidemment $k = \pm\alpha^{(m)}$, $p = \pm\gamma^{(m)}$; dans les deux cas, la comparaison des équations (1) et (5) donne $A = \pm a^{(m)}$, et de l'équation (9), $B - b^{(m)} = \pm(l\delta^{(m)} - q\beta^{(m)})$, ou $B \equiv b^{(m)} \pmod{A}$; on conclut de là, comme plus haut, que $B = b^{(m)}$, partant $\frac{l}{q} = \frac{\beta^{(m)}}{\delta^{(m)}}$, et comme l et q, $\beta^{(m)}$ et $\delta^{(m)}$ sont premiers entre eux, $l = \pm\beta^{(m)}$, $q = \pm\delta^{(m)}$. L'équation (7) donne alors, en la comparant à l'équation (3), $-A' = \mp a^{(m+1)}$, ainsi les formes F et $f^{(m)}$ sont identiques. A l'aide de l'équation $kq - lp = \alpha^{(m)}\delta^{(m)} - \beta^{(m)}\gamma^{(m)}$, on prouve sans difficulté que si l'on prend k et p avec le signe $+$ ou avec le signe $-$, il faut prendre l et q de même.

$l\alpha^m - q\gamma^m \doteq 1$; si l'on en retranche l'équation (4), on a

$$l(\alpha^m \mp k) - q(\gamma^m \mp p) = 0, \text{ d'où } \frac{\alpha^m \mp k}{\gamma^m \mp p} = \frac{l}{q};$$

et comme l et q sont premiers entre eux, on a généralement $\alpha^m \mp k = rl$, $\gamma^m \mp p = rq$, ou $\alpha^m = \pm k + rl$, $\gamma^m = \pm p + rq$.

Substituant dans l'équation (6) les valeurs de α^m, β^m, γ^m, δ^m, il vient

$$\mp\gamma A' = B - b^m.$$

Or on démontre que $B = b^m$; donc $r = 0$, et $\alpha^m = \pm k$ et $\gamma^m = \pm p$.
De même, pour le paragraphe suivant. (*Note du Traducteur*).

III. Si le signe des quantités $\frac{k}{p}$, etc. est opposé à celui de a, la démonstration est tellement semblable à la précédente, qu'il suffit d'ajouter seulement les points principaux.

$\frac{-\sqrt{D}+b}{a'}$ tombera entre $\frac{p}{k}$ et $\frac{q}{l}$; $\frac{q}{l}$ sera égal à une des fractions $\frac{'\delta}{'\beta}$, $\frac{''\delta}{''\beta}$, $\frac{'''\delta}{'''\beta}$, etc., et en supposant donc $\frac{q}{l}=\frac{^{(m)}\delta}{^{(m)}\beta}$, on aura $\frac{p}{k}=\frac{^{(m)}\gamma}{^{(m)}\alpha}$. La première de ces deux assertions se prouve comme il suit: si $\frac{q}{l}$ n'est pas égal à une de ces fractions, elle devra tomber entre deux $\frac{^{(m)}\delta}{^{(m)}\beta}$ et $\frac{^{(m+1)}\delta}{^{(m+1)}\beta}$. Or on démontre, comme plus haut, qu'alors $\frac{p}{k}$ sera nécessairement $=\frac{^{(m+1)}\delta}{^{(m+1)}\beta}=\frac{^{(m)}\gamma}{^{(m)}\alpha}$, et partant $p=\pm{}^{(m)}\gamma$ et $k=\pm{}^{(m)}\alpha$. Mais f, par la substitution propre ${}^{(m)}\alpha$, ${}^{(m)}\beta$, ${}^{(m)}\gamma$, ${}^{(m)}\delta$, se change en ${}^{(m)}f=(\pm{}^{(m)}a, {}^{(m)}b, \pm{}^{(m+1)}a)$, d'où naissent trois équations qui, jointes à l'équation ${}^{(m)}\alpha{}^{(m)}\delta-{}^{(m)}\beta{}^{(m)}\gamma=1$, et aux équations (1), (2), (3) et (4), prouvent d'abord que le terme A de la forme F est égal au premier terme de la forme ${}^{(m)}f$, ensuite que le terme moyen de la première est congru à celui de la seconde, suivant le module A, et que comme les deux formes sont réduites, chacun d'eux tombe entre $\sqrt{D}$ et $\sqrt{D}\mp A$, ces deux termes moyens sont égaux; et de là on conclut que $\frac{q}{l}=\frac{^{(m)}\delta}{^{(m)}\beta}$. Ainsi la vérité de cette première assertion est dérivée de la supposition même qu'elle fût fausse.

Or en supposant $\frac{q}{l}=\frac{^{(m)}\delta}{^{(m)}\beta}$, on démontre absolument de la même manière et par les mêmes équations, que $\frac{p}{k}=\frac{^{m}\gamma}{^{m}\alpha}$, et au moyen de l'équation $kq-lp={}^{(m)}\alpha{}^{(m)}\delta-{}^{(m)}\beta{}^{(m)}\gamma$, on prouve que si l'on prend pour q et l, ${}^{(m)}\delta$ et ${}^{(m)}\beta$ avec le signe + ou le signe —, il faudra pour p et k prendre ${}^{(m)}\gamma$ et ${}^{(m)}\alpha$ avec le même signe, et partant que les formes F et ${}^{(m)}f$ sont identiques.

194. Comme les formes que nous avons appelées associées (n° 187, 6°.), sont toujours improprement équivalentes (n° 159, à la fin), il est clair que si les formes réduites F et f sont improprement équivalentes, et que la forme G soit associée à F,

les formes f et G seront proprement équivalentes, et partant, la forme 6 sera contenue dans la période de la forme f; si donc les formes F et f sont équivalentes tant proprement qu'improprement, on devra trouver F et G dans la période de f. Cette période sera donc elle-même son associée (n° 187, 7°.); ce qui sert de confirmation au théorème du n° 165, par lequel nous nous étions convaincus qu'on pouvait trouver une forme ambiguë équivalente à deux autres F et f.

195. PROBLÈME. *Étant données deux formes* Φ *et* φ *dont le déterminant est le même, distinguer si elles sont équivalentes, ou si elles ne le sont pas.*

On cherchera deux formes réduites F et f, respectivement et proprement équivalentes aux formes Φ et φ (n° 183). Selon que ces formes réduites seront seulement proprement ou improprement équivalentes, ou qu'elles le seront des deux manières, ou qu'elles ne le seront point, les proposées le seront proprement, improprement, ou de deux manières, ou ne le seront d'aucune manière. On cherchera la période de l'une de ces deux formes réduites, par exemple de f; et si la forme F s'y trouve sans que son associée y soit, le premier cas aura lieu; si cette dernière seule s'y trouve, le second cas aura lieu; si toutes deux y sont, ce sera le troisième cas; et le quatrième, quand il n'y aura ni l'une ni l'autre.

Exemple. Soient les formes (129, 92, 65), (42, 59, 81) dont le déterminant est 79; on trouve pour réduites équivalentes (10, 7, —3), (5, 8, —3). La période de la première est

(10,7,—3),(—3,8,5),(5,7,—6),(—6,5,9),(9,4,—7),(—7,3,10),

et comme la forme (5, 8, —3) n'y est pas comprise, mais seulement son associée (—3, 8, 5), les formes proposées sont improprement équivalentes.

Si l'on distribue, comme ci-dessus (n° 187, 5°.), toutes les formes réduites d'un déterminant donné en périodes P, Q, R, etc., et qu'on prenne dans chacune d'elles une forme quelconque, F dans P, G dans Q, H dans R, etc., il ne pourra y avoir parmi ces formes deux qui soient proprement équivalentes; mais toute autre forme de même déterminant sera proprement équivalente à

une

une d'elles et à une seule. Il suit évidemment de là, *que toutes les formes de même déterminant peuvent se distribuer en autant de classes qu'il y a de périodes*, en renfermant dans la première toutes celles qui sont proprement équivalentes à F, dans la seconde, toutes celles qui sont proprement équivalentes à G, etc. Ainsi toutes les formes renfermées dans la même classe, seraient proprement équivalentes, mais deux formes prises dans des classes différentes ne le seront pas. Au reste nous n'insisterons pas davantage ici sur ce sujet, que nous expliquerons plus bas avec détail.

196. PROBLÈME. *Étant données deux formes* Φ *et* φ *proprement équivalentes, trouver une transformation propre qui change l'une en l'autre.*

Par la méthode du n° 183, on peut trouver deux suites de $\Phi, \Phi', \Phi''\ldots\Phi^{(n)}, \varphi, \varphi', \varphi''\ldots\varphi^{(\nu)}$, telles que chacune des formes soit equivalente à celle qui la précède, et que les dernières $\Phi^{(n)}$ et $\varphi^{(\nu)}$ soient des formes réduites; et comme Φ et φ sont supposées équivalentes, $\Phi^{(n)}$ doit se trouver dans la période de $\varphi^{(\nu)}$. Soit $\varphi^{(\nu)} = f$, et sa période prolongée jusqu'à la forme $\Phi^{(n)}$: $f, f', f''\ldots f^{(m-1)}, f^{(m)}$, desorte que $\Phi^{(n)} = f^{(m)}$; et désignons par $\Psi, \Psi', \Psi''\ldots\Psi^{(n)}$ les formes opposées (n° 159) aux associées des formes $\Phi, \Phi', \Phi''\ldots\Phi^{(n)}$, respectivement; alors dans la suite $\varphi, \varphi', \varphi''\ldots f, f', f'', f^{(m-1)}, \Psi^{(n-1)}, \Psi^{(n-2)}\ldots\Psi$, chaque forme est contiguë par la dernière partie à celle qui la précède; d'où, par le n° 177, on pourra trouver une transformation de la première φ en la dernière Φ. Cette liaison entre les formes est évidente depuis φ jusqu'à $f^{(m-1)}$, et depuis $\Psi^{(n-2)}$ jusqu'à Φ. Quant aux formes $f^{(m-1)}$ et $\Psi^{(n-1)}$, on la prouvera comme il suit : soit $f^{(m-1)} = (g, h, i)$; $f^{(m)} = \Phi^{(n)} = (g', h', i')$, $\Phi^{(n-1)} = (g'', h'', i'')$. La forme (g', h', i') sera contiguë par la dernière partie à chacune des formes (g, h, i), (g'', h'', i''); ainsi $i = g' = i''$, et $-h \equiv h' - h''$ (mod.) $i = g' = i''$; donc la forme $(i'', -h'', g'') = \Psi^{(n-1)}$ est contiguë par la dernière partie à la forme $(g, h, i) = f^{(m-1)}$.

Si les formes Φ et φ sont improprement équivalentes, la forme φ sera proprement équivalente à la forme dont Φ est l'opposée; ainsi on pourra trouver une transformation de φ en cette forme; et si elle se fait par la substitution $\alpha, \beta, \gamma, \delta$, on voit facilement

que φ se change improprement en Φ par la substitution $\alpha, -\beta, \gamma, -\delta$.

Il suit de là que si Φ et φ sont équivalentes proprement et improprement, on peut trouver deux transformations, l'une propre et l'autre impropre.

Exemple. Soit la forme (129, 92, 65) à transformer en la forme (42, 59, 81) que nous avons trouvé lui être improprement équivalente (n° précéd.); il faudra commencer par trouver la transformation propre de la forme (129, 92, 65) en la forme (44, −59, 81). Pour y parvenir, on établira la suite de formes

(129, 92, 65), (65, −27, 10), (10, 7, −3), (−3, 8, 5),
(5, 22, 81), (81, 59, 42), (42, −59, 81);

de là on déduit la transformation propre −47, 56, 73, −87, qui change (129, 92, 65) en (42, −59, 81); donc la transformation impropre −47, −56, 73, 87 la changera en (42, 59, 81).

197. Si l'on connaît une transformation d'une forme $\varphi = (a, b, c)$ en une autre Φ qui lui est équivalente, on pourra déduire de celle-là toutes les transformations semblables, pourvu qu'on connaisse toutes les solutions de l'équation indéterminée $t^2 - Du^2 = m^2$, dans laquelle D est le déterminant des formes Φ et φ, et m le plus grand diviseur commun des nombres a, $2b$, c (n° 162). Nous allons attaquer, en supposant D positif, ce problème que nous avons déjà résolu pour le cas de D négatif. Mais comme il est évident que toute valeur qui satisfera à l'équation, y satisfera aussi avec un signe contraire, il suffira d'assigner les valeurs positives de t et de u, et chaque solution en nombres positifs fournira quatre solutions effectives. Pour y parvenir, nous chercherons d'abord les plus petites valeurs de t et u (excepté $t = m$, $u = 0$ qui se présentent d'elles-mêmes); et celles-ci une fois connues, nous indiquerons le moyen d'en déduire les autres.

198. PROBLÈME. *Trouver les plus petits nombres qui satisfont à l'équation indéterminée* $t^2 - Du^2 = m^2$, *pourvu qu'il existe une forme* (M, N, P), *dont le déterminant soit* D, *et que* m *soit le plus grand diviseur commun des nombres* M, 2N, P.

On prendra à volonté une forme réduite $f = (a, b, a')$ dont le

déterminant soit D, et telle que m soit le plus grand diviseur commun des nombres a, $2b$, a', ce qui ne peut manquer d'arriver, puisque l'on peut trouver une forme réduite équivalente à la forme (M, N, P), et qu'alors (n° 161) elle jouira de cette propriété. Mais pour la proposition actuelle, on pourra employer une forme réduite quelconque, pourvu qu'elle satisfasse à cette condition. On formera la période de f, où nous supposerons qu'il y ait n formes; en reprenant tous les signes dont nous nous sommes servis au n° 188, on aura $f^{(n)} = (a^{(n)}, b^{(n)}, -a^{(n+1)})$, parceque n est pair, et f deviendra $f^{(n)}$ par la substitution propre $\alpha^{(n)}$, $\beta^{(n)}$, $\gamma^{(n)}$, $\delta^{(n)}$; mais comme f et $f^{(n)}$ sont identiques, f deviendra aussi $f^{(n)}$ par la substitution propre 1, 0, 0, 1. De ces deux transformations semblables de f en $f^{(n)}$, on peut déduire, au moyen du n° 162, une solution en nombres entiers de l'équation $t^2 - Du^2 = m^2$; savoir, $t = \frac{1}{2}(\alpha^{(n)} + \delta^{(n)})m$ (équation (18), n° 162), $u = \frac{\gamma^{(n)} m}{a}$ (équation (19)) (*). Désignons par T et U ces valeurs prises positivement, si elles ne se présentent pas telles, et T, U seront les plus petites valeurs de t, u (excepté $l = m$ et $u = 0$, auxquelles elles ne pourront jamais revenir, parcequ'on ne peut pas avoir $\gamma^{(n)} = 0$.

Supposons en effet qu'il existe des valeurs τ et υ plus petites que T et U et parmi lesquelles on n'ait pas $U = 0$. Alors, par le n° 162, la forme f se transforme en elle-même par la substitution propre

$$\frac{1}{m}(\tau - b\upsilon),\ \frac{1}{m}a'\upsilon,\ \frac{1}{m}a\upsilon,\ \frac{1}{m}(\tau + b\upsilon).$$

Or (n° 193, II) $\pm\frac{1}{m}(\tau - b\upsilon)$ doit être égal à l'un des nombres α'', α''', α^{IV}, etc., $= \alpha^{(\mu)}$, par exemple. En effet, comme.... $\tau^2 = D\upsilon^2 + m^2 = b^2\upsilon^2 + aa'\upsilon^2 + m^2$, on aura $\tau^2 > b^2\upsilon^2$, et partant $\tau - b\upsilon$ positif; donc la fraction $\frac{\tau - b\upsilon}{a\upsilon}$, qui répond à la frac-

(*) Les quantités qui étaient, au n° 162, α, β, γ, δ; α', β', γ', δ'; A, B, C; A', B', C'; e; sont ici 1, 0, 0, 1; α^n, β^n, γ^n, δ^n; a, b, $-a'$; a, b, $-a'$; 1.

tion $\frac{k}{p}$ (n° 193), aura le même signe que a ou a'; ainsi l'on aura

$$\frac{1}{m}a'v,\ \frac{1}{m}av,\ \frac{1}{m}(t+bv) = \beta^{(\mu)},\ \gamma^{(\mu)},\ \delta^{(\mu)} \text{ respectivement;}$$

mais comme on a $v < U$, c'est-à-dire, $v < \frac{\gamma^{(n)}m}{a}$, et > 0, on aura $\gamma^{(\mu)} < \gamma^{(n)}$ et > 0; d'où il suit que les quantités $\gamma, \gamma', \gamma''$, etc. allant toujours en croissant, μ tombera entre 0 et n exclusivement; mais la forme $f^{(\mu)}$, qui correspond à l'accent μ est identique avec la forme f, ce qui est absurde, puisque toutes les formes f, f', f'', etc. jusqu'à $f^{(n-1)}$ sont supposées différentes. Donc T et U sont les plus petites valeurs de t et u, excepté m et 0.

Exemple. Si $D = 79$ et $m = 1$, on pourra employer la forme réduite $(3, 8, -5)$, pour laquelle $n = 6$ et $\alpha^{(n)} = -8$, $\gamma^{(n)} = -27$, $\delta^{(n)} = -152$ (n° 188); d'où résultent $T = 80$ et $U = 9$, qui sont les plus petites valeurs de t et u qui satisfassent à l'équation $t^2 - 79u^2 = 1$.

199. On peut trouver des formules encore plus commodes pour la pratique. En effet, on aura $2b\gamma^{(n)} = -a(\alpha^{(n)} - \delta^{(n)})$, en multipliant (n° 162) l'équation (19) par $2b$, l'équation (20) par a, et changeant les caractères comme nous l'avons fait, on tire de là $\alpha^{(n)} + \delta^{(n)} = 2\delta^{(n)} - \frac{2b}{a}\gamma^{(n)}$, et partant

$$\pm T = m\left(\delta^{(n)} - \frac{b}{a}\gamma^{(n)}\right), \quad \pm U = \frac{\gamma^{(n)}m}{a}.$$

On tirera de même des équations (20) et (21)

$$\pm T = m\left(\alpha^{(n)} + \frac{b}{a'}\beta^{(n)}\right), \quad \pm U = \frac{\beta^{(n)}m}{a'}.$$

Ces formules deviennent très-commodes, parcequ'on a $\gamma^{(n)} = \delta^{(n-1)}$, $\alpha^{(n)} = \beta^{(n-1)}$, et qu'en se servant de la première, il suffira de calculer la suite $\delta^{v}, \delta^{vi}, \delta^{vii}$, etc., et qu'en se servant de la seconde, il suffira de calculer la suite $\beta', \beta'', \beta'''$, etc. En outre, on déduit facilement du n° 189, 3°., que n étant pair, $\alpha^{(n)}$ et $\frac{b}{a'}\beta^{(n)}$ au-

ront le même signe, ainsi que $\delta^{(n)}$ et $\frac{b}{a}\gamma^{(n)}$, desorte que dans la première formule, on doit prendre pour T une différence absolue et une somme dans la seconde, sans qu'il soit besoin de faire attention au signe.

Exemple. Pour $D=61$ et $m=2$, on peut employer la forme $(2, 7, -6)$; on trouve $n=6$, $h'=-2$, $h''=2$, $h'''=-7$, $h^{IV}=2$, $h^{V}=-2$, $h^{VI}=7$. De là $\delta^{VI}=1444$ et $\gamma^{VI}=\delta^{V}=195$ (abstraction faite du signe); d'où $T=2(1444-\frac{7}{2}.195)=1523$ et $U=195$. On trouve la même chose par l'autre formule.

Au reste, il y a plusieurs autres artifices par lesquels on peut simplifier le calcul; mais le desir d'abréger ne nous permet pas d'en parler avec plus d'étendue.

200. Pour tirer toutes les valeurs de t et de u de la connaissance des plus petites, nous mettrons l'équation $T^2-DU^2=m^2$ sous la forme $\left(\frac{T}{m}+\frac{U}{m}\sqrt{D}\right).\left(\frac{T}{m}-\frac{U}{m}\sqrt{D}\right)=1$; d'où l'on tire

$$\left(\frac{T}{m}+\frac{U}{m}\sqrt{D}\right)^{e}.\left(\frac{T}{m}-\frac{U}{m}\sqrt{D}\right)^{e}=1.....(1),$$

e étant un nombre quelconque. Faisons pour abréger,

$$\frac{m}{2}\left(\frac{T}{m}+\frac{U}{m}\sqrt{D}\right)^{e}+\frac{m}{2}\left(\frac{T}{m}-\frac{U}{m}\sqrt{D}\right)^{e}=t^{(e)}.....$$

$$\frac{m}{2\sqrt{D}}\left(\frac{T}{m}+\frac{U}{m}\sqrt{D}\right)^{e}-\frac{m}{2\sqrt{D}}\left(\frac{T}{m}-\frac{U}{m}\sqrt{D}\right)^{e}=u^{(e)},$$

ensorte que ces expressions soient représentées par t^{o} et u^{o} quand $e=0$ (elles sont alors m, 0); par t', u' quand $e=1$ (elles sont alors T et U); par t'' et u'' quand $e=2$; par t''' et u''' quand $e=3$, etc. Nous allons démontrer qu'en prenant pour e tous les nombres entiers positifs depuis 0 jusqu'à $\frac{1}{0}$: 1°. toutes les valeurs de ces expressions satisferont à l'équation proposée; 2°. toutes ces valeurs sont entières; 3°. il n'y a pas de valeurs de t et u qui ne soient contenues dans ces formules.

I. En substituant pour $t^{(e)}$ et $u^{(e)}$ leurs valeurs, on prouve sans peine qu'on a $(t^{(e)}+u^{(e)}\sqrt{D})(t^{(e)}-u^{(e)}\sqrt{D})=m^2$, c'est-à-dire, $t^{(e)}.t^{(e)}-Du^{(e)}.u^{(e)}=m^2$.

II. On démontre facilement de la même manière qu'on a gé-

néralement $t^{(\epsilon+1)}+t^{(\epsilon-1)}=\frac{2T}{m}t^{(\epsilon)}$, et $u^{(\epsilon+1)}+u^{(\epsilon-1)}=\frac{2T}{m}u^{(\epsilon)}$. Il suit de là que les deux progressions : t^0, t', t'', t''', etc.; u^0, u', u'', u''', etc. sont récurrentes, et que l'échelle de relation est pour chacune d'elles $\frac{2T}{m}$, -1, savoir, $t''=\frac{2T}{m}t'-t$; $t'''=\frac{2T}{m}t''-t'$, etc. $u''=\frac{2T}{m}u'-u$, etc.

Or, par hypothèse, il existe une forme (M, N, P) dont le déterminant est D et dans laquelle M, $2N$, P sont divisibles par m, et l'équation $t^2=Du^2+m^2$ donne $T^2=(N^2-MP)U^2+m^2$, ainsi $4T^2$ sera divisible par m^2; donc $\frac{2T}{m}$ est un nombre entier et positif. Comme d'ailleurs $t^0=m$, $t'=T$, $u^0=0$, $u'=U$, les termes des deux séries sont entiers; il est clair aussi que T^2 étant $>m^2$, ces mêmes termes sont tous positifs, et vont en augmentant à l'infini.

III. Supposons qu'il y ait d'autres valeurs positives de t, u qui ne soient pas contenues dans les progressions t^0, t', t'', etc. u^0, u', u'', etc.; T' et U', par exemple. Puisque la série u^0, u', etc. croît à l'infini, U' sera nécessairement compris entre deux termes consécutifs u^n et u^{n+1}, ensorte qu'on ait $U'>u^n$ et $U'<u^{n+1}$. Pour démontrer l'absurdité de cette supposition, observons que:

1°. L'équation $t^2-Du^2=m^2$ sera satisfaite en posant $t=\frac{1}{m}(T't^{(n)}-DU'u^{(n)})$, $u=\frac{1}{m}(U't^{(n)}-T'u^{(n)})$, ce qui peut se confirmer sans peine par la substitution. Représentons ces valeurs par τ et υ, nous prouverons, comme il suit, que ce sont des nombres entiers. Si (M, N, P) est une forme dont le déterminant est D, et que m soit le diviseur commun des nombres M, $2N$, P, $T'+NU'$ et $t^{(n)}+Nu^{(n)}$ sont divisibles par m, et partant $U'(t^{(n)}+Nu^{(n)})-u^{(n)}(T'-NU')=U't^{(n)}-u^{(n)}T'$ l'est aussi; donc υ sera entier et τ par suite, puisque $\tau^2=D\upsilon^2+m^2$.

2°. Il est clair que υ ne peut être $=0$; en effet, il s'ensuivrait $U'^2t^{(n)}.t^{(n)}=T'^2.u^{(n)}u^{(n)}$, ou

$$U'^2(Du^{(n)}u^{(n)}+m^2)=u^{(n)}u^{(n)}(DU'^2+m^2);$$

d'où l'on tire $U'^2=u^{(n)}.u^{(n)}$, contre l'hypothèse par laquelle

$U' > u^{(n)}$. Mais comme U est la plus petite valeur de u, après zéro, v ne sera certainement pas $< U$.

3°. Des valeurs de $t^{(n)}$, $t^{(n+1)}$, $u^{(n)}$, $u^{(n+1)}$, on tire aisément $mU = u^{(n+1)}t^{(n)} - t^{(n+1)}u^{(n)}$; donc $U't^{(n)} - T'u^{(n)}$ ne sera pas plus petit que $u^{n+1}t^n - t^{n+1}u^n$.

4°. L'équation $T'^2 - DU'^2 = m^2$ donne $\frac{T'}{U'} = \sqrt{\left(D + \frac{m^2}{U'^2}\right)}$, et l'on a de même $\frac{t^{(n+1)}}{u^{(n+1)}} = \sqrt{\left(D + \frac{m^2}{u^{(n+1)}u^{(n+1)}}\right)}$; d'où l'on conclut facilement que $\frac{T'}{U'} > \frac{t^{(n+1)}}{u^{(n+1)}}$. De là et de la conclusion précédente, il suit que

$$(U't^{(n)} - T'u^{(n)})\left(t^{(n)} + u^{(n)}\frac{T'}{U'}\right) > (u^{(n+1)}t^{(n)} - t^{(n+1)}u^{(n)})\left(t^{(n)} + u^{(n)}\frac{t^{(n+1)}}{u^{(n+1)}}\right).$$

En développant, et remplaçant T'^2, $t^{(n)}.t^{(n)}$, $t^{(n+1)}.t^{(n+1)}$ par leurs valeurs $DU'^2 + m^2$, $Du^{(n)}.u^{(n)} + m^2$, $Du^{(n+1)}.u^{(n+1)} + m^2$, on a

$$\frac{1}{U'}(U'^2 - u^{(n)}u^{(n)}) > \frac{1}{u^{(n+1)}}(u^{(n+1)}u^{(n+1)} - u^{(n)}u^{(n)}),$$

ou transposant, ce qui est permis puisque les quantités sont positives,

$$U' + \frac{u^{(n)}\,u^{(n)}}{u^{(n+1)}} > u^{(n+1)} + \frac{u^{(n)}\,u^{(n)}}{U'},$$

résultat absurde, puisque $U' < u^{(n+1)}$, et que partant $\frac{u^{(n)}\,u^{(n)}}{u^{(n+1)}} < \frac{u^{(n)}\,u^{(n)}}{U'}$. Ainsi la supposition ne peut avoir lieu, et les séries t^0, t', t'', etc.; u^0, u', u'', etc.; renferment toutes les valeurs positives de t et u.

Exemple. Pour $D = 61$ et $m = 2$, nous avons trouvé que les plus petites valeurs de t et u étaient 1523, 195; ainsi toutes les valeurs positives seront données par les formules

$$t = \left(\frac{1523}{2} + \frac{195}{2}\sqrt{61}\right)^e + \left(\frac{1523}{2} - \frac{195}{2}\sqrt{61}\right)^e \ldots\ldots$$

$$u = \frac{1}{\sqrt{61}}\left\{\left(\frac{1523}{2} + \frac{195}{2}\sqrt{61}\right)^e - \left(\frac{1523}{2} - \frac{195}{2}\sqrt{61}\right)^e\right\},$$

et l'on trouve

$t^0 = 2$, $t' = 1523$, $t'' = 1523t' - t^0 = 2319527$, $t''' = 1523t'' - t' = 3532618098$, etc.
$u^0 = 0$, $u' = 195$, $u'' = 1523u' - u^0 = 296985$, $u''' = 1523u'' - u' = 452307960$, etc.

201. Relativement au problème résolu dans les numéros précédens, nous ajouterons encore quelques observations.

I. Comme nous avons appris à résoudre l'équation $t^2 - Du^2 = m^2$, où m est le plus grand diviseur commun des nombres $M, 2N, P$, tels qu'on ait $N^2 - MP = D$, il est utile d'assigner les nombres qui peuvent être de tels diviseurs, c'est-à-dire, toutes les valeurs de m pour une valeur donnée de D.

On fera $D = n^2 D'$, desorte que D' soit délivré de tout facteur quadratique, ce qu'on obtiendra en prenant pour n^2 le plus grand quarré qui puisse diviser D. Si D ne renfermait aucun facteur quadratique, il faudrait prendre $n = 1$.

1°. Si D' est de la forme $4k+1$, tout diviseur de $2n$ sera une valeur de m et réciproquement. En effet, si g divise $2n$, on aura la forme $\left(g, n, \frac{-n^2(D'-1)}{g}\right)$, dont le déterminant est D, et dans laquelle g est évidemment le plus grand diviseur commun entre g, $2n$, $\frac{n^2(D'-1)}{g}$; (car $\frac{n^2(D'-1)}{g^2} = \frac{4n^2}{g^2} \cdot \frac{D'-1}{4}$ est évidemment un nombre entier). Réciproquement, si g est une valeur de m, c'est-à-dire, si g est le plus grand commun diviseur des nombres $M, 2N, P$, et qu'on ait $N^2 - MP = D$, il est évident que $4D$ ou $4n^2 D'$ sera divisible par g^2, et il suit de là que $2n$ est nécessairement divisible par g; car si g ne divisait pas $2n$, g et $2n$ auraient pour plus grand commun diviseur un nombre $\delta < g$, et en faisant $2n = \delta n'$, $g = \delta g'$, $\frac{n'^2 D}{g'^2}$ serait un nombre entier; mais n' est premier avec g', et partant n'^2 avec g'^2; donc D' serait divisible par g'^2, contre l'hypothèse, puisque D' est délivré de tout facteur quadratique.

2°. Si D' est de la forme $4k+2$ ou $4k+3$, tout diviseur de n sera valeur de m, et réciproquement toute valeur de m divisera n. En effet, si g est diviseur de n, on aura la forme $\left(g, o, \frac{-n^2 D'}{g}\right)$, dont le déterminant est D, et où g est évidemment le plus grand commun diviseur des nombres g, o, $\frac{n^2 D'}{g}$. Réciproquement, si g est supposé valeur de m, c'est-à-dire, le plus grand commun diviseur

viseur des nombres M, $2N$, P, pour lesquels on a $N^2 - MP = D$, on prouvera, comme ci-dessus, que $\frac{2n}{g}$ est un nombre entier. Or supposons que ce quotient soit impair, le quarré $\frac{4n^2}{g^2}$ sera $\equiv 1$ (mod. 4), et partant $\frac{4n^2D'}{g^2} \equiv D' \equiv 2$ ou $\equiv 3$ (mod. 4). Mais $\frac{4n^2D'}{g^2} = \frac{4D}{g^2} = \frac{4N^2}{g^2} - \frac{4MP}{g^2} \equiv \frac{4N^2}{g^2}$ (mod. 4); ainsi $\frac{4N^2}{g^2}$ serait $\equiv 2$ ou $\equiv 3$ (mod. 4), ce qui est absurde, puisqu'un quarré doit être congru à zéro ou à l'unité, suivant le module 4. Donc $\frac{2n}{g}$ étant pair, $\frac{n}{g}$ sera entier et n divisible par g.

Ainsi il est clair que 1 est toujours valeur de m, c'est-à-dire que l'équation $t^2 - Du^2 = 1$ est toujours résoluble par ce qui précède, pour toute valeur de D positive et non quarrée. Ce nombre 2 ne sera valeur de m que dans le cas où B sera de la forme $4k$ ou de la forme $4k+1$.

II. Si m est plus grand que 2, mais qu'il soit un nombre convenable, la solution de l'équation $t^2 - Du^2 = m^2$ pourra être ramenée à celle d'une équation semblable où $m = 1$ ou 2. En effet posons, comme plus haut, $D = n^2D'$, si m divise n, m^2 divisera D. Alors si l'on suppose que pour l'équation $p^2 - \frac{D}{m^2}q^2 = 1$, les plus petites valeurs de p et q soient $p = P$, $q = Q$; les plus petites valeurs de t, u, dans l'équation $t^2 - Du^2 = m^2$ seront $t = mP$, $u = Q$. Mais si m ne divise pas n, il divisera au moins $2n$; alors il sera pair, et partant $\frac{4D}{m^2}$ sera un nombre entier, et si les plus petites valeurs de p et q dans l'équation $p^2 - \frac{4D}{m^2}q^2 = 4$ sont $p = P$, $q = Q$, les plus petites valeurs de t, u, dans l'équation $t^2 - Du^2 = m^2$, seront $t = \frac{m}{2}P$, $u = Q$.

Au reste, dans les deux cas, on peut déduire, non-seulement les plus petites valeurs de t, u, de la connaissance des plus petites valeurs de p, q, mais toutes les valeurs des premières de toutes les valeurs des secondes.

III. En désignant par t°, u°; t', u'; t'', u'', etc. toutes les valeurs positives de t, u dans l'équation $t^2 - Du^2 = m^2$, comme dans le n° précédent, s'il arrive que certaines valeurs dans cette série soient congrues aux premières, suivant un module quelconque donné r; si, par exemple, on a $t^{(\mu)} \equiv t^\circ \equiv m$, $u^{(\mu)} \equiv u^\circ \equiv 0 \pmod{r}$, et que les valeurs suivantes le soient aux secondes, $t^{(\mu+1)} \equiv t'$, $u^{(\mu+1)} \equiv u'$; on aura de même $t^{(\mu+2)} \equiv t''$, $u^{(\mu+2)} \equiv u''$, etc., ce qui se déduit facilement de la loi même des deux séries. En effet, puisque $t'' = \frac{2T}{m} t' - t^\circ$, et que $t^{(\mu+2)} = \frac{2T}{m} t^{(\mu+1)} - t^{(\mu)}$, on aura $t'' \equiv t^{(\mu+2)}$, et ainsi des autres. Il suit de là qu'on a généralement $t^{(h+\mu)} \equiv t^{(\mu)}$, $u^{(h+\mu)} \equiv u^{(\mu)} \pmod{r}$, h étant un nombre quelconque, et plus généralement si $\pi \equiv \nu \pmod{\mu}$, on aura $t^{(\pi)} \equiv t^{(\nu)}$ et $u^{(\pi)} \equiv u^{(\nu)} \pmod{r}$.

IV. Or on peut toujours satisfaire aux conditions de l'observation précédente, c'est-à-dire, on peut toujours trouver un indice μ pour lequel on ait $t^\mu \equiv t^\circ$, $t^{\mu+1} \equiv t'$, $u^\mu \equiv u^\circ$, $u^{\mu+1} \equiv u'$, suivant un module quelconque donné r. En effet,

1°. On peut toujours satisfaire à la troisième condition, puisqu'il est aisé de s'assurer, par les caractères présentés dans la première observation, que l'équation $p^2 - r^2 D q^2 = m^2$ est résoluble; et si les plus petites valeurs de p, q sont $p = P$, $q = Q$, on en déduira $t = P$, $u = rQ$; ainsi P et rQ seront contenus dans les suites t°, t', etc., u°, u', etc.; et si $P = t^{(\lambda)}$, $rQ = u^{(\lambda)}$, on aura $u^{(\lambda)} \equiv 0 \equiv u^\circ \pmod{r}$. En outre on voit facilement qu'entre u° et u^λ aucun terme ne sera congru à u°, suivant le module r.

2°. Il est clair que si dans ce cas les trois autres conditions sont remplies, c'est-à-dire, si $u^{(\lambda+1)} \equiv u'$, $t^{(\lambda)} \equiv t^\circ$, $t^{(\lambda+1)} \equiv t'$, on pourra prendre $\mu = \lambda$; mais si l'une de ces conditions manque, on pourra prendre à coup sûr $\mu = 2\lambda$. En effet, de l'équation (1) et des formules générales qui donnent $t^{(\varphi)}$ et $u^{(\varphi)}$ dans le n° précédent, on déduit

$$t^{(2\lambda)}=\frac{1}{m}\left(t^{(\lambda)}.t^{(\lambda)}+Du^{(\lambda)}u^{(\lambda)}\right)=\frac{1}{m}\left(m^{\lambda}+2Du^{(\lambda)}u^{(\lambda)}\right),$$

et partant $\frac{t^{(2\lambda)}-t^{\circ}}{r}=\frac{2Du^{(\lambda)}.u^{(\lambda)}}{mr}$, qui est un nombre entier; puisque r divise $u^{(\lambda)}$, et que, m^{λ} divisant $4D$, à plus forte raison m divisera $2D$. On trouvera de même $u^{(2\lambda)}=\frac{2}{m}t^{(\lambda)}u^{(\lambda)}$, et comme $4t^{(\lambda)}t^{(\lambda)}=4Du^{(\lambda)}u^{(\lambda)}+4m^{\lambda}$ et est parconséquent divisible par m^{λ}, $2t^{(\lambda)}$ le sera par m, et partant $u^{(2\lambda)}$ par r, c'est-à-dire que $u^{(2\lambda)}\equiv u^{\circ}$ (mod. r). On a encore $t^{(2\lambda+1)}=t'+\frac{2Du^{(\lambda)}u^{(\lambda+1)}}{m}$, et comme, par la même raison, $\frac{2Du^{(\lambda)}}{mr}$ est un nombre entier, on en déduit $t^{(2\lambda+1)}\equiv t'(\text{mod.}\,r)$: enfin on trouve $u^{(2\lambda+1)}=u'+\frac{2t^{(\lambda+1)}u^{(\lambda)}}{m}$, et comme $2t^{(\lambda+1)}$ est divisible par m et $u^{(\lambda)}$ par r, il s'ensuit que $u^{(2\lambda+1)}\equiv u'$ (mod. r).

Au reste, on reconnaîtra par la suite l'usage de ces deux dernières observations.

202. Le cas particulier où l'équation est $t^{2}-Du^{2}=1$ a déjà été traité par les géomètres du siècle dernier. *Fermat* avait proposé ce problème aux analystes anglais, et *Wallis* rapporte (*Algèb. chap.* 98, *T. II de ses Œuvres, p.* 418), une solution qu'il attribue à *Brounker*. De son côté, *Ozanam* prétend qu'elle est de *Fermat*; enfin *Euler*, qui s'en est occupé, (*Comm. Petrop. VI, p.* 175; *Comm. Nov. XI, p.* 28 (*); *Algèbre, T. II, p.* 226; *Opusc. Anal. I, p.* 310), dit que *Pellius* l'a trouvée le premier, ce qui a fait donner par quelques-uns à ce problème le nom de *Pellien*. Toutes ces solutions, en n'en regardant que l'esprit, retombent dans celle

(*) Dans ce Mémoire, l'algorithme que nous avons exposé n° 32, est présenté avec les mêmes signes, ce que nous avons négligé de remarquer alors.

que nous obtenons, si, dans le n° 198, nous nous servons d'une forme réduite dans laquelle $a=1$; mais personne, avant *Lagrange*, n'avait démontré rigoureusement (*) que l'opération qu'elles prescrivent devait nécessairement finir, c'est-à-dire, que le problême était toujours résoluble (*Mélanges de la Société de Turin, T. IV, p.* 19, et d'une manière plus élégante, *Hist. de l'Acad. de Berlin*, 1767, *p.* 237). Cette recherche se trouve encore dans les *Supplémens à l'Algèbre d'Euler*. Au reste, notre méthode, tirée de principes absolument différens, ne se borne pas au cas de $m=1$, et donne le plus souvent différens moyens de parvenir à la solution, puisque dans le n° 198, nous pouvons partir d'une forme réduite quelconque $(a, b, -a')$.

203. PROBLÈME. *Si les formes* Φ *et* φ *sont équivalentes, trouver toutes les transformations de l'une en l'autre.*

Quand ces formes ne seront équivalentes que d'une seule manière, c'est-à-dire, ou proprement ou improprement, on cherchera, par le n° 196, une transformation $\alpha, \beta, \gamma, \delta$ de la forme φ en Φ, et il est clair qu'il n'y aura pas d'autres transformations qui ne soient semblables à celle-là. Mais quand φ et Φ seront équivalentes des deux manières, on cherchera deux transformations dissemblables, c'est-à-dire, une propre et une impropre, $\alpha, \beta, \gamma, \delta$; $\alpha', \beta', \gamma', \delta'$, et toute autre transformation sera semblable à l'une d'elles. Si donc $\varphi = (a, b, c)$ et que son déterminant soit D, que m soit, à l'ordinaire, le plus grand commun diviseur des nombres $a, 2b, c$ et t, u les valeurs indéterminées qui satisfont à l'équation $t^2 - Du^2 = m^2$; dans le premier cas, toutes les transformations de φ en Φ seront contenues dans la première (1) des formules suivantes, et dans le second cas, dans la première (1) et dans la seconde (2):

(*) Ce que *Wallis* a avancé à ce sujet (*Alg. pp.* 427, 428), n'est d'aucun poids. Le paralogisme consiste en ce qu'il suppose qu'étant donnée une quantité p on peut trouver des nombres entiers a et z tels que $\frac{z}{a}$ soit $< p$, et que la différence soit plus petite qu'un nombre assigné, ce qui est vrai quand la différenc assignée a une valeur déterminée, mais non lorsque, comme dans le cas présent elle est fonction de a et de z, et partant variable.

$$(1)\ldots\ldots \frac{1}{m}(\alpha t-(\alpha b+\gamma c)u),\ \frac{1}{m}(\beta t-(\beta b+\delta c)u),$$
$$\frac{1}{m}(\gamma t+(\alpha a+\gamma b)u),\ \frac{1}{m}(\delta t+(\beta a+\delta b)u);$$
$$(2)\ldots\ldots \frac{1}{m}(\alpha' t-(\alpha' b+\gamma' c)u),\ \frac{1}{m}(\beta' t-(\beta' b+\delta' c)u),$$
$$\frac{1}{m}(\gamma' t+(\alpha' a+\gamma' b)u),\ \frac{1}{m}(\delta' t+(\beta' a+\delta' b)u).$$

Exemple. On demande toutes les transformations de la forme (129, 92, 65) en la forme (42, 59, 81). Nous avons trouvé (n° 195) qu'elles étaient improprement équivalentes, et dans le n° suivant nous avons eu cette transformation impropre : $-47, -56, 73, 87$; ainsi toutes les transformations semblables seront contenues dans les formules

$$-(47t+421u),\ -(56t+503u),\ 73t+653u,\ 87t+780u,$$

t, u étant les nombres indéterminés qui satisfont à l'équation $t^2-79u^2=1$; ils sont donnés par les formules

$$\pm t = \frac{1}{2}\{(80+9\sqrt{79})^e+(80-9\sqrt{79})^e\},$$
$$\pm u = \frac{1}{2\sqrt{79}}\{(80+9\sqrt{79})^e-(80-9\sqrt{79})^e\},$$

où l'on doit prendre pour e tous les nombres entiers positifs.

204. Il est évident que la formule générale qui donne toutes les transformations, devient d'autant plus simple, que la transformation initiale d'où elle est tirée l'est elle-même davantage, et comme il est indifférent de quelle transformation on parte, on peut souvent rendre la formule générale plus simple, si de la première qu'on trouve, on déduit une transformation plus simple en attribuant à t, u des valeurs déterminées, et si l'on forme avec une autre formule. En faisant, par exemple, dans la formule de l'exemple précédent, $t=80$, $u=-9$, il en résulte une transformation plus simple que celle d'où nous étions partis, savoir, $29, 47, -37, -60$; d'où l'on déduit la transformation générale

$$29t-263u,\ 47t-424u,\ -37t+337u,\ -60t+543u.$$

Ainsi, lorsqu'on a trouvé la formule générale au moyen de ce qui précède, on pourra essayer si en attribuant à t, u les valeurs

déterminées $\pm t'$, $\pm t''$, $\pm t'''$, etc.; $\pm u'$, $\pm u''$, $\pm u'''$, etc. on obtient une transformation plus simple que celle d'où l'on a déduit la formule, et dans ce cas on pourra trouver une formule plus simple. Au reste, il y a quelque chose d'arbitraire dans le choix, desorte qu'il serait utile de l'amener à une règle certaine et d'assigner dans la progression t', u'; t'', u'', etc. des limites après lesquelles on n'obtient que des transformations moins simples, desorte qu'il fût suffisant de faire les essais parmi elles. Cependant comme le plus souvent, par les méthodes que nous avons données, on obtient la transformation la plus simple, soit sur-le-champ, soit en employant les valeurs $\pm t'$, $\pm u'$, nous supprimons cette recherche.

205. PROBLÈME. *Trouver toutes les représentations d'un nombre donné* M *par une forme donnée* $ax^2+2bxy+cy^2$, *dont le déterminant positif non quarré est* $=D$.

Observons d'abord que la recherche des représentations par des valeurs de x, y non premières entre elles, peut se ramener ici absolument de la même manière que pour les formes de déterminant négatif (n° 181), au cas où ces valeurs sont premières entre elles. Or pour qu'il soit possible de représenter le nombre M par des valeurs premières entre elles, il faut que D soit résidu quadratique de M, et si les valeurs de l'expression $\sqrt{D}$ (mod. M) sont: N, $-N$, N', $-N'$, etc. qu'on peut prendre telles qu'aucune ne soit $>\frac{1}{2}M$, toute représentation du nombre M par la forme proposée appartiendra à une de ces valeurs. Ainsi, avant tout, on devra chercher les nombres N, N', etc. et ensuite les représentations qui appartiennent à chacun d'eux. Il n'y aura pas de représentations appartenantes à la valeur N, si les formes (a, b, c), $\left(M, N, \frac{N^2-D}{M}\right)$ ne sont pas proprement équivalentes; mais si elles le sont, on cherchera une transformation propre $\alpha, \beta, \gamma, \delta$ de la première en la seconde, alors on aura, en faisant $x=\alpha$, $y=\gamma$ une représentation du nombre M appartenante à la valeur N, et toutes les représentations seront données par les formules

$$x=\frac{1}{m}\{\alpha t-(\alpha b+\gamma c)u\}\ldots\ldots y=\frac{1}{m}\{\gamma t+(\alpha a+\gamma b)u\}.$$

Au reste, il est évident que cette formule générale sera d'autant plus simple, que la transformation $\alpha, \beta, \gamma, \delta$, dont elle est déduite, le sera elle-même davantage. Ainsi il sera utile de trouver, d'après le n° précédent, la transformation la plus simple de la forme (a, b, c) en la forme $\left(M, N, \frac{N^2-D}{M}\right)$. On trouvera absolument de la même manière les formules générales qui donnent les représentations appartenantes aux valeurs $-N, N', -N'$, etc., s'il en existe.

Exemple. On cherche les représentations du nombre 585 par la forme $42x^2+62xy+21y^2$.

Pour ce qui regarde les représentations par des valeurs de x, y non premières entre elles, il est clair qu'il ne peut y en avoir d'autres que celles où le plus grand diviseur commun des nombres x, y serait 3, puisque 9 est le seul diviseur quadratique de 585. Ainsi quand on aura les représentations du nombre $65=\frac{585}{9}$ par la forme $42x'^2+62x'y'+21y'^2$, dans lesquelles x' et y' sont premiers entre eux, on en tirera toutes les représentations du nombre 585, par la forme $42x^2+62xy+21y^2$, en posant $x=3x'$ et $y=3y'$.

Les valeurs de l'expression $\sqrt{79}$ (mod. 65) sont ± 12, ± 27. On trouve que la représentation du nombre 65 appartenante à la valeur -12, est $x'=2, y'=-1$, d'où il suit que toutes les représentations de 65 appartenantes à la même valeur seront données par la formule $x'=2t-41u$, $y'=-t+53u$, et partant toutes les représentations du nombre 585, par la formule $x=6t-123u$, $y=-3t+159u$. De la même manière, on trouve que les représentations du nombre 65 appartenantes à la valeur 12 sont données par la formule générale $x'=22t-199u$, $y'=-23t+211u$, et celles qui en naissent pour 585 par $x=66t-597u$, $y=-69t+633u$. Mais il n'y a aucune représentation du nombre 65 appartenante à la valeur ± 27.

Pour trouver les représentations de 585 par des valeurs de x, y premières entre elles, il faut d'abord trouver les valeurs de l'expression $\sqrt{79}$ (mod. 585) qui sont ± 77, ± 103, ± 157, ± 248. On trouve qu'aucune représentation n'appartient aux valeurs ± 77, ± 103, ± 248. Mais pour la valeur -157 on a la repré-

sentation $x=3$, $y=1$, d'où l'on tire la formule générale $x=3t-114u$, $y=t+157u$. Pour la valeur $+157$, on a de même la représentation $x=83$, $y=-87$, et la formule qui contient toutes les transformations semblables est $x=83t-746u$, $y=-87t+789u$.

On a donc quatre formules générales, dans lesquelles sont contenues toutes les représentations du nombre 585 par la forme $42x^2+62xy+21y^2$,

$x=6t-123u$, $y=-3t+159u$, $x=66t-597u$, $y=-69t+633u$,
$x=3t-114u$, $y=t+157u$, $x=83t-746u$, $y=-87t+789u$.

Pour abréger, nous ne nous arrêterons pas davantage aux applications particulières des recherches précédentes, parceque chacun pourra y parvenir de lui-même, en imitant ce qui a été fait n°s 176, 182, et nous passons aux formes de déterminant positif quarré qui nous restent à examiner.

206. PROBLÈME. *Étant donnée une forme* (a, b, c) *de déterminant quarré* h^2 *dont* h *est la racine positive, trouver une forme* (A, B, C) *qui lui soit proprement équivalente, dans laquelle* A *tombe entre* 0 *et* 2h$-$1 *inclusivement, et où l'on ait* B$=$h, C$=$0.

I. Puisque $h^2=b^2-ac$, on aura $\frac{h-b}{a}=\frac{c}{-(h+b)}$. Soit fait ce rapport $=\frac{\beta}{\delta}$, β étant premier avec δ, et déterminons α, γ de manière que $\alpha\delta-\beta\gamma=1$, ce qui peut se faire. Par la substitution α, β, γ, δ, la forme (a, b, c) se changera en une autre (a', b', c'), qui lui sera proprement équivalente. Or on aura

$$b'=a\alpha\beta+b(\alpha\delta+\beta\gamma)+c\gamma\delta=(h-b)\alpha\delta+b(\alpha\delta+\beta\gamma)-(h+b)\beta\gamma=h(\alpha\delta-\beta\gamma)=h$$
$$c'=a\beta^2+2b\beta\delta+c\delta^2=(h-b)\beta\delta+2b\beta\delta-(h+b)\beta\delta=0.$$

Si donc a' est situé entre 0 et $2h-1$, la forme (a', b', c') satisfera à toutes les conditions.

II. Mais si a' tombe hors de ces deux limites, soit A le résidu *minimum* positif de A', suivant le module $2h$, A sera évidemment entre 0, et $2h-1$; soit posé $A-a'=2hk$, alors la forme $(a', b', c')=(a', h, 0)$, se changera, par la substitution 1, 0, k, 1, en $(A, h, 0)$ qui sera proprement équivalente aux formes (a', b', c'),

$(a,$

(a, b, c), et satisfera à toutes les conditions. Au reste, il est aisé de voir que la forme (a, b, c) se change en $(A, h, 0)$ par la substitution $\alpha+\beta k, \beta, \gamma+\delta k, \delta$.

Exemple. Soit la forme (27, 15, 8) dont le déterminant est 9; ici $h=3$ et $\frac{\beta}{\delta}=\frac{4}{-9}$; en prenant donc $\beta=4$, $\delta=-9$, $\alpha=-1$, $\gamma=2$, la forme $(a', b' c')$ se trouve être $(-1, 3, 0)$, qui se change en $(5, 3, 0)$ par la substitution $1, 0, 1, 1$. Cette dernière est par-conséquent la forme demandée, et la proposée se change en elle par la substitution propre $3, 4, -7, -9$.

Les formes telles que $(A, h, 0)$, dans lesquelles A est compris entre 0 et $2h-1$ inclusivement, s'appelleront *formes réduites;* mais il faut bien les distinguer des formes réduites de déterminant négatif et de déterminant positif non quarré.

207. THÉORÈME. *Deux formes réduites* $(a, h, 0)$, $(a', h, 0)$ *ne peuvent être proprement équivalentes sans être identiques.*

En effet, si on les suppose proprement équivalentes, soit $\alpha, \beta, \gamma, \delta$ la transformation qui change la première en la seconde, on aura les équations

$$a\alpha^2+2h\alpha\gamma=a' \ldots\ldots(1) \qquad a\alpha\beta+h(\alpha\delta+\beta\gamma)=h \ldots\ldots(2)$$
$$a\beta^2+2h\beta\delta=0 \ldots\ldots(3) \qquad a\delta-\beta\gamma=1 \ldots\ldots\ldots\ldots(4).$$

De l'équation (3) on tire $\beta=0$ ou $a\beta+2h\delta=0$; mais si l'on suppose que β ne soit pas zéro, comme l'équation (2) peut se mettre sous la forme $a\alpha\beta+2h\beta\gamma=0$, qui donne alors nécessairement $a\alpha+2h\gamma=0$, il s'ensuivrait par l'équation (1) que $a'=0$. Donc on doit seulement supposer $\beta=0$, ce qui réduit l'équation (4) à $\alpha\delta=1$, d'où $\alpha=\pm 1$. Ainsi l'équation (1) devient $a\pm 2h\gamma=a'$, ce qui ne peut avoir lieu qu'en supposant $\gamma=0$, puisque a et a' sont tous les deux compris entre 0 et $2h-1$; ainsi on a donc $a=a'$, c'est-à-dire que les deux formes sont identiques.

On résout par là sans difficulté les problèmes suivans, qui en offraient beaucoup pour les autres déterminans.

I. *Déterminer si deux formes* F, F', *de même déterminant quarré, sont équivalentes ou non.*

On cherchera deux formes réduites équivalentes aux formes F et F' respectivement, et suivant que ces réduites seront ou non identiques, les formes proposées seront ou non équivalentes.

II. *Déterminer si deux formes* F, F' *sont improprement équivalentes.*

Soit G la forme opposée à l'une des deux formes, à F, par exemple; si G est proprement équivalente à F', F et F' seront improprement équivalentes.

208. PROBLÈME. *Étant données deux formes* F *et* F' *de même déterminant* h² *proprement équivalentes, trouver une transformation propre de l'une en l'autre.*

Soit φ la réduite équivalente à F et à F'; on cherchera par le n° 106 une transformation propre $\alpha, \beta, \gamma, \delta$ de F en φ, et une transformation propre $\alpha', \beta', \gamma', \delta'$ de F' en φ. Alors φ se changera en F' par la substitution propre $\delta', -\beta', -\gamma', \alpha'$, et partant F en F' par la substitution propre $\alpha\delta'-\beta\gamma'$, $\beta\alpha'-\alpha\beta'$, $\gamma\delta'-\delta\gamma'$, $\delta\alpha'-\gamma\beta'$.

Il peut être utile de donner pour cette transformation de F en F' une autre formule, pour laquelle il n'est pas nécessaire de connaître la réduite φ elle-même. Soit $F=(a, b, c)$, $F'=(a', b', c')$, $\varphi=(A, h, 0)$; puisque $\frac{\beta}{\delta}$ est la plus simple expression de la fraction $\frac{h-b}{a}$ ou de la fraction $\frac{c}{-(h+b)}$, on aura $\frac{h-b}{\beta}=\frac{a}{\delta}$ égal à un entier que nous supposerons $=f$, et de même $\frac{c}{\beta}=\frac{-h-b}{\delta}=g$. On a

$$A=a\alpha^2+2b\alpha\gamma+C\gamma^2, \quad \text{d'où} \quad \beta A=a\alpha^2\beta+2b\alpha\beta\gamma+C\gamma^2\beta,$$

ou en substituant pour $a\beta$, $\delta(h-b)$, pour c, βg,

$$\beta A=\alpha^2\delta h+b(2\beta\gamma-\alpha\delta)\alpha+\beta^2\gamma^2 g;$$

et comme $b=-h-\delta g$,

$$\beta A=2\alpha(\alpha\delta-\beta\gamma)h+(\alpha\delta-\beta\gamma)^2 g=2\alpha h+g;$$

de même

$$\delta A = a\alpha^2\delta + 2b\alpha\gamma\delta + c\gamma\delta = \alpha^2\delta^2 f + b(2\alpha\delta - \beta\gamma)\gamma - \beta\gamma^2 h$$
$$= (\alpha\delta - \beta\gamma)^2 f + 2\gamma(\alpha\delta - \beta\gamma)h = f + 2\gamma h;$$

donc $\alpha = \frac{\beta A - g}{2h}$ et $\gamma = \frac{\delta A - f}{2h}$.

On a de même, relativement à la forme F', $\alpha' = \frac{\beta' A - g'}{2h}$ et $\gamma' = \frac{\delta' A - f'}{2h}$.

En substituant ces valeurs de α, γ, α', γ' dans la formule précédente, elle se change en la substitution suivante :

$$\frac{\beta f' - \delta' g}{2h}, \frac{\beta' g - \beta g'}{2h}, \frac{\delta f' - \delta' f}{2h}, \frac{\beta' f - \delta g'}{2h};$$

d'où A a disparu.

Si l'on propose deux formes F, F' improprement équivalentes, et qu'on demande une transformation impropre de l'une en l'autre, soit G la forme opposée à F, et α, β, γ, δ une transformation propre de G en F', il est clair que α, β, $-\gamma$, $-\delta$, sera une transformation impropre de F en F'.

Enfin on voit que si les formes sont proprement et improprement équivalentes, on pourra trouver de cette manière deux transformations, l'une propre et l'autre impropre.

209. Il ne nous reste plus parconséquent qu'à déduire d'une seule transformation toutes celles qui lui sont semblables, ce qui dépend de la solution de l'équation $t^2 - h^2u^2 = m^2$. Mais cette équation ne peut se résoudre que de deux manières, savoir, en faisant $t = m$, $u = 0$, ou $t = -m$, $u = 0$. Supposons en effet une autre solution $t = T$, $u = U$ où U ne soit pas zéro; comme m^2 divise $4h^2$, on aura $\frac{4T^2}{m^2} = \frac{4h^2U^2}{m^2} + 4$, et $\frac{4T^2}{m^2}$, ainsi que $\frac{4h^2U^2}{m^2}$ sont des quarrés entiers; mais on voit facilement que la différence de deux quarrés entiers ne peut être 4, à moins que le plus petit ne soit $= 0$; si donc la forme F se change en F' par la transformation α, β, γ, δ, on ne trouvera d'autre transformation semblable que $-\alpha$, $-\beta$, $-\gamma$, $-\delta$, et si elles ne sont équivalentes que d'une manière, il n'y aura que deux transformations; il y en aura quatre si elles sont équivalentes des deux manières, savoir, deux propres et deux impropres.

210. THÉORÈME. *Si deux formes réduites* (a, h, o), (a′, h, o) *sont improprement équivalentes, on aura* $aa' \equiv m^2 \pmod{2mh}$, m *étant le plus grand commun diviseur des nombres* a, 2h *ou* a′, 2h; *et réciproquement si* a, 2h; a′, 2h *ont le même plus grand diviseur commun* m, *et qu'on ait* $aa' \equiv m^2 \pmod{2hm}$, *les formes* (a, h, o), (a′, h, o) *seront improprement équivalentes.*

I. Si la forme (a, h, o) se change en (a', h, o) par la transformation impropre $\alpha, \beta, \gamma, \delta$, on aura les équations

$$a\alpha^2 + 2h\alpha\gamma = a' \ldots\ldots\ldots (1), \quad a\alpha\beta + h(\alpha\delta + \beta\gamma) = h \ldots\ldots (2),$$
$$a\beta^2 + 2h\beta\delta = o \ldots\ldots\ldots (3), \quad \alpha\delta - \beta\gamma = -1 \ldots\ldots\ldots (4).$$

On déduit de l'équation (1)

$$(a\alpha + 2h\gamma)^2 - (a\alpha + 2h\gamma)2h\gamma = aa', \text{ ou } (a\alpha + 2h\gamma)^2 \equiv aa' \pmod{2h\gamma.(a\alpha + 2h\gamma)}$$

Or en combinant les équations (2) et (4), on tire $(a\beta + 2h\delta)\alpha = o$, et comme la supposition $\alpha = o$ réduirait l'équation (1) à $a' = o$, contre l'hypothèse, on doit avoir $a\beta + 2h\delta = o$, ou $\frac{\beta}{\delta} = -\frac{2h}{a}$, et partant $\beta = \pm\frac{2h}{m}$, $\delta = \mp\frac{a}{m}$; l'équation (4) donne alors $\frac{\mp a\alpha \mp 2h\gamma}{m} = -1$, ou $a\alpha + 2h\gamma = \pm m$. Ainsi la congruence que nous avions trouvée devient $m^2 \equiv aa' \pmod{2mh}$.

II. Si m est le plus grand diviseur commun des nombres a, $2h$; a', $2h$, et qu'on ait $aa' \equiv m^2 \pmod{2mh}$, $\frac{a}{m}$, $\frac{2h}{m}$, $\frac{a'}{m}$, $\frac{aa' - m^2}{2mh}$ seront entiers, et l'on s'assure aisément que la forme (a, h, o) se change en (a', h, o) par la substitution $-\frac{a'}{m}$, $-\frac{2h}{m}$, $\frac{aa' - m^2}{2mh}$, $\frac{a}{m}$, et que cette substitution est impropre. Ainsi ces formes seront improprement équivalentes.

On peut aussi juger sur-le-champ si une forme réduite (a, h, o) est improprement équivalente à elle-même, puisqu'on aura alors $a^2 \equiv m^2 \pmod{2mh}$.

211. On trouve toutes les formes réduites de déterminant h^2 en prenant pour A dans la forme (A, h, o) tous les nombres entiers depuis et y compris o, jusqu'à $2h - 1$ inclusivement; ainsi le nombre en sera $2h$. Il est évident que l'on peut distribuer toutes les formes de déterminant h^2 en autant de classes, et qu'elles jouiront de la même propriété que ci-dessus (nos 175, 185), pour les formes de déterminant négatif et de déterminant positif non quarré.

Ainsi toutes les formes de déterminant $=25$ peuvent se distribuer en dix classes, qui se distingueront par les différentes formes réduites qui y seront contenues. Ces formes réduites sont : (0, 5, 0), (1, 5, 0), (2, 5, 0), (5, 5, 0), (8, 5, 0), (9, 5, 0), qui sont improprement équivalentes à elles-mêmes; (3, 5, 0), qui est improprement équivalente à (7, 5, 0); (4, 5, 0), qui est improprement équivalente à (6, 5, 0).

212. PROBLÈME. *Trouver toutes les représentations d'un nombre donné* M, *par une forme donnée* $ax^2+2bxy+cy^2$ *de déterminant* h^2.

On peut tirer la solution de ce problème, des principes de l'art. 165, absolument de la même manière que nous l'avons fait plus haut (nos 180, 181, 205), pour les formes de déterminant négatif, et positif non quarré, et comme il n'y a en cela aucune difficulté, il serait superflu de le reprendre ici. Mais il ne sera pas hors de propos de déduire la solution d'un autre principe qui est propre à ce cas particulier.

Ayant fait comme aux nos 206, 208, $\frac{h-b}{a}=\frac{c}{-(h+b)}=\frac{\beta}{\delta}$, $\frac{h-b}{\beta}=\frac{a}{\delta}=f$, $\frac{c}{\beta}=\frac{-h-b}{\delta}=g$, on prouve sans peine que la forme proposée est le produit des deux facteurs $\delta x-\beta y$ et $fx-gy$; d'où il suit évidemment que toute représentation du nombre M par la forme proposée donne la résolution du nombre M en deux facteurs. Si donc tous les diviseurs du nombre M sont d, d', d'', etc. (1 et M y compris et chacun d'eux étant pris positivement et négativement), il est clair que l'on obtiendra toutes les représentations du nombre M, en posant successivement $\delta x-\beta y=d$, $fx-gy=\frac{M}{d}$; $\delta x-\beta y=d'$, $fx-gy=\frac{M}{d'}$, etc. On tirera de là différentes valeurs de x et de y, parmi lesquelles on rejettera celles qui ne sont pas entières. Or les deux premières équations donnent évidemment

$$x=\frac{\beta M-gd^2}{(\beta f-\delta g)d}\ldots\ldots\ldots\ldots y=\frac{\delta M-fd^2}{(\beta f-\delta g)d},$$

valeurs qui sont toujours déterminées parceque $\beta f-\delta g=2h$, et que parconséquent le dénominateur des fractions n'est jamais $=0$.

On aurait pu tirer de la décomposition en deux facteurs, les problèmes précédens; mais nous avons préféré employer une méthode analogue à celle que nous avions suivie pour les autres déterminans.

Exemple. Cherchons les représentations du nombre 12 par la forme $3x^2+4xy-7y^2$. Cette forme se décompose en deux facteurs $x-y$ et $3x+7y$; les diviseurs du nombre 12 sont: ± 1, 2, 3, 4, 6. 12. Faisons $x-y=1$, $3x+7y=12$, on tire $x=\frac{19}{10}$, $y=\frac{9}{10}$, valeurs à rejeter comme fractionnaires. Les diviseurs -1, ± 3, ± 4, ± 6, ± 12 donnent aussi des valeurs inutiles; mais le diviseur $+2$ donne $x=-2$, $y=0$, et le diviseur -2 donne $x=-2$, $y=0$. Ainsi il n'y aura exactement que ces deux représentations.

Cette méthode ne peut s'employer si $M=0$; mais dans ce cas, il est clair que toutes les valeurs de x et y doivent satisfaire à l'une des équations $\delta x-\beta y=0$, $fx-gy=0$. Or toutes les solutions de la première équation sont contenues dans la formule $x=\beta z$, $y=\delta z$, en désignant par z un nombre quelconque, si β, δ sont premiers entre eux, comme on le suppose. De même, nommant m le plus grand diviseur commun des nombres f, g, toutes les solutions de la seconde équation seront données par la formule $x=\frac{gz}{m}$, $y=\frac{hz}{m}$. Ainsi ces deux formules contiendront toutes les représentations du nombre $M=0$.

Dans ce qui précède, tout ce qui appartient à la recherche des caractères de l'équivalence des formes, à leur transformation et à la représentation des nombres donnés par des formes données, a été expliqué de manière à ne rien laisser à desirer. Il ne nous reste plus parconséquent qu'à prendre deux formes de déterminant différent, qui parconséquent ne peuvent être équivalentes, et à enseigner le moyen de juger si l'une est contenue dans l'autre, et dans ce cas, celui de trouver les transformations de l'une en l'autre.

213. Nous avons déjà fait voir (n°s 157 et 158) que si une forme f de déterminant D renferme la forme F de déterminant E, et se

change en F par la substitution $\alpha, \beta, \gamma, \delta$, on a $E=(\alpha\delta-\beta\gamma)^2 D$, et que si l'on a $\alpha\delta-\beta\gamma=\pm 1$, la forme f non-seulement renferme la forme F, mais lui est équivalente, et que partant, si f renferme F sans lui être équivalente, le quotient $\frac{E}{D}$ sera entier >1. Ainsi le problème à résoudre est : *Juger si une forme donnée* f *de déterminant* D *renferme la forme donnée de déterminant* De^2, où e est supposé un nombre positif >1. Pour y parvenir, nous assignerons un nombre fini de formes contenues sous la forme f, et telles que F soit équivalente à l'une d'elles, si elle est contenue dans f.

I. Soient m, m', m'', etc. les diviseurs positifs du nombre e (y compris 1 et e) et $mn=m'n'=m''n''=\ldots=e$. Désignons, pour abréger, par $(m; 0)$ la forme en laquelle f se change par la substitution propre $m, 0, 0, n$; par $(m; 1)$ celle qui résulte de la substitution propre $m, 1, 0, n$, etc., et généralement par $(m; k)$ celle qui résulte de la substitution propre $m, k, 0, n$. On entendra de même les expressions $(m'; 0)$, $(m'; 1)$, etc. $(m'; k)$, etc. Toutes ces formes seront contenues proprement dans la forme f, et le déterminant de chacune d'elles sera De^2. Nous représenterons par Ω l'ensemble de toutes les formes $(m; 0)$, $(m; 1), \ldots (m; m-1)$; $(m'; 0)$, $(m'; 1), \ldots (m'; m-1)$, etc., dont le nombre est $m+m'+m''+$etc., et qui sont toutes différentes, comme on le verra aisément.

Si l'on a, par exemple, $f=(2, 5, 7)$ et $e=5$, Ω comprendra les six formes (1; 0); (5; 0), (5; 1), (5; 2), (5; 3), (5; 4), qui sont, calcul fait, (2, 25, 175); (50, 25, 7), (50, 35, 19), (50, 45, 35), (50, 55, 55), (50, 65, 79).

II. Or je dis que si la forme F de déterminant De^2 est contenue dans f, elle sera nécessairement proprement équivalente à une des formes Ω. Supposons en effet que f se change en F par la substitution propre $\alpha, \beta, \gamma, \delta$; on aura $\alpha\delta-\beta\gamma=e$ (*). Soit n

(*) L'auteur a été probablement conduit à sa démonstration par l'analyse suivante qui peut la remplacer.

Supposons la forme F renfermée dans la forme f, et que f se change en F par

le plus grand commun diviseur des nombres γ, δ, qui ne peuvent être nuls tous les deux, et $\frac{e}{n}=m$. Soient les nombres g, h tels que $\gamma g+\delta h=n$, k le résidu *minimum* positif du nombre $\alpha g+\beta h$, suivant le module m. Alors la forme $(m; k)$, qui est évidemment une des formes Ω, sera proprement équivalente à la forme F, et se changera même en elle par la substitution propre

$$\frac{\gamma}{n}\cdot\frac{\alpha g+\beta h-k}{m}+h,\quad \frac{\delta}{n}\cdot\frac{\alpha g+\beta h-k}{m}-g,\quad \frac{\gamma}{n},\quad \frac{\delta}{n}.$$

---

la substitution $\alpha, \beta, \gamma, \delta$. Soit φ une des formes Ω, et m, k, o, n, la substitution qui change f en φ. Soit enfin $\alpha', \beta', \gamma', \delta'$ la substitution propre qui change φ en une forme équivalente; la forme f se changera en cette dernière par la substitution : $m\alpha'+k\gamma'$, $m\beta'+k\delta'$. Si donc l'on peut déterminer les nombres $m, k, n, \alpha', \beta', \gamma', \delta'$, de manière qu'on ait

$$m\alpha'+k\gamma'=\alpha,\ m\beta'+k\delta'=\beta,\ n\gamma'=\gamma,\ n\delta'=\delta,$$

il est clair que φ sera équivalente à F.

Or les équations $n\gamma'=\gamma$, $n\delta'=\delta$ donnent $\gamma'=\frac{\gamma}{n}$, $\delta'=\frac{\delta}{n}$: et comme γ', δ' doivent être premiers entre eux, n sera le plus grand commun diviseur des nombres γ, δ. Des deux autres équations, on tire en éliminant m ou k,

$$k=\alpha'\beta-\alpha\beta',\quad m=\alpha\delta'-\beta\gamma';$$

et comme la seconde de ces équations revient évidemment à $\alpha\delta-\beta\gamma=e=mn$, il ne reste plus qu'à satisfaire à la première et à l'équation $\alpha'\delta'-\beta'\gamma'=1$. Si l'on suppose que $\alpha'=h$ et $\beta'=g$ soit une solution quelconque de cette dernière, on aura en général $\alpha'=h+p\gamma'$, $\beta'=g+p\delta'$; substituant ces valeurs dans celle de k, elle devient

$$k=h\beta-g\alpha+p(\beta\gamma'-\alpha\delta)=h\beta-g\alpha-pm,\ \text{ou}\ k\equiv h\beta-g\alpha\ (\text{mod. } m.).$$

Ainsi en prenant pour k le résidu *minimum* positif de $h\beta-g\alpha$, suivant le module m, la forme φ ou $(m; k)$ se trouvera parmi les formes Ω. On a pour lors

$$\alpha'=\gamma'\cdot\frac{h\beta-g\alpha-k}{m}+h,\quad \beta'=\delta'\cdot\frac{h\beta-g\alpha-k}{m}+g,$$

ce qui est, au signe de g près, le résultat de l'auteur.

Il est aisé de voir que la forme φ restera la même de quelque manière que p et q soient déterminés; elle serait encore la même, quand on aurait d'autres valeurs de $\alpha, \beta, \gamma, \delta$, pourvu que le diviseur commun de $\delta\gamma$ n'eût pas changé, non plus que le résidu *minimum* positif de $h\beta-g\alpha$: mais dans tout autre cas la forme φ changera. Il suit de là qu'il peut y avoir plusieurs formes $\varphi, \varphi', \varphi''$, etc. Les propositions que l'auteur démontre dans le n° suivant, sont évidentes d'après ces observations. (*Note du traducteur*).

Car

Car, 1°. il est évident que ces quatre nombres sont entiers; 2°. on s'assure aisément que la substitution est propre; 3°. il est clair (n° 159) que la forme en laquelle se change $(m; k)$, par la transformation précédente, est la même que celle en laquelle f se change par la transformation

$$m\left(\frac{\gamma}{n}\cdot\frac{\alpha g+\beta h-k}{m}+h\right)+\frac{k\gamma}{n},\quad m\left(\frac{\delta}{n}\cdot\frac{\alpha g+\beta h-k}{m}-g\right)+\frac{k\delta}{n},\ \gamma,\ \delta.$$

Or le premier de ces quatre nombres se réduit sur-le-champ à $\frac{1}{n}(\alpha\gamma g+(\beta\gamma+mn)h)$, le second à $\frac{1}{n}((\alpha\delta-mn)g+\beta\delta h)$; d'ailleurs on a $mn=e=\alpha\delta-\beta\gamma$: donc $\beta\gamma+mn=\alpha\delta$ et $\alpha\delta-mn=\beta\gamma$, ce qui donne pour les deux expressions précédentes $\frac{\alpha}{n}(\gamma g+\delta h)$, $\frac{\beta}{n}(\gamma g+\delta h)$, qui se réduisent évidemment à α, β, puisqu'on a $\gamma g+\delta h=n$. Ainsi cette transformation est α, β, γ, δ; donc $(m; k)$ se change en F, et partant $(m; k)$ et F sont proprement équivalentes, puisqu'elles ont d'ailleurs le même déterminant.

On pourra toujours juger par là si une forme f de déterminant D renferme proprement une forme de déterminant De^2; mais quand on cherche si f renferme F improprement, on doit chercher si la forme opposée à F est renfermée dans f.

214. PROBLÈME. *Étant données deux formes* f *et* F, *dont les déterminans sont respectivement* D *et* De^2, *et dont la première renferme la seconde proprement; trouver toutes les transformations propres de* f *en* F.

En représentant par Ω le même ensemble de formes qu'au numéro précédent, on en extraira toutes les formes auxquelles F est proprement équivalente. Désignons-les par φ, φ', φ'', etc.; chacune de ces formes fournira des transformations propres de f en F, en donnera de différentes, et il n'y aura aucune transformation de la forme f en F qui ne soit donnée par une des formes φ, φ', φ'', etc. Au reste, comme la méthode est la même pour toutes ces formes, nous ne nous occuperons que d'une seule.

Supposons $\varphi=(M; K)$ et $e=MN$, de manière que f se change en φ par la substitution propre, M, K, o, N. Désignons par α',

β', γ', δ^{IV} une transformation propre quelconque de φ en F, la forme f se changera évidemment en F par la substitution propre $M\alpha' + K\gamma'$, $M\beta' + K\delta^{IV}$, $N\gamma'$, $N\delta^{IV}$; et de même, toute transformation de φ en F en donnera une de f en F, et ainsi des autres: pour prouver que cette solution est complète, il reste à démontrer,

1°. Que *de cette manière on obtient toutes les transformations possibles de* f *en* F. Soit α, β, γ, δ une transformation propre quelconque de f en F, et comme au n° précédent, n le plus grand commun diviseur des nombres γ, δ, et les nombres m, g, h, k déterminés de la même manière qu'à ce numéro. Alors la forme $(m; k)$ se trouve parmi les formes φ, φ', φ'', etc.

$$\frac{\gamma}{n}\cdot\frac{\alpha g+\beta h-k}{m}+h,\ \frac{\delta}{n}\cdot\frac{\alpha g+\beta h-k}{m}-g,\ \frac{\gamma}{n},\ \frac{\delta}{n}$$

sera une transformation de cette forme en F, et de cette transformation on tire par la règle que nous venons de donner, α, β, γ, δ pour celle de f en F. Tout ceci a été démontré au n° précédent.

2°. *Toutes les transformations que l'on obtient de cette manière sont différentes.* On voit sans peine que des transformations différentes d'une même forme φ, φ', etc. en F, ne peuvent produire la même transformation de f en F. Il reste donc seulement à prouver que deux formes différentes φ et φ', par exemple, ne peuvent donner la même transformation.

Supposons que la transformation propre α, β, γ, δ de la forme f en F, s'obtienne de la transformation α', β', γ', δ' de φ en F, et de la transformation α'', β'', γ'', δ'' de φ' en F. Soit $\varphi = (m; k)$, $\varphi' = (m'; k')$, $e = mn = m'n'$. On aura les équations

$\alpha = m\alpha' + k\gamma' = m'\alpha'' + k'\gamma''$...(1), $\beta = m\beta' + k\delta^{IV} = m'\beta'' + k'\delta''$...(2),
$\gamma = n\gamma' = n'\gamma''$...(3), $\delta = n\delta' = n'\delta''$...(4), $\alpha'\delta' - \beta'\gamma' = \alpha''\delta'' - \beta''\gamma'' = 1$...(5).

Multipliant les équations (4) et (3) par α' et β' respectivement, on trouvera par la soustraction, $n = n'(\alpha'\delta'' - \beta'\gamma'')$; en les multipliant au contraire par α'' et β'' respectivement, on trouvera de même $n' = n(\alpha''\delta' - \beta''\gamma')$; donc n est divisible par n' et n' par n, ce qui exige qu'on ait $n = n'$, puisque n et n' sont supposés tous les deux positifs. Donc aussi $m = m'$, $\gamma' = \gamma''$, $\delta^{IV} = \delta''$. Or en éliminant m entre les équations (1) et (2), on trouve

$k = m'(\alpha'\beta'' - \beta'\alpha'') + k(\alpha'\delta'' - \beta'\gamma'') = m(\alpha'\beta'' - \beta'\alpha'') + k'$;

donc $k \equiv k' \pmod{m}$; ce qui ne peut avoir lieu à moins que l'on n'ait $k = k'$, puisque k et k' sont compris entre 0 et $m - 1$. Donc les formes φ et φ' sont les mêmes contre l'hypothèse.

Au reste, il est clair que si le déterminant D est négatif, ou positif et quarré, on trouvera effectivement par cette méthode, toutes les transformations propres de f en F; mais que s'il est positif et non quarré, on trouvera certaines formules générales qui contiendront toutes les transformations propres, dont le nombre est infini.

Enfin si la forme F est contenue improprement dans la forme f, on peut trouver par la même méthode toutes les transformations de f en F. Soit en effet $\alpha, \beta, \gamma, \delta$ une transformation indéterminée de f en la forme opposée à F, toutes les transformations impropres de f en F seront représentées par $\alpha, -\beta, \gamma, -\delta$.

Exemple. On demande toutes les transformations de la forme (2, 5, 7) en (275, 0, — 1), qui y est contenue des deux manières. Nous avons donné au n° précédent la suite Ω de formes pour la proposée. Examen fait, on trouve que dans cette suite les formes (5; 1) et (5; 4) sont proprement équivalentes à la forme (275,0,—1). Toutes les transformations de la forme (5; 1) = (50, 35, 19) en (275, 0, — 1) se trouvent, par la théorie que nous avons expliquée plus haut, être contenues dans la formule générale,

$$16t - 275u, \quad -t + 16u, \quad -15t + 275u, \quad t - 15u,$$

où t, u désignent les nombres entiers qui satisfont à l'équation indéterminée $t^2 - 275u^2 = 1$; ainsi toutes les transformations propres de la forme (2, 5, 7) en (275, 0, — 1) qui en résultent, seront comprises dans la formule générale

$$65t - 1100u, \quad -4t + 65u, \quad -15t + 275u, \quad t - 15u.$$

De même, toutes les transformations propres de la forme (5; 4) = (50, 65, 79) en (275, 0, — 1) sont contenues dans la formule

$$14t + 275u, \quad t + 14u, \quad -15t - 275u, \quad -t - 15u,$$

ce qui donne encore la suivante pour les transformations propres de (2, 5, 7) en (275, 0, — 1),

$$10t + 275u,\ t + 10u,\ -15t - 275u,\ -t - 15u.$$

Ainsi ces deux formules embrassent toutes les transformations propres cherchées.

On trouve de la même manière que les transformations impropres sont données par les deux formules,

$$65t - 1100u,\quad 4t - 65u,\ -15t + 275u,\ -t + 15u,$$
$$10t + 275u,\ -10 - 10u,\ -15t - 275u,\quad t + 15u,$$

215. Jusqu'à présent nous avons écarté de nos recherches les formes dont le déterminant $= 0$. Pour compléter notre théorie, il nous reste à ajouter quelque chose à leur sujet. Comme il a été démontré généralement que si une forme de déterminant D renferme une forme de déterminant D', D' étant multiple de D; il s'ensuit qu'une forme de déterminant $= 0$ ne peut renfermer aucune forme dont le déterminant ne soit aussi $= 0$. Il ne nous reste donc que deux problèmes à résoudre; savoir:

1°. *Étant données deux formes* f *et* F, *dont la seconde a* 0 *pour déterminant, découvrir si la première renferme la seconde; et dans ce cas, trouver toutes les transformations de* f en F.

2°. *Trouver toutes les représentations d'un nombre donné par une forme donnée de déterminant* $= 0$.

Le premier problème doit être traité différemment, quand le déterminant de la première forme est aussi $= 0$, et quand il ne l'est pas.

I. Observons avant tout qu'une forme $ax^2 + 2bxy + cy^2$ dont le déterminant $= 0$, peut se représenter ainsi: $m(gx + hy)^2$, g et h étant entiers et premiers entre eux, et m un nombre entier. Soit en effet m le plus grand commun diviseur des nombres a, c, en lui donnant le même signe qu'à ces nombres, qui doivent évidemment en avoir un semblable, $\frac{a}{m}$ et $\frac{c}{m}$ seront entiers, positifs et premiers entre eux; leur produit doit être égal à $\frac{b^2}{m^2}$ qui est un quarré, et partant, chacun d'eux en doit être un aussi. Soit $\frac{a}{m} = g^2$, $\frac{c}{m} = h^2$, g et h seront aussi premiers entre eux, et l'on

aura $g^2h^2 = \frac{b^2}{m^2}$, ou $gh = \pm\frac{b}{m}$. D'où il suit qu'on a

$$ax^2 + 2bxy + cy^2 = m(gx \pm hy)^2.$$

Soient proposées maintenant deux formes f et F de déterminant $= 0$, et $f = m(gx + hy)^2$, $F = M(GX + HY)^2$, dans lesquelles g est premier avec h, et G avec H. Je dis que si f renferme F, on aura $m = M$, ou que du moins m divisera M, et donnera pour quotient un quarré, et réciproquement. En effet, si f se change en F par la substitution $x = \alpha X + \beta Y$, $y = \gamma X + \delta Y$, on aura

$$\frac{M}{m}(GX + HY)^2 = \{(\alpha g + \gamma h)X + (\beta g + \delta h)Y\}^2,$$

d'où il suit évidemment que $\frac{M}{m}$ est un quarré ; faisons $\frac{M}{m} = e^2$, on aura

$$e(GX + HY) = \pm\{(\alpha g + \gamma h)X + (\beta g + \delta h)Y\};$$

et partant, $eG = \pm(\alpha g + \gamma h)$, $eH = \pm(\beta g + \delta h)$; comme G, H sont premiers entre eux, on peut déterminer deux nombres G', H', tels qu'on ait $G.G' + H.H' = 1$; et partant, $\pm e = G'(\alpha g + \gamma h) + H'(\beta g + \delta h)$, ou égal à un entier. Réciproquement, si l'on suppose que $\frac{M}{m}$ soit un quarré entier $= e^2$, la forme f renfermera la forme F, c'est-à-dire qu'on pourra toujours déterminer des valeurs entières à α, β, γ, δ, de manière à satisfaire aux équations

$$\alpha g + \gamma h = \pm eG, \quad \beta g + \delta h = \pm eH,$$

car ces équations sont toujours résolubles en nombres entiers. Il suffit, comme on sait, de résoudre l'équation $g'g + h'h = 1$, et on aura

$$\alpha = \pm eGg' + hz, \ \gamma = eGh' - gz, \ \beta = eHg' + hz', \ \delta = eHh' - gz',$$

en donnant à z, z' des valeurs entières quelconques.

Il est clair en même temps que ces formules donnent toutes les transformations de f en F, pourvu qu'on attribue à z et z' toutes les valeurs entières.

II. Supposons maintenant que tout restant le même d'ailleurs, la forme $f = ax^2 + 2bxy + cy^2$ n'ait pas o pour déterminant. Je dis que, 1°. si f renferme F, le nombre M pourra se représenter

par la forme f; 2°. si M peut être représenté par f, la forme F sera renfermée dans f; 3°. si, dans ce cas, la formule $x=\xi$, $y=\upsilon$ donne indéfiniment toutes les représentations du nombre M par la forme f; les transformations de f en F seront contenues dans la formule $G\xi$, $H\xi$, $G\upsilon$, $H\upsilon$.

Supposons que f se change en F par la substitution α, β, γ, δ; en prenant les nombres G', H', tels qu'on ait $GG'+HH'=1$; si l'on fait $x=\alpha G'+\beta H'$, $y=\gamma G'+\delta H'$, la valeur de la forme f devient M, et partant, M peut être représenté par f.

2°. Si l'on suppose $a\xi^2+2b\xi\upsilon+c\upsilon^2=M$, il est évident que par la substitution $G\xi$, $H\xi$, $G\upsilon$, $H\upsilon$, la forme f se change en F.

3°. Pour démontrer que la substitution $G\xi$, $H\xi$, $G\upsilon$, $H\upsilon$ donne toutes les transformations de f en F, si ξ, υ représentent toutes les valeurs de x, y qui rendent $f=M$; soit α, β, γ, δ une transformation quelconque de f en F, et, comme plus haut, $GG'+HH'=1$, parmi les valeurs de x, y seront les suivantes: $x=\alpha G'+\beta H'$, $y=\gamma G'+\delta H'$, qui donneront la substitution

$$G(\alpha G'+\beta H'),\ H(\alpha G'+\beta H'),\ G(\gamma G'+\delta H'),\ H(\gamma G'+\delta H'),$$

d'où l'on tire

$$\alpha+H'(BG-\alpha H),\ \beta+G'(\alpha H-\beta G),\ \gamma+H'(\delta G-\gamma H),\ \delta+G'(\gamma H-\delta G):$$

mais comme on a

$$a(\alpha X+\beta Y)^2+2b(\alpha X+\beta\gamma)(\gamma X+\delta Y)+c(\gamma X+\delta Y)^2=M(GX+HY)^2;$$

on en tire au moyen des trois équations qui en dérivent,

$$M(\beta G-\alpha H)^2=c(\alpha\delta-\beta\gamma)^2,\quad M(\delta G-\gamma H)^2=a(\alpha\delta-\beta\gamma)^2.$$

Or $\alpha\delta-\beta\gamma=0$, puisque le déterminant de F qui est $=0$, est égal au produit de $\alpha\delta-\beta\gamma$ par le déterminant de f qui n'est pas égal à zéro; on a donc $\beta G-\alpha H=0$, et partant, la substitution en question se réduit à α, β, γ, δ. Ainsi la formule que nous avons donnée fournit toutes les transformations de f en F (*).

(*) On pourrait encore présenter ces différentes propositions de la manière uivante.

Si la forme f se change en F par la substitution α, β, γ, δ, on aura les

III. Il ne reste plus qu'à faire voir comment on peut trouver toutes les représentations d'un nombre donné par une forme donnée dont le déterminant $= 0$. Soit cette forme $m(gx + hy)^2$, il suit de là que ce nombre doit être divisible par M, et que le quotient doit être un quarré. Ainsi, en représentant ce nombre par me^2, on aura à trouver les valeurs de x, y pour qu'on ait $(gx+hy)^2 = e^2$, ou ce qui revient au même, $gx + hy = \pm e$. Or cette équation est toujours résoluble en nombres entiers, puisque g et h sont premiers entre eux. On déterminera g' et h' de manière qu'on ait $gg' + hh' = 1$, et l'on aura $x = \pm g'e + hz$, $y = \pm h'e - gz$, où z est un nombre entier quelconque.

Comme application des recherches précédentes, nous ajouterons le problème suivant.

216. PROBLÈME. *Trouver toutes les solutions en nombres entiers, de l'équation générale du second degré à deux inconnues,*

$$ax^2 + 2bxy + cy^2 + 2dx + 2ey + f = 0, \quad (*)$$

équations

$a\alpha^2 + 2b\alpha\gamma + c\gamma^2 = MG^2$, $a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta = MGH$, $a\beta^2 + 2b\beta\delta + c\delta^2 = MH^2$;

on aura encore $\alpha\delta - \beta\gamma = 0$, ou $\frac{\alpha}{\beta} = \frac{\gamma}{\delta}$.

Si de la première, multipliée par δ, on retranche la seconde, multipliée par γ, on en déduit sur-le-champ $G\delta - H\gamma = 0$, ou $\frac{\gamma}{\delta} = \frac{G}{H}$, et puisqu'on a $\frac{\alpha}{\beta} = \frac{\gamma}{\delta}$; $\frac{\alpha}{\beta} = \frac{G}{H}$; G et H sont premiers entre eux, donc γ et α sont divisibles par G, et δ et β par H; desorte que l'on aura $\alpha = \xi G$, $\beta = \xi H$, $\gamma = \upsilon G$, $\delta = \upsilon H$, ξ et υ étant des indéterminées. Or ces valeurs, substituées dans les trois équations, réduisent chacune d'elles à

$$a\xi^2 + 2b\xi\upsilon + c\upsilon^2 = M.$$

Donc nous prouvons à-la-fois, 1°. que M doit être représentable par la forme (a, b, c); 2°. que s'il est représentable, la transformation de f en F est possible; 3°. qu'elle se fait par la substitution ξG, ξH, υG, υH, et en même temps qu'on obtiendra ainsi toutes les transformations. (*Note du traducteur*).

(*) Si l'on proposait une équation dans laquelle le 2e, le 4e et le 5e coefficiens ne fussent pas pairs, cette équation, multipliée par 2, prendrait la forme que nous lui supposons.

ou a, b, c, *etc. sont des nombres entiers quelconques.*

Si l'on introduit à la place des inconnues x, y, d'autres inconnues

$$p=(b^2-ac)x+be-cd, \quad q=(b^2-ac)y+bd-ae,$$

qui seront évidemment entiers quand x, y le seront, on aura l'équation

$$ap^2+2bpq+cq^2+(b^2-ac)(ae^2-2bed+cd^2)+f(b^2-ac)^2=0,$$

ou, en faisant pour abréger $(b^2-ac)(ae^2-2bde+cd^2)+f(b^2-ac)^2=-M$,

$$ap^2+2bpq+cq^2=M.$$

Or nous avons donné la manière de trouver toutes les solutions de cette équation, c'est-à-dire, toutes les représentations du nombre M par la forme (a, b, c); mais on a par les relations entre p, q, x et y,

$$x=\frac{p+cd-be}{b^2-ac}, \quad y=\frac{q+ae-bd}{b^2-ac}.$$

Si donc on rejette de toutes les valeurs qui en résultent pour x et y, celles qui sont fractionnaires, il ne restera que les solutions cherchées.

A l'égard de cette solution, il y a plusieurs observations à faire.

1°. Si M ne peut être représenté par la forme (a, b, c), ou si aucune représentation ne fournit de valeurs entières pour x, y; l'équation n'est pas résoluble.

2°. Quand le déterminant b^2-ac de la forme (a, b, c) est négatif ou positif quarré, et qu'on a en même temps $\pm M>0$, les représentations du nombre M par la forme (a, b, c) sont limitées, et parconséquent aussi les solutions de l'équation proposée, s'il en existe.

3°. Quand b^2-ac est positif non quarré, ou qu'il est quarré, et qu'on a en même temps $M=0$, si le nombre M peut être représenté par la forme (a, b, c), le nombre des représentations sera infini. Mais comme il est impossible de trouver alors toutes ces

ces représentations, et partant, d'essayer si elles donnent pour x, y des valeurs fractionnaires ou entières, il est nécessaire d'établir une règle par laquelle on puisse s'assurer, quand cela arrive, qu'il n'y a aucune représentation qui donne des valeurs entières pour x, y; car, sans cette règle, quel que fût le nombre des représentations essayées, on n'arriverait jamais à la certitude, et quand une partie des représentations donne des valeurs entières, et l'autre des valeurs fractionnaires, il faudra savoir distinguer les premières représentations des dernières.

4°. Quand $b^2 - ac = 0$, les formules précédentes ne déterminent pas les valeurs de x, y. Ainsi, dans ce cas, il faudra avoir recours à une méthode particulière.

217. Dans le cas où $b^2 - ac$ est un nombre positif non quarré, nous avons fait voir plus haut que toutes les représentations du nombre M par la forme (a, b, c), s'il y en a quelques-unes, peuvent être données par une ou plusieurs formules telles que

$$p = \frac{1}{m}(At + Bu), \quad q = \frac{1}{m}(Ct + Du);$$

A, B, C, D étant des nombres entiers donnés, m le plus grand diviseur commun des nombres $a, 2b, c$; enfin t, u des nombres entiers qui satisfont à l'équation $t^2 - (b^2 - ac)u^2 = m^2$. Comme les valeurs de t, u peuvent être prises positivement et négativement, au lieu des formules précédentes, on peut prendre les quatre suivantes:

$$p = \frac{1}{m}(At + Bu), \quad q = \frac{1}{m}(Ct + Du); \quad p = \frac{1}{m}At - Bu), \quad q = \frac{1}{m}(Ct - Du);$$

$$p = \frac{1}{m}(-At + Bu), \quad q = \frac{1}{m}(-Ct + Bu); \quad p = -\frac{1}{m}(At + Bu), \quad q = -\frac{1}{m}(Ct + Du).$$

ensorte que le nombre de toutes les formules soit quatre fois plus grand qu'auparavant, mais que u et t soient positifs; examinons donc séparément chacune de ces formules, et cherchons quelles sont les valeurs de t, u qui donnent des valeurs entières pour x, y.

La formule

$$p = \frac{1}{m}(At + Bu), \quad q = \frac{1}{m}(Ct + Du) \ldots\ldots (1)$$

donne pour x et y

$$x = \frac{At + Bu + mcd - mbe}{m(b^2 - ac)}, \quad y = \frac{Ct + Du + mae - mbd}{m(b^2 - ae)}.$$

Or nous avons fait voir plus haut que toutes les valeurs positives de t forment une suite récurrente t, t', t'', etc., et que les valeurs correspondantes de u en forment une autre u, u', u'', etc.; qu'en outre on pouvait toujours trouver un nombre μ tel qu'on eût, suivant un module donné quelconque,

$$t^{\mu} \equiv t^0,\ t^{\mu+1} \equiv t',\ t^{\mu+2} \equiv t'',\ \text{etc.},\ u^{\mu} \equiv u^0,\ u^{\mu+1} \equiv u',\ u^{\mu+2} \equiv u'',\ \text{etc.}$$

Prenons pour ce module le nombre $m(b^2 - ac)$, et désignons par x^0, y^0 les valeurs qui résultent pour x, y de la substitution de t^0, u^0; par x', y' celles qui résultent de t', u', etc. On voit alors sans peine que si $x^{(h)}$, $y^{(h)}$ sont des nombres entiers, et que μ soit convenablement déterminé, les valeurs $x^{h+\mu}$, $y^{h+\mu}$; $x^{h+2\mu}$, $y^{h+2\mu}$, etc.; $x^{h+k\mu}$, $y^{h+k\mu}$ seront des nombres entiers, et qu'au contraire si x^h ou y^h est fractionnaire $x^{h+k\mu}$, ou $y^{h+k\mu}$ le sera aussi. Il suit de là que si l'on cherche les valeurs de x, y depuis x^0, y^0 jusqu'à $x^{\mu-1}$, $y^{\mu-1}$, et qu'aucunes d'elles ne soient entières, la formule (1) ne donnera absolument aucunes valeurs entières pour x, y. Mais si l'on en trouve quelques-unes, par exemple, x^{ν}, y^{ν}, $x^{\nu'}$, $y^{\nu'}$, etc., toutes les valeurs entières données par la formule (1) seront celles de x, y, dont les accens seront $\nu + k\mu$, $\nu' + k\mu$, etc., k désignant tous les nombres entiers positifs, y compris zéro.

Les autres formules dans lesquelles sont contenues les valeurs de p, q doivent être traitées absolument de la même manière, et s'il arrivait que d'aucune d'elles on n'obtînt des valeurs entières pour x, y, l'équation proposée ne serait pas résoluble en nombres entiers; mais toutes les fois qu'elle le sera, les solutions entières pourront s'obtenir par ce que nous venons d'exposer.

218. Quand $b^2 - ac$ est un quarré et qu'on a $M = 0$, toutes les valeurs de p, q sont comprises sous deux formules de cette forme

$$p = Az, \quad q = Bz; \quad p = A'z, \quad q = B'z$$

où z est un nombre entier quelconque, A, B, A', B', des nombres

entiers premiers entre eux; c'est-à-dire A avec B, A' avec B' (n° 212). Il en résulte

$$x=\frac{Az+cd-be}{b^2-ac},\quad y=\frac{Bz+ae-bd}{b^2-ac}\ldots\ldots(1),$$
$$x=\frac{A'z+cd-be}{b^2-ac},\quad y=\frac{B'z+ae-bd}{b^2-ac}\ldots\ldots(2).$$

Mais comme ces formules peuvent conduire à des valeurs fractionnaires pour x, y, à moins que l'on n'ait $b^2-ac=1$; il sera utile de distinguer les valeurs de z qui rendent x et y entiers dans chaque formule; d'ailleurs il suffira de considérer la première, parceque la même méthode s'appliquera à la seconde.

Puisque A et B sont premiers entre eux, on peut déterminer deux nombres A_1, B_1, tels qu'on ait $AA_1+BB_1=1$; substituant A et B leurs valeurs tirées de la formule (1), on a

$$(A_1x+B_1y)(b^2-ac)=z+A_1(cd-be)+B_1(ae-bd);$$

d'où il suit que les valeurs de z qui rendront x, y entiers, doivent être congrues à $A_1(be-cd)+B_1(bd-ae)$, suivant le module b^2-ac, ou être contenues sous la formule $(b^2-ac)z'+A_1(be-cd)+B_1(bd-ce)$, z' étant un nombre entier quelconque. On obtient facilement par là, au lieu de la formule (1), la formule suivante:

$$x=Az'+B_1.\frac{A(bd-ae)-B(be-cd)}{b^2-ac},\quad y=Bz'-A_1.\frac{A(bd-ae)-B(be-cd)}{b^2-ac},$$

qui donnera évidemment des valeurs entières pour toutes les valeurs de z', si elle en donne pour une seule. Or il suffit pour cela, qu'on ait $A(bd-ae)\equiv B(be-ad)$ (mod. b^2-ac). Si cette congruence n'a pas lieu, la formule (1) ne donnera pas de valeurs entières. On traitera de même la formule (2).

219. Quand $b^2-ac=0$, la forme $ax^2+2bxy+cy^2$ peut se changer en $m(\alpha x+\beta y)^2$, où m, α, β sont des entiers (n° 215). Soit fait $\alpha x+\beta y=z$, l'équation proposée devient

$$mz^2+2dx+2ey+f=0;$$

éliminant entre cette équation et l'équation $\alpha x+\beta y=z$, on a

$$x=\frac{\beta mz^2+2ez+\beta f}{2(\alpha e-\beta d)},\quad y=\frac{\alpha mz^2+2dz+\alpha f}{2(\beta d-\alpha e)}.$$

Or il est clair que ces valeurs satisferont à l'équation, en donnant

à z une valeur quelconque, à moins qu'on n'ait $\alpha e = \beta\delta$, cas que nous considérerons tout-à-l'heure à part; il ne reste donc qu'à faire voir quelles doivent être les valeurs de z, pour qu'il en résulte des valeurs entières de x et de y.

Comme $\alpha x + \beta y = z$, on ne peut prendre pour z que des nombres entiers; en outre, il est évident que si une valeur de z rend x et y entiers, la même chose aura lieu pour toutes les valeurs de z congrues à celle-là, suivant le module $2(\alpha e - \beta d)$. Si donc on substitue pour z tous les nombres entiers depuis 0 jusqu'à $\pm 2(\alpha e - \beta d) - 1$, suivant que $\alpha e - \beta d$ sera positif ou négatif, et qu'aucune de ces substitutions ne rende x et y entiers, l'équation proposée ne sera pas résoluble en nombres entiers; mais si quelques-unes de ces valeurs ont cette propriété, supposons que ce soient les valeurs ζ, ζ', ζ'', etc., on aura toutes les solutions, en prenant $z = 2(\alpha e - \beta d)k + \zeta$, $z = 2(\alpha e - \beta d)k + \zeta'$, etc., k étant un entier quelconque. Les valeurs de z, ζ, ζ', etc. peuvent aussi par la solution se trouver des congruences du second degré. (Voyez Section IV.)

220. Pour le cas où $\alpha e = \beta d$, il faut chercher une méthode particulière. Par le n° 215, α et β sont premiers entre eux; ainsi $\frac{d}{\alpha} = \frac{e}{\beta}$ sera un nombre entier que nous nommerons h. Alors l'équation proposée prend la forme

$$(m\alpha x + m\beta y + h)^2 - h^2 + mf = 0,$$

et partant ne peut avoir de solutions rationnelles, à moins que $h^2 mf$ ne soit un quarré. Soit donc $h^2 - mf = k^2$, on tire de l'équation précédente

$$m\alpha x + m\beta y + h \pm k = 0.$$

Cette équation exige, pour être résoluble en nombres entiers, que $h \pm k$ soit divisible par m; car d'ailleurs α, β étant premiers entre eux, on trouvera toutes les solutions par les règles connues.

221. Eclaircissons par un exemple le cas du n° 217, qui est le plus difficile. Soit l'équation

$$x^2 + 8xy + y^2 + 2x - 4y + 1 = 0.$$

En introduisant de nouvelles indéterminées $p = 15x - 9$,

$q = 15y + 6$, on en tire l'équation $p^2 + 8pq + q^2 = -540$. Or on trouve que toutes les solutions de cette équation sont renfermées dans les quatre formules

$$p = 6t,\quad q = -24t - 90u;\quad p = 6t,\quad q = -24t + 90u,$$
$$p = -6t,\quad q = 24t - 90u;\quad p = -6t,\quad q = 24t + 90u,$$

t, u étant des nombres indéterminés qui doivent satisfaire à l'équation $t^2 - 15u^2 = 1$, et qui sont donnés par la formule

$$t = \frac{1}{2}\{(4+\sqrt{15})^n + (4-\sqrt{15})^n\},\quad u = \frac{1}{2\sqrt{15}}\{(4+\sqrt{15})^n - (4-\sqrt{15})^n\},\ (\text{n}^\circ 200).$$

Ainsi toutes les valeurs de x, y seront contenues dans les formules

$$x = \tfrac{1}{5}(2t + 3),\ y = -\tfrac{1}{5}(8t + 3ou + 2);\quad x = \tfrac{1}{5}(2t + 3),\ y = -\tfrac{1}{5}(8t - 3ou + 2)$$
$$x = \tfrac{1}{5}(-2t + 3),\ y = \tfrac{1}{5}(8t - 3ou - 2);\quad x = \tfrac{1}{5}(-2t + 3),\ y = \tfrac{1}{5}(8t + 3ou - 2).$$

En appliquant convenablement ce que nous avons dit plus haut, on trouvera que pour avoir des nombres entiers il faut prendre pour t, u, dans la première et la seconde formule, les valeurs qui résultent en supposant x pair, et au contraire, dans la troisième et la quatrième, celles qui résultent en le supposant impair. Les solutions les plus simples sont $x = 1, -1, -1$; $y = 2, 0, 12$, respectivement.

Au reste, nous ferons remarquer que la solution du problème précédent peut le plus souvent s'abréger par un grand nombre d'artifices, surtout quand on en vient à l'exclusion des valeurs entières; mais nous sommes obligés de ne pas nous y arrêter pour éviter les longueurs.

222. Comme beaucoup des choses que nous avons traitées jusqu'ici l'ont été aussi par d'autres géomètres, nous ne pouvons passer sous silence leurs travaux. Lagrange a fait des Recherches générales sur l'*équivalence des formes* (*nouv. Mém. de l'Acad. de Berlin*, 1773, *p.* 263, *et* 1775, *p.* 323), où il prouve surtout que, pour un déterminant donné quelconque, on peut trouver un nombre fini de formes telles, que toute forme de même déterminant soit équivalente à une d'entre elles, et que partant, toutes les formes d'un déterminant donné peuvent se distribuer par classes. Ensuite Legendre a découvert plusieurs propriétés élégantes de cette classification, mais pour la plus grande partie par induction,

et nous les donnerons plus bas avec les démonstrations. Au reste, personne n'avait encore songé à faire la distinction de l'équivalence *propre* et *impropre*, dont l'usage est sensible dans les recherches délicates.

Le fameux problème du n° 216 a été résolu complètement, pour la première fois, par Lagrange (*Hist. de l'Acad. de Berlin*, 1767, *p.* 165, *et* 1768, *p.* 181). Sa solution existe aussi, mais moins complète, dans les *Supplémens à l'Algèbre d'Euler*. Euler lui-même avait auparavant attaqué le même sujet (*Comm. Petr. T. VI*, *p.* 175; *Comm. nov. T. IX*, *p.* 3; *ibid. T. XVIII*, *p.* 185); mais il a toujours borné sa recherche à déduire toutes les solutions d'une seule qu'il suppose connue; et d'ailleurs ses méthodes ne donnent toutes les solutions que dans un petit nombre de cas. Bien que le dernier de ces trois mémoires soit postérieur à celui dans lequel est renfermée la solution de Lagrange qui embrasse le problème dans toute sa généralité, et à cet égard ne laisse rien à desirer; il paraît cependant qu'Euler à cette époque ne la connaissait pas encore. Au reste, notre solution, ainsi que tout ce qui a été donné dans cette section, est fondée sur des principes tout-à-fait différens.

Ce que d'autres, tels que Diophante, Fermat, etc. ont fait connaître à ce sujet, n'appartient qu'à des cas très-particuliers; aussi, comme nous avons rappelé en temps et lieu ce qui était le plus digne de mémoire, nous ne nous arrêtons pas à parler de chaque chose en particulier.

Ce que nous avons dit jusqu'à présent sur les formes du second degré, ne doit être regardé que comme les premiers élémens de cette théorie. Nous avons vu le champ s'agrandir considérablement, en poursuivant nos recherches avec persévérance; nous donnons dans ce qui va suivre les choses qui nous ont paru les plus dignes d'attention. Car la fertilité de ce sujet est telle, que nous sommes forcés pour abréger, de passer sous silence une grande partie de ce que nous avons pu découvrir; et une plus grande partie sans doute est encore cachée et attend de nouveaux efforts. Nous prévenons que les formes dont le déterminant $= 0$ sont exclues

de nos Recherches, à moins que nous n'avertissions spécialement du contraire.

223. Nous avons déjà fait voir plus haut, (nos 175, 195, 211), qu'étant donné un nombre entier quelconque D, on pouvait assigner une suite de formes F, F', F'', etc. de déterminant D, telles que toute forme de déterminant D soit proprement équivalente à l'une d'elles, et à une seule. Ainsi toutes les formes de déterminant donné D, dont le nombre est infini, peuvent se classer d'après ces formes, en composant la première classe de toutes les formes équivalentes à F, la seconde, de toutes les formes équivalentes à F', etc.

On pourra choisir dans chaque classe de formes de déterminant D, une d'entre elles que l'on considérera comme *forme représentante* de toute la classe. Il est indifférent en soi quelle forme on prend dans chaque classe, cependant on doit toujours préférer celle qui est plus simple que toutes les autres. Or la simplicité d'une forme (a, b, c) dépend évidemment de la grandeur des nombres a, b, c; et on dira à juste titre que la forme (a, b, c) est plus simple que la forme (a', b', c'), si l'on a $a < a'$, $b < b'$, $c < c'$. Mais il reste encore à savoir laquelle, par exemple, nous choisirions des deux formes $(17, 0, -45)$, $(5, 0, -153)$. Le plus souvent il sera avantageux d'observer la règle suivante :

I. Quand D est négatif, on prendra les formes réduites pour formes représentatives dans chaque classe; mais s'il y a deux formes réduites dans la même classe, elles seront opposées (n° 172), et l'on prendra celle où le terme du milieu sera positif.

II. Quand D sera positif non quarré, on formera la période d'une forme réduite contenue dans la classe proposée; cette période renfermera deux formes ambiguës, ou n'en renfermera aucune (n° 187).

1°. Dans le premier cas, soient (A, B, C), $(A', B' C')$ ces formes ambiguës; M, M' les résidus *minima* des nombres B, B', suivant les modules A, A', résidus qu'on prendra positivement s'ils ne sont $= 0$; enfin $N = \frac{D - M^2}{A}$, $N' = \frac{D - M'^2}{A'}$. Cela posé, on choisira celle des deux formes $(A, M, -N)$, $(A', M', -N')$,

qui paraîtra la plus simple pour forme représentante. Dans ce choix, on préférera la forme dont le terme du milieu $= 0$; mais quand cela arrive dans les deux formes, ou que cela n'arrive dans aucune, on doit choisir celle dans laquelle le premier terme est le plus petit, et quand il y a égalité au signe près, celle où le premier terme est positif.

2°. Dans le second cas, on choisira dans toute la période la forme dont le premier terme est le plus petit, abstraction faite du signe, de manière cependant que si dans la même période deux formes avaient le premier terme au signe près, on préférerait celle où il est positif. Soit (A, B, C) cette forme, on en déduira, comme dans le cas précédent, une autre forme $(A, M, -N)$ (en prenant pour M le résidu *minimum* absolu de B, suivant le module A, et en faisant $N = \frac{D - M^2}{A}$), et on la choisira pour représentante.

S'il arrivait que plusieurs formes de la période eussent le même plus petit premier terme, on les traiterait toutes comme il vient d'être prescrit, et parmi les formes qui en résulteraient, on prendrait pour représentante celle dans laquelle le terme du milieu serait le plus petit.

Ainsi, par exemple, pour $D = 305$, on a entr'autres la période

$(17, 4, -17)$, $(-17, 13, 8)$, $(8, 11, -23)$, $(-23, 12, 7)$,
$(7, 16, -7)$, $(-7, 12, 23)$, $(23, 11, -8)$, $(-8, 13, 17)$,

dans laquelle on choisit d'abord la forme $(7, 16, -7)$, d'où l'on tire ensuite la forme représentante $(7, 2, -43)$.

III. Quand le déterminant sera un nombre quarré $= K^2$, on cherchera une forme réduite $(A, K, 0)$ contenue dans la classe proposée; et si $A < K$ ou $= K$, on la prendra pour la forme représentante; mais si $A > K$, on prendra à sa place la forme $(A, -2K, K, 0)$ dont le premier membre sera négatif, mais $< K$.

Exemple. De cette manière, on distribuera en 16 classes toutes les formes de déterminant -235, classes dont les formes représentantes seront

$(1, 0, 235)$, $(2, 1, 118)$, $(4, 1, 59)$, $(4, -1, 59)$,
$(5, 0, 47)$, $(10, 5, 26)$, $(13, 5, 20)$, $(13, -5, 20)$,

et

et huit autres qui ne diffèrent des précédentes que par le signe des termes extrêmes : $(-1, 0, -235)$, $(-2, 1, -118)$, etc.

Toutes les formes de déterminant 79 se distribuent en six classes dont les représentantes sont

$$(1, 0, -79),\ (-1, 0, 79),\ (3, -1, -26),$$
$$(-3, -1, 26),\ (-3, 1, 26),\ (3, 1, -26),$$

224. Par cette classification, on sépare des autres toutes les formes qui sont proprement équivalentes; ainsi deux formes de la même classe sont proprement équivalentes; tout nombre qui peut être représenté par l'une d'elles, peut l'être par l'autre; et si un nombre M peut être représenté par la première en donnant des valeurs premières aux indéterminées, il pourra être représenté par la seconde de la même manière, desorte même que les deux représentations appartiennent à la même valeur de l'expression $\sqrt{D}$ (mod. M). Mais deux formes qui appartiennent à des classes différentes, ne pourront être proprement équivalentes, et l'on ne peut pas conclure de ce qu'un nombre est représentable par l'une d'elles, qu'il le soit par l'autre; au contraire, nous sommes en droit d'affirmer que si un nombre M peut se représenter par la première, en donnant à x, y des valeurs premières entre elles, on ne pourra pas trouver de représentations de ce nombre par l'autre forme, appartenant à la même valeur de l'expression $\sqrt{D}$ (mod. M), (nos 167, 168).

Au contraire, comme il peut arriver que deux formes F, F', prises dans deux classes différentes K, K', soient improprement équivalentes, auquel cas toute forme de la première classe sera improprement équivalente à toute forme de la deuxième; chaque forme de K aura son opposée dans K', et les classes K, K', seront dites *opposées*. Ainsi, dans le premier exemple de l'article précédent, la troisième classe des formes de déterminant -235 est opposée à la quatrième, et la septième à la huitième; dans le second exemple, la troisième l'est à la sixième, et la quatrième à la cinquième. Etant donc proposées deux formes prises dans des classes opposées, tout nombre qui pourra être représenté par l'une d'elles, pourra l'être aussi par l'autre. Si pour l'une la représentation a lieu par des valeurs premières, il en sera de même pour l'autre, de manière

cependant, que les représentations appartiendront à des valeurs opposées de l'expression $\sqrt{D}$ (mod. M). Au reste, les règles que nous avons données pour le choix des formes représentantes, sont établies de manière que les classes opposées obtiennent des représentantes opposées.

Enfin, il y a aussi des classes qui sont elles-mêmes leurs opposées; savoir, si une forme et son opposée sont contenues dans la même classe, on voit facilement que toutes les formes de cette classe sont équivalentes entre elles, tant proprement qu'improprement, et qu'elles ont toujours leurs opposées dans la même classe. Toute classe jouira de cette propriété, lorsqu'elle contiendra une forme ambiguë, et réciproquement on trouvera une forme ambiguë dans toute classe qui est elle-même son opposée (nos 163, 165); aussi cette classe s'appellera *ambiguë*. Ainsi, parmi les classes de déterminant —235, on trouve huit ambiguës, dont les représentantes sont :

(1, 0, 235), (2, 1, 118), (5, 0, 47), (10, 5, 26), (—1, 0, —235), (—2, 1, —118), (—5, 0, —47), (—10, 5, —26).

Parmi les classes de déterminant 79, il y en a deux: (1, 0, —79), (—1, 0, 79).

Au reste, si l'on détermine les formes représentantes d'après les règles que nous avons données, on trouvera sans peine les classes ambiguës; pour le déterminant positif non quarré, on trouvera nécessairement des représentantes ambiguës pour des classes qui le sont (n° 194); pour le déterminant négatif, la forme représentante d'une classe ambiguë sera elle-même ambiguë, ou bien ses termes extrêmes seront égaux (n° 172). Enfin, pour les formes de déterminant positif quarré, il est aisé de juger (n° 210) si la forme représentante est improprement équivalente à elle-même, et partant, si la classe est ambiguë.

225. Nous avons déjà fait voir plus haut (n° 175) que dans une forme (a, b, c) de déterminant négatif, les termes extrêmes doivent avoir le même signe, non-seulement entre eux, mais encore, que les termes extrêmes de toute autre forme qui lui est équivalente. Si a, c sont positifs, nous appellerons *positive* la forme (a, b, c), et la classe qui la renferme, et qui ne contiendra que des formes

positives, s'appellera *classe positive*. Au contraire, si a, c sont négatifs, (a, b, c) sera une forme négative, et elle sera contenue dans une classe négative. Les nombres négatifs ne peuvent être représentés par une forme positive, ni les nombres positifs par une forme négative. Si (a, b, c) est la représentante d'une certaine classe, la forme $(-a, b, -c)$ sera celle de la classe négative, et il suit de là qu'il y a autant de classes positives que de négatives, et que les dernières seront déterminées, lorsque les premières le seront. Ainsi, dans les recherches sur les formes de déterminant négatif, il suffit le plus souvent de considérer les classes positives, puisque leurs propriétés se rapportent facilement aux classes négatives.

Au reste, cette distinction n'a lieu que pour les formes de déterminant négatif; les nombres positifs et négatifs peuvent être représentés également par des formes quelconques de déterminant positif, ensorte qu'il n'est pas rare que les deux formes (a, b, c), $(-a, b, -c)$ doivent être rapportées à la même classe.

226. Nous appelons *forme primitive* une forme quelconque (a, b, c), lorsque les nombres a, b, c n'ont pas de diviseur commun, autrement elle s'appellera *dérivée*, de manière que la forme (a, b, c) sera dite *dérivée de la forme primitive* $\left(\frac{a}{m}, \frac{b}{m}, \frac{c}{m}\right)$, si m est le plus grand commun diviseur des nombres a, b, c. Il suit de là que toute forme sera primitive, si son déterminant n'est divisible par aucun quarré (1 excepté). Or, par le n° 161, il est clair que s'il y a une forme primitive dans une classe donnée, toutes les formes de cette classe le seront également, et on l'appellera *classe primitive*. Il est d'ailleurs évident que si une forme F de déterminant D est dérivée d'une forme primitive f de déterminant $\frac{D}{m^2}$, et que K et k soient respectivement les classes qui renferment les formes F, f, toutes les formes de K seront dérivées de la classe k; ainsi la classe K sera dite *dérivée de la classe primitive* k.

Si (a, b, c) est une forme primitive, et que a, c ne soient pas tous les deux pairs, on voit facilement que a, $2b$, c n'auront pas non plus de diviseur commun. Dans ce cas, la forme (a, b, c) sera

dite *proprement primitive*, ou plus simplement *forme propre*; mais si a, c sont pairs, les nombres a, $2b$, c auront 2 pour commun et même pour plus grand commun diviseur; alors la forme (a, b, c) sera *improprement primitive*, ou plus simplement *impropre* (*). Dans ce cas, b sera nécessairement impair, car autrement la forme (a, b, c) ne serait pas primitive; ainsi l'on aura $b^2 \equiv 1 \pmod 4$, et partant, puisque ac est divisible par 4, $b^2 - ac \equiv 1 \pmod 4$: les formes impropres auront donc des déterminans de la forme $4n+1$ ou $-(4n+3)$, suivant qu'ils seront positifs ou négatifs. Mais, par le n° 161, il est clair que s'il y a dans une classe une forme proprement primitive, toutes les autres le seront, et que de même, une classe qui renferme une forme improprement primitive, n'en renfermera que de cette espèce. Ainsi nous appellerons cette classe, dans le premier cas, *proprement primitive* ou *propre*, et dans le second cas; *improprement primitive* ou *impropre*. Par exemple, parmi les classes positives de déterminant -235, il y en a six propres, savoir, celles dont les représentantes sont :

$(1, 0, 235)$, $(4, 1, 59)$, $(4, -1, 59)$, $(5, 0, 47)$, $(13, 5, 20)$, $(13, -5, 20)$,

et autant parmi les classes négatives; il y en a deux impropres de chaque espèce. Quant aux classes de déterminant 79, elles sont toutes propres, puisque 79 est de la forme $4n+3$.

Si la forme (a, b, c) est dérivée de la forme primitive $\left(\frac{a}{m}, \frac{b}{m}, \frac{c}{m}\right)$; cette dernière peut être propre ou impropre. Dans le premier cas m, dans le second $2m$, sera le plus grand commun diviseur des nombres a, $2b$, c, ce qui fait entendre la distinction entre *une forme dérivée d'une forme proprement primitive*, et une *forme dérivée d'une forme improprement primitive*, et partant (n° 161) entre une *classe dérivée d'une classe proprement primitive*, et une *classe dérivée d'une classe improprement primitive*.

(*) Nous ne nous sommes servis de ces termes de propre et d'impropre qu'à défaut d'autres plus convenables, car ils n'ont aucun rapport avec ceux que nous avons employés depuis le n° 157. Au reste, il n'y a pas à craindre qu'on puisse les confondre.

Par cette distinction nous avons trouvé le principe qui nous servira à distribuer par *ordres* toutes les classes de formes de déterminant donné.

Nous rangerons dans le *même ordre* les deux formes (a, b, c), (a', b', c'), si l'on a à-la-fois le même plus grand diviseur commun pour a, b, c; a', b', c', pour $a, 2b, c$ et $a', 2b', c'$; mais si l'une ou l'autre de ces conditions n'a pas lieu, les classes se rapporteront à des *ordres différens*. Il suit de là immédiatement, que les classes proprement primitives composent un ordre, et toutes les classes improprement primitives, un autre. Si m^2 est le quarré qui divise le déterminant D, les classes dérivées des classes proprement primitives de déterminant D composeront un ordre particulier, et les classes dérivées des classes improprement primitives de déterminant $\frac{D}{m^2}$ en composeront un autre. Si par hasard D n'est divisible par aucun quarré (excepté 1), il n'y aura pas d'ordres de classes dérivées, et partant il n'y aura qu'un ordre, lorsque $D \equiv 2$ ou $3 \pmod 4$, celui des classes proprement primitives, ou deux, lorsque $D \equiv 1 \pmod 4$, celui des classes proprement primitives, et celui des classes improprement primitives.

On déduit sans peine la règle suivante par le calcul des combinaisons (n° 17). En supposant $D = D' . 2^{2\mu} . a^{2\alpha} . b^{2\beta} . c^{2\gamma}$, etc., desorte que D' ne renferme aucun facteur quarré, le nombre des ordres sera $(\mu+1)(\alpha+1)(\beta+1)(\gamma+1)\ldots$ si $D' \equiv 2$ ou $\equiv 3 \pmod 4$; ou $(\mu+2)(\alpha+1)(\beta+1)(\gamma+1)\ldots$ si $D' \equiv 1 \pmod 4$.

Exemple Ier. Si $D = 45 = 5 . 3^2$, on aura six classes dont les représentantes sont:

$(1, 0, -45)$, $(-1, 0, 45)$, $(2, 1, -22)$, $(-2, 1, 22)$, $(3, 0, -15)$, $(6, 3, -6)$,

et elles peuvent se distribuer en quatre ordres,

1°. $(1, 0, -45)$, $(-1, 0, 45)$, propres; 2°. $(2, 1, -22)$, $(-2, 1, 22)$, impropres; 3°. la classe $(3, 0, -15)$ dérivée d'une classe propre de déterminant 5; 4°. la classe $(6, 3, -6)$ dérivée d'une classe impropre de déterminant 5.

Exemple II. Les classes positives de déterminant $-99 = -11 . 3^2$

peuvent se distribuer en quatre ordres, en désignant les classes par leurs représentantes.

Le premier contient les classes propres suivantes :

(1, 0, 99), (4, 1, 25), (4, —1, 25), (5, 1, 20), (5, —1, 20), (9, 0, 11);

Le deuxième, les classes impropres: (2, 1, 50), (10, 1, 10);

Le troisième, les classes dérivées de classes propres de déterminant — 11: (3, 0, 33), (9, 3, 12), (9, —3, 12);

Le quatrième, une classe dérivée d'une impropre de déterminant — 11: (6, 3, 18).

On distribuera par ordre, de la même manière, les classes négatives de même déterminant.

On voit sans peine que les classes opposées se rapportent au même ordre.

227. Parmi tous les ordres, celui des classes proprement primitives mérite la plus grande attention; car toutes les classes dérivées tirent leur origine de certaines classes primitives de déterminant moindre, de la considération desquelles suit le plus souvent de soi-même ce qui regarde les premières. Or nous ferons voir plus bas qu'une classe improprement primitive quelconque répond toujours à une ou à trois classes proprement primitives, et l'on sait que les classes négatives répondant toujours à certaines classes positives, on pourra ne pas s'en occuper.

Afin d'examiner plus à fond la nature des classes proprement primitives, nous expliquerons avant tout une certaine différence essentielle, d'après laquelle un ordre entier de classes peut se subdiviser en genres, et comme nous n'avons pas encore parlé de cet important sujet, il faudra prendre la chose dès l'origine.

228. Théorème. *Il y a une infinité de nombres non divisibles par un nombre premier donné* p *quel qu'il soit, qui peuvent être représentés par une forme proprement primitive* F.

Soit $F=ax^2+2bxy+cy^2$, il est évident que p ne divisera pas à-la-fois les nombres a, $2b$, c. Or, quand a n'est pas divisible par p, il suffira de donner à x une valeur non-divisible par p, et à y une valeur divisible. Quand c n'est pas divisible par p,

on pourra donner à y une valeur non-divisible et à x une valeur divisible; enfin, quand a et c sont divisibles par p, et que partant $2b$ ne l'est pas, on pourra donner à x et à y des valeurs non-divisibles. Dans ces trois cas, il est évident que la valeur de la forme F ne sera pas divisible par p.

Le théorème a lieu également pour les formes improprement primitives, pourvu qu'on n'ait pas $p = 2$.

Comme plusieurs conditions de cette espèce peuvent exister à-la-fois, de manière qu'un nombre soit divisible par de certains nombres premiers, et qu'il ne soit pas divisible par d'autres, on voit facilement que les nombres x, y peuvent être déterminés d'une infinité de manières qui rendent F non-divisible par tant de nombres premiers qu'on voudra (excepté 2 lorsque la forme est improprement primitive). Ainsi le théorème peut être énoncé plus généralement ainsi qu'il suit :

On peut représenter par une forme primitive quelconque, une infinité de nombres premiers à un nombre donné quelconque (impair, quand la forme est improprement primitive).

229. THÉORÈME. *Soit* F *une forme primitive de déterminant* D, p *un nombre premier qui divise* D; *alors tous les nombres non-divisibles par* p, *qui peuvent être représentés par la forme* F, *seront tous résidus quadratiques de* p, *ou tous non-résidus.*

Soit $F = (a, b, c)$; m, m' deux nombres quelconques non-divisibles par p, et qui peuvent être représentés par la forme F, on aura

$$m = ag^2 + 2bgh + ch^2, \qquad m' = ag'^2 + 2bg'h' + ch'^2,$$

et partant

$$mm' = (agg' + b(gh' + g'h) + chh')^2 - D(gh' - hg')^2;$$

donc mm' sera congru à un quarré, suivant le module D, et parconséquent suivant le module p, c'est-à-dire que mm' est résidu quadratique de p. Il suit de là que m et m' seront tous deux résidus ou non-résidus (n° 98).

On prouve de la même manière, que si D est divisible par 4, les nombres impairs qui peuvent être représentés par F,

sont tous $\equiv 1$, ou tous $\equiv 3$; en effet, le produit de deux d'entre eux sera résidu de 4, et partant $\equiv 1 \pmod 4$; parconséquent ils seront tous les deux $\equiv 1$, ou tous les deux $\equiv 3$.

Enfin, quand D est divisible par 8, le produit de nombres impairs qui peuvent être représentés par F, est résidu de 8, et partant $\equiv 1 \pmod 8$; ainsi dans ce cas les nombres impairs qui peuvent être représentés par F sont tous $\equiv 1$, ou tous $\equiv 3$, ou tous $\equiv 5$, ou tous $\equiv 7 \pmod 8$.

Par exemple, le nombre 10, qui est non-résidu de 7, pouvant être représenté par la forme (10, 3, 17), tous les nombres non-divisibles par 7 qui pourront être représentés par cette forme seront non-résidus de 7. Comme -3 peut être représenté par la forme $(-5, 1, 49)$ et qu'il est $\equiv 1 \pmod 4$, tous les nombres impairs qui pourront être représentés par cette forme seront aussi $\equiv 1 \pmod 4$.

Au reste, s'il était nécessaire pour notre objet, nous pourrions démontrer facilement que les nombres représentables par la forme F n'ont pas ainsi une relation fixe à l'égard d'un nombre premier qui ne divise pas D, et que l'on peut représenter par la forme F des résidus ou non-résidus de ce nombre premier indifféremment. Mais quant aux nombres 4 et 8, il y a dans les autres cas quelque chose d'analogue que nous ne pouvons pas passer sous silence.

I. *Quand le déterminant* D *d'une forme primitive* F *est* $\equiv 3 \pmod 4$, *les nombres impairs représentables par* F *seront tous* $\equiv 1$, *ou tous* $\equiv 3 \pmod 4$.

Soient, en effet, m, m' deux nombres représentables par F, on pourra, comme ci-dessus, ramener leur produit à la forme $p^2 - Dq^2$, et les deux nombres m, m' étant impairs, l'un des deux nombres p, q sera pair et l'autre impair, et partant l'un des quarrés p^2, q^2 sera $\equiv 0$, l'autre $\equiv 1 \pmod 4$; d'où l'on conclut aisément que $p^2 - Dq^2 \equiv 1 \pmod 4$, et parconséquent m, m' tous deux $\equiv 1$ ou tous deux $\equiv 3 \pmod 4$. Ainsi, par exemple, par la forme (10, 3, 17) on ne peut représenter d'autres nombres impairs que ceux qui sont de la forme $4n+1$.

II. *Quand le déterminant* D *d'une forme primitive* F *est* $\equiv 2 \pmod 8$, *tous les nombres impairs représentables par* F *seront*

ou

ou en partie $\equiv 1$ *et en partie* $\equiv 7$, *ou en partie* $\equiv 3$ *et en partie* $\equiv 5$ (*mod.* 8).

Soient m, m' deux nombres représentables par F; leur produit peut être ramené à la forme $p^2 - Dq^2$; si m et m' sont impairs, p doit l'être puisque D est pair, et parconséquent on a $p^2 \equiv 1$ (mod. 8); or si q est pair, q^2 sera $\equiv 0$, ou $\equiv 4$ (mod. 8); s'il est impair, q^2 sera $\equiv 1$ (mod. 8); ainsi Dq^2 ne peut être que $\equiv 0$ ou $\equiv 2$. Il suit de là que $p^2 - Dq^2 = mm' \equiv 0$ ou $\equiv 7$, et que si $m \equiv 1$ ou $\equiv 7$, on aura aussi $m' \equiv 1$ ou $\equiv 7$; si $m \equiv 3$ ou $\equiv 5$, m' sera $\equiv 3$ ou $\equiv 5$. Par exemple, tous les nombres représentables par la forme (3, 1, 5) sont $\equiv 3$ ou $\equiv 5$ (mod. 8), et aucun nombre de la forme $8n+1$ ou $8n+7$ ne peut être représenté par la forme (3, 1, 5).

III. *Quand le déterminant* D *d'une forme primitive* F *est* $\equiv 6$ (*mod.* 8), *les nombres impairs qui pourront être représentés par* F *seront ou en partie* $\equiv 1$ *et en partie* $\equiv 3$, (*mod.* 8), *ou en partie* $\equiv 5$ *et en partie* $\equiv 7$ (*mod.* 8).

Chacun pourra faire la démonstration, qui est absolument semblable à la précédente.

Par exemple, par la forme (5, 1, 7) on ne pourra représenter que des nombres qui sont $\equiv 5$ ou $\equiv 7$ (mod. 8).

230. Ainsi tous les nombres qui peuvent être représentés par une forme primitive donnée de déterminant D, ont une relation déterminée avec les différens diviseurs premiers de D, par lesquels ils ne sont pas divisibles, et les nombres impairs qui peuvent être représentés par F, ont, dans certains cas, une relation avec les nombres 4 et 8, savoir, avec 4, toutes les fois que $D \equiv 0$ ou $\equiv 3$ (mod. 4), et avec 8, toutes les fois que $D \equiv 0$, ou $\equiv 2$, ou $\equiv 6$ (mod. 8). Cependant on pourra négliger la relation qui a lieu avec 4, lorsque D sera divisible par 8, car cette relation est contenue dans celles qui ont lieu avec 8. Nous appellerons *caractère* ou *caractère particulier* cette espèce de relation, et nous l'exprimerons de la manière suivante. Quand il n'y a que les résidus du nombre premier p qui peuvent être représentés par la forme F, nous lui attribuerons le caractère $R.p$, et dans le cas contraire, le

caractère $N.p$; de même nous écrirons $1,4$, quand on ne pourra représenter par la forme F d'autres nombres impairs que ceux qui sont $\equiv 1 \pmod 4$, d'où l'on voit clairement quels sont les caractères exprimés par les signes

$$3,4;\quad 1,8;\quad 3,8;\quad 5,8;\quad 7,8.$$

Enfin quand on ne pourra représenter que des nombres qui sont $\equiv 1$ ou $\equiv 7 \pmod 8$, nous attribuerons à la forme le caractère 1 et $7,8$, d'où l'on voit ce que signifient les caractères 3 et $5,8$; 1 et $3,8$; 5 et $7,8$.

Les différens caractères d'une forme primitive donnée (a, b, c) de déterminant D peuvent se connaître au moins par un des nombres a, c qui sont évidemment représentables par cette forme. En effet, toutes les fois qu'un nombre premier p est diviseur de D, il y aura au moins un des nombres a, c qui ne sera pas divisible par p, puisqu'on a $b^2 = D + ac$, et que d'après cela b^2 et parconséquent b sera divisible par tout diviseur premier de D et de l'un des nombres a, c, et que si tous les deux l'étaient, il s'ensuivrait que la forme (a, b, c) ne serait pas primitive. De même, dans les cas où la forme (a, b, c) a une relation déterminée avec les nombres 4 et 8, il y aura au moins un des nombres a, c impair et dont on pourra tirer la relation.

Par exemple, le caractère de la forme $(7, 0, 23)$ à l'égard du nombre 23, se conclut du nombre 7, et il est $N.23$, et à l'égard du nombre 7, il se conclut du nombre 23, et il est $R.7$; enfin le caractère de cette forme, à l'égard du nombre 4, peut se déduire du nombre 7 et du nombre 23.

Comme tous les nombres qui peuvent être représentés par une forme F contenue dans une classe K, peuvent l'être aussi par toute autre forme de la même classe, il est évident que les différens caractères de la forme F appartiennent aussi à toutes les autres formes de cette classe. Ainsi les caractères d'une forme primitive quelconque se connaissent par leur représentante. Les classes opposées ont toujours tous les mêmes caractères.

231. L'ensemble des caractères particuliers d'une forme ou d'une classe donnée constitue le caractère complet de cette forme

ou de cette classe. Ainsi, par exemple, le caractère de la forme (10, 3, 17), ou celui de toute la classe qu'elle représente, est 1,4; $N.7$; $N.23$. De la même manière, le caractère complet de la forme (7, 1, —17) sera 7,8; $R.3$; $N.5$: car le caractère particulier de la forme 3,4 est compris dans le caractère 7,8 De là nous tirons une subdivision de tout l'ordre des classes proprement primitives (positives, quand le déterminant est négatif) d'un déterminant donné en plusieurs genres, en rapportant au même genre toutes les classes qui ont le même caractère complet, et à des genres différens toutes celles qui ont différens caractères complets. Nous attribuerons à ces genres les caractères complets des classes qui y sont contenues.

Par exemple, pour le déterminant —161, il y a seize classes positives proprement primitives, qui peuvent se distribuer en quatre genres, de la manière suivante :

Caractère.	*Formes représentantes des classes.*
1,4; $R.7$; $R.23$..	(1, 0, 161), (2, 1, 81), (9, 1, 18), (9, —1, 18)
1,4; $N.7$; $N.23$..	(5, 2, 33), (5, —2, 33), (10, 3, 17), (10, —3, 17)
3,4; $R.7$; $N.23$..	(7, 0, 23), (11, 2, 15), (11, —2, 15), (14, 7, 15)
3,4; $N.7$; $R.23$..	(3, 1, 54), (3, —1, 54), (6, 1, 27), (6, —1, 27).

On peut faire les remarques suivantes sur le nombre des caractères complets différens.

I. Quand le déterminant D est divisible par 8, à l'égard du nombre 8 il peut y avoir quatre caractères particuliers différens ; le nombre 4 ne donne aucun caractère particulier (n° précéd.). En outre, à l'égard de chacun des diviseurs impairs et premiers de D, il peut y avoir deux caractères, ainsi, si leur nombre est m, il y a 2^{m+2} caractères complets différens, en faisant $m=0$ toutes les fois que D est une puissance de 2.

II. Quand D n'est pas divisible par 8, mais par 4 et en outre par m nombres premiers impairs, il y aura 2^{m+1} caractères complets différens.

III. Quand D est pair, mais non divisible par 4, il sera $\equiv 2$ ou $\equiv 6$ (mod. 8); dans le premier cas, on aura à l'égard du nombre 8, savoir, 1 et 7,8; 3 et 5,8, et autant dans le second.

Si donc l'on suppose m diviseurs premiers impairs, il y aura 2^{m+1} caractères complets.

IV. Quand D est impair, il sera $\equiv 1$ ou $\equiv 3 \pmod 4$. Le caractère du premier cas n'entre pas dans le caractère complet. Dans le second cas, il y a à l'égard de 4 deux caractères. Ainsi m étant le même que ci-dessus, il y aura dans le premier cas 2^m, dans le second 2^{m+1} caractères complets.

Mais il faut bien remarquer qu'il ne suit pas de là qu'on ait autant de genres différens que de caractères complets possibles. Dans l'exemple précédent, le nombre des genres est moitié de celui des caractères, et il n'y a pas de classes positives qui aient pour caractère

$$1,4;\ R.7;\ N.33, \quad \text{ou} \quad 1,4;\ N.7;\ N.23,$$
$$\text{ou} \quad 3,4;\ R.7;\ R.23, \quad \text{ou} \quad 3,4;\ N.7;\ R.23.$$

Nous traiterons plus bas avec détail ce sujet important.

Comme la forme $(1, 0, -D)$ est évidemment la plus simple des formes de déterminant D, nous lui donnerons le nom de *forme principale*, à la classe dans laquelle elle est contenue, celui de *classe principale*, et enfin au genre auquel cette classe appartient, celui de *genre principal*. Ainsi il faut bien distinguer la forme principale, de la forme d'une classe principale et de la forme d'un genre principal, ainsi qu'une classe principale et une classe d'un genre principal. Nous nous servirons toujours de ces dénominations, même quand il arriverait que pour un certain déterminant il n'y eût pas d'autre classe que la classe principale, ou pas d'autre genre que le genre principal, comme cela a lieu souvent dans le cas où D est un nombre positif de la forme $4n+1$.

232. Quoique ce qui a été expliqué sur les caractères des formes l'ait été surtout dans le dessein d'en déduire la subdivision en genres de l'ordre entier des classes positives proprement primitives, rien n'empêche qu'on ne l'applique aux formes et aux classes négatives ou improprement primitives, et qu'on ne subdivise en genres, tant l'ordre proprement primitif positif ou négatif, que l'ordre improprement primitif positif ou négatif.

Ainsi, par exemple, lorsqu'on a partagé en deux genres l'ordre proprement primitif des formes de déterminant 145,

$R.5$; $R.29$.....	(1, 0, —145), (5, 0, —29)
$N.5$; $N.29$.....	(3, 1, — 48), (3, —1, —48);

l'ordre improprement positif peut se subdiviser de même en deux genres,

$R.5$; $R.29$.....	(4, 1, —36), (4, —1, —36)
$N.5$; $N.29$.....	(2, 1, —72), (10, 5, —12)

ou, de même que les classes positives des formes de déterminant — 129 se distribuent en quatre genres,

1,4; $R.3$; $R.43$....	(1, 0, 129), (10, 1, 13), (10, —1, 13)
1,4; $N.3$; $N.43$....	(2; 1, 65), (5, 1, 26), (5, —1, 26)
3,4; $R.3$; $N.43$....	(3, 0, 43), (7, 2, 19), (7, —2, 19)
3,4; $N.3$; $R.43$....	(6, 3, 23), (11, 5, 14), (11, —5, 14);

les classes négatives se partagent aussi en quatre ordres,

3,4; $N.3$; $N.43$...	(—1, 0, —129), (—10, 1, —13), (—10, —1, —13)
3,4; $R.3$; $R.43$...	(—2, 1, — 65), (— 5, 1, —26), (— 5, —1, —26)
1,4; $N.3$; $R.43$...	(—3, 0, — 43), (— 7, 2, —19), (— 7, —1, —19)
1,4; $R.3$; $N.43$...	(—6, 3, — 23), (—11, 5, —14), (—11, —5, —14).

Mais puisque le système des classes négatives se trouve toujours si semblable à celui des classes positives, il semble qu'il est le plus souvent inutile de les considérer séparément. Quant à l'ordre improprement primitif, nous enseignerons plus bas à le réduire à l'ordre proprement primitif.

Pour la subdivision des ordres dérivés, il n'est pas nécessaire de donner de nouvelles règles; puisque chaque ordre dérivé tirant son origine de quelque ordre primitif de déterminant moindre, la subdivision d'un ordre dérivé suit naturellement de celle de l'ordre primitif dont il provient.

233. Si une forme primitive $F=(a, b, c)$ est telle que l'on puisse trouver deux nombres g, h pour lesquels on ait $g^2 \equiv a$, $gh \equiv b$, $h^2 \equiv c$, suivant un module donné m, on aura....

$(gx+hy)^2 \equiv ax^2+2bxy+cy^2 \pmod{m}$, et partant on peut dire que la forme F est résidu de m, et que $hx+hy$ est la valeur de l'expression $\sqrt{(ax^2+2bxy+cy^2)} \pmod{m}$, ce que nous exprimerons plus simplement en écrivant que (g, h) est une valeur de $\sqrt{F} \pmod{m}$; plus généralement, si un nombre M premier avec m est tel qu'on ait $g^2 \equiv Ma$, $gh \equiv Mb$, $h^2 \equiv Mc \pmod{m}$, nous dirons que MF est résidu de m et $(g, h) = \sqrt{MF} \pmod{m}$. Ainsi, par exemple, la forme $(3, 1, 54)$ est résidu quadratique de 23, et $(7, 10)$ est la valeur de $\sqrt{(3, 1, 54)} \pmod{m}$. De même $(2, -4)$ est la valeur de l'expression $\sqrt{5}(10, 3, 17) \pmod{23}$.

On verra plus bas l'usage de ces expressions; ici nous ferons les remarques suivantes :

1°. Si $M(a, b, c)$ est résidu quadratique de m, m divisera le déterminant de la forme (a, b, c); en effet, puisqu'on a $g^2 \equiv aM$, $gh \equiv bM$, $h^2 \equiv cM \pmod{m}$, on en tire

$$b^2M^2 - acM^2 = (b^2 - ac)M^2 \equiv 0 \pmod{m}.$$

Mais comme M est premier avec m, il s'ensuit donc que b^2-ac est divisible par m.

2°. Si $M(a, b, c)$ est résidu de m, et que m soit un nombre premier, ou une puissance d'un nombre premier, p^μ, par exemple, le caractère particulier de la forme (a, b, c), à l'égard du nombre p, sera $R.p$ ou $N.p$, suivant que M sera résidu ou non-résidu de p. En effet, aM et cM sont résidus de p, et il y a au moins un des nombres a, c qui n'est pas divisible par p (n° 230); donc si M est résidu ou non-résidu, un des deux nombres a et c le sera aussi.

De même, si toutes choses d'ailleurs égales, $m=4$, le caractère particulier de la forme (a, b, c) sera 1,4 ou 3,4, suivant que l'on aura $M \equiv 1$ ou $\equiv 3 \pmod{4}$, et si $m=8$ ou une plus haute puissance de 2, le caractère particulier de la forme (a, b, c) sera 1,8; 3,8; 5,8; 7,8, suivant que $M \equiv 1; 3; 5; 7 \pmod{8}$.

3°. Réciproquement si m est un nombre premier ou une puissance d'un nombre premier $\equiv p^\mu$ qui divise b^2-ac, et que M soit résidu ou non-résidu de p, suivant que le caractère par-

ticulier de la forme (a, b, c), à l'égard du nombre p, est $R.p$ ou $N.p$ respectivement, $M(a, b, c)$ sera résidu de m. En effet, quand a n'est pas divisible par p, aM sera résidu de p, et partant de m lui-même; si donc g est une valeur de l'expression $\sqrt{aM}$ (mod. m) et que h soit une valeur de $\frac{bg}{a}$ (mod. m), on aura $g^2 \equiv aM$, $ah \equiv bg$, et partant $agh \equiv bg^2 \equiv abM$ et $gh \equiv bM$; enfin $ah^2 \equiv bgh \equiv b^2M \equiv b^2M - (b^2 - ac)M \equiv acM$, d'où $h^2 \equiv cM$; donc (g, h) est une valeur de l'expression $\sqrt{(a, b, c)M}$. Mais quand a est divisible par p, comme alors c ne l'est surement pas, on voit qu'on arrivera au même résultat, en prenant $h = \sqrt{cM}$ (mod. m) et $g = \frac{bh}{c}$ (mod. m).

On démontre de la même manière, que si $m = 4$, qu'il divise $b^2 - ac$, et qu'on prenne le nombre $M \equiv 1$ ou $\equiv 3$, suivant que le caractère particulier de la forme est 1,4 ou 3,4, $M(a, b, c)$ sera résidu de m, et que $m = 8$ ou une plus haute puissance de 2, par laquelle $b^2 - ac$ soit divisible, et que l'on prenne $M \equiv 1$; 3; 5; 7 (mod. 8, suivant que le caractère particulier de la forme le demande, $M(a, b, c)$ sera résidu de m.

4°. Si le déterminant de la forme (a, b, c) est $= D$, et que $M(a, b, c)$ soit résidu de D, tous les caractères particuliers de la forme, tant à l'égard des diviseurs premiers de D, qu'à l'égard des nombres 4 et 8, s'ils sont diviseurs de D, peuvent se connaître sur-le-champ par le nombre M. Ainsi, par exemple, comme 3(20, 10, 27) est résidu de 440, c'est-à-dire que (150, —9) est une valeur de l'expression $\sqrt{3}(20, 10, 27)$ (mod. 440), et qu'on a $3N.5$ et $3R.11$; les caractères de la forme (20, 10, 27) sont 3,8; $N.5$; $R.11$. Les caractères relatifs à 4 et à 8, toutes les fois que ces nombres ne divisent pas D, sont les seuls qui ne dépendent pas nécessairement du nombre M.

5°. Réciproquement, si le nombre M premier avec D renferme tous les caractères particuliers de la forme (a, b, c) excepté ceux relatifs à 2 et à 8, quand ces nombres ne divisent pas D, $M(a, b, c)$ sera résidu de D. En effet, par ce qui a été dit (3°.), il est clair qu'en mettant D sous la forme $\pm A^\alpha, B^\beta, C^\gamma \ldots$, A, B, C, etc.

étant des nombres premiers différens, $M(a, b, c)$ sera résidu de chacun des nombres A^α, B^β, C^γ, etc.; si donc la valeur de $\sqrt{M(a, b, c)}$ (mod. A^α) est (G, G'); que $\sqrt{M(a, b, c)}$ (mod. B^β) soit (H, H'), que $\sqrt{M(a, b, c)}$ (mod. C^γ) soit (L, L'), etc. et que les nombres g, h soient déterminés de manière qu'on ait $g \equiv G, H, L$, etc., $h \equiv G', H', L'$, etc., suivant les modules A^α, B^β, C^γ, etc. Respectivement (n° 32), on verra facilement que l'on aura $g^2 \equiv aM$, $gh \equiv bM$, $h^2 \equiv cM$, suivant chacun des modules A^α, B^β, C^γ, et parconséquent suivant le module D, qui est leur produit.

6°. Pour toutes ces raisons, les nombres tels que M, qu'on peut trouver sans peine, par ce que nous avons dit (5°.), dès qu'on connaît les caractères particuliers de la forme, se nommera *nombre caractéristique*. On trouve sans peine les plus simples, par tâtonnement, dans un grand nombre de cas. Il est évident que si M est le nombre caractéristique d'une forme primitive donnée de déterminant D, tous les nombres qui lui seront congrus suivant le module D, seront caractéristiques de la même forme; que les formes d'une même classe, ou même de classes différentes, mais du même ordre, ont le même nombre caractéristique, et que parconséquent tout nombre caractéristique de la forme donnée peut être attribué à toute la classe et à tout l'ordre; enfin que 1 est nombre caractéristique des forme, classe et genre principaux, c'est-à-dire, que toute forme principale est résidu de son déterminant.

7°. Si (g, h) est une valeur de l'expression $\sqrt{M(a, b, c)}$ (mod. m), et qu'on ait $g' \equiv g$, $h' \equiv h$ (mod. m), (g', h') sera aussi valeur de cette expression. De telles valeurs peuvent être regardées comme équivalentes; au contraire, si (g, h) et (g', h') sont valeurs de l'expression $\sqrt{M(a, b, c)}$, et qu'on n'ait pas $g' \equiv g$, $h' \equiv h$ (mod. m), on doit les considérer comme différentes. Il est évident que si (g, h) est une valeur, $(-g, -h)$ en est une aussi, et on démontre facilement qu'elles sont différentes, à moins qu'on n'ait $m = 2$. On démontre aussi facilement que l'expression $\sqrt{M(a, b, c)}$ ne peut pas avoir plus de valeurs

valeurs différentes que ses deux opposées, quand m est un nombre premier impair, ou une puissance d'un nombre premier impair, ou $=4$; mais quand $m=8$ ou une plus haute puissance de 2, il y en a quatre en tout. On conclut facilement de là, au moyen de ce qui a été exposé (6°.), que si le déterminant D de la forme (a, b, c) est $=\pm 2^{\mu} A^{\alpha} B^{\beta}$, etc, A, B, etc. étant des nombres premiers impairs dont le nombre est n, et que M soit le nombre caractéristique de cette forme, il y aura en tout 2^n, 2^{n+1} ou 2^{n+2} valeurs différentes de l'expression $\sqrt{M}(a, b, c)$ (mod. D), suivant que $\mu<2$, $=2$ ou >2. Ainsi, par exemple, on a 16 valeurs de l'expression $\sqrt{7}(12, 6, -17)$ (mod. 240), qui sont :

$(\pm 18, \mp 11)$, $(\pm 18, \pm 29)$, $(\pm 18, \mp 91)$, $(\pm 18, \pm 109)$,
$(\pm 78, \pm 19)$, $(\pm 78, \pm 59)$, $(\pm 78, \mp 61)$, $(\pm 78, \mp 101)$.

Nous supprimons la démonstration, qui est assez longue, et qui n'est pas nécessaire ici.

8°. Observons enfin que si deux formes équivalentes F, F' ont D pour déterminant, que le nombre caractéristique soit M et que F se change en F' par la substitution α, β, γ, δ, d'une valeur (g, h) de $\sqrt{M.F}$ (mod. D), on tirera $(\alpha g+\gamma h, \beta g+\delta h)$ pour la valeur de $\sqrt{M.F'}$ (mod. D), chacun pourra trouver sans peine la démonstration.

234. Après avoir exposé ces détails sur la distribution des formes en classes, en genres et en ordres, et avoir expliqué les propriétés qui naissent de ces distinctions, nous allons passer à un autre sujet très-important et dont personne ne s'est encore occupé, à la *composition* des formes; mais avant de commencer cette recherche, nous placerons le lemme suivant, pour ne pas être obligé d'interrompre l'ordre des démonstrations.

LEMME. *Si l'on a quatre suites de nombres entiers :* a, a′, a″,...a^n; b, b′, b″,...b^n; c, c′, c″,...c^n; d, d′, d″,...d^n, *composées d'autant de termes, et telles qu'on ait*

$$cd'-dc'=k(ab'-ba'),\quad cd''-dc''=k(ab''-ba''),\ \textit{etc.}$$
$$c'd''-c''d'=k(a'b''-a''b'),\ \textit{etc.},\ \textit{etc.}$$

ou généralement $c^{\lambda}d^{\mu} - d^{\lambda}c^{\mu} = k(a^{\lambda}b^{\mu} - b^{\lambda}a^{\mu})$, k *étant un nombre entier donné,* μ, ν *des entiers différens dont* μ *est le plus grand, et compris entre* o *et* n; *qu'en outre, toutes les quantités de la forme* $a^{\lambda}b^{\mu} - b^{\lambda}a^{\mu}$ *n'aient pas de diviseur commun; alors on peut trouver quatre nombres entiers* α, β, γ, δ *tels que l'on ait*

$$\alpha a + \beta b = c,\ \alpha a' + \beta b' = c',\ \alpha a'' + \beta b'' = c'',\ \text{etc.}$$
$$\gamma a + \delta b = d,\ \gamma a' + \delta b' = d',\ \text{etc.}$$

ou généralement $\alpha a^{\nu} + \beta b^{\nu} = c^{\nu}$, $\gamma a^{\nu} + \delta b^{\nu} = d^{\nu}$; *auquel cas on aura* $\alpha\delta - \beta\gamma = k$.

Puisque, par hypothèse, les nombres $ab' - a'b$, $ab'' - a''b$, etc. $a'b'' - a''b'$, etc., dont le nombre est $\frac{1}{2}(n+1)n$, n'ont pas de diviseur commun, on peut trouver autant de nombres entiers tels que la somme des produits des premiers par les derniers soit $= 1$ (n° 40). Désignons ces multiplicateurs par (0, 1), (0, 2), etc. (1, 2), etc.; ou généralement désignons le multiplicateur de $a^{\lambda}b^{\mu} - b^{\lambda}a^{\mu}$ par (λ, μ), desorte qu'on ait $\Sigma(\lambda, \mu)(a^{\lambda}b^{\mu} - b^{\lambda}a^{\mu}) = 1$, Σ désignant la somme de toutes les valeurs qui peuvent résulter de la quantité qu'il précède, lorsqu'on donne successivement à λ et μ toutes les valeurs comprises entre o et n, de manière que $\mu > \lambda$. Cela posé, si l'on fait

$$\Sigma(\lambda, \mu)(c^{\lambda}b^{\mu} - b^{\lambda}c^{\mu}) = \alpha,\ \Sigma(\lambda, \mu)(a^{\lambda}c^{\mu} - c^{\lambda}a^{\mu}) = \beta,$$
$$\Sigma(\lambda, \mu)(d^{\lambda}b^{\mu} - b^{\lambda}d^{\mu}) = \gamma,\ \Sigma(\lambda, \mu)(a^{\lambda}d^{\mu} - d^{\lambda}a^{\mu}) = \delta,$$

les nombres α, β, γ, δ jouiront des propriétés énoncées ci-dessus.

I. ν étant un nombre entier quelconque entre o et n, on aura

$$\alpha a^{\nu} + \beta b^{\nu} = \Sigma(\lambda, \mu)(c^{\lambda}b^{\mu}a^{\nu} - b^{\lambda}c^{\mu}a^{\nu} + a^{\lambda}c^{\mu}b^{\nu} - c^{\lambda}a^{\mu}b^{\nu})$$
$$= \frac{1}{k}\Sigma(\lambda, \mu)(c^{\lambda}d^{\mu}c^{\nu} - d^{\lambda}c^{\mu}c^{\nu}) = \frac{1}{k}c^{\nu}\Sigma(\lambda, \mu)(c^{\lambda}d^{\mu} - d^{\lambda}c^{\mu})$$
$$= c^{\nu}\Sigma(\lambda, \mu)(a^{\lambda}b^{\mu} - b^{\lambda}c^{\mu}) = c^{\nu};$$

et par un calcul semblable, on prouve que $\gamma a^{\nu} + \delta b^{\nu} = d^{\nu}$.

II. On a parconséquent $c^\lambda = \alpha a^\lambda + \beta b^\lambda$, $c^\mu = \alpha a^\mu + \beta b^\mu$, et partant

$$c^\lambda b^\mu - b^\lambda c^\mu = \alpha(a^\lambda b^\mu - a^\mu b^\lambda);$$

de même.....$a^\lambda c^\mu - c^\lambda a^\mu = \beta(a^\lambda b^\mu - b^\lambda a^\mu)$

$$d^\lambda b^\mu - b^\lambda d^\mu = \gamma(a^\lambda b^\mu - a^\mu b^\lambda)$$

$$a^\lambda d^\mu - d^\lambda a^\mu = \delta(a^\lambda b^\mu - a^\mu b^\lambda),$$

d'où l'on tirera plus facilement les valeurs de α, β, γ, δ, pourvu qu'on prenne λ et μ de manière que $a^\lambda b^\mu - b^\lambda a^\mu$ ne soit pas $= 0$, ce qui est possible, puisque toutes les quantités de cette forme sont supposées ne pas avoir de diviseur commun, et que parconséquent elles ne peuvent pas être toutes $= 0$. On tire aisément de ces équations

$$(\alpha\delta - \beta\gamma)(a^\lambda b^\mu - a^\mu b^\lambda)^2 = (a^\lambda b^\mu - b^\lambda a^\mu)(c^\lambda d^\mu - d^\lambda c^\mu) = k(a^\lambda b^\mu - b^\lambda a^\mu)^2,$$

d'où nécessairement $\alpha\delta - \beta\gamma = k$.

235. Si la forme $AX^2 + 2BXY + CY^2 = F$, se change en le produit des deux formes $ax^2 + 2bxy + cy^2 = f$, $a'x'^2 + 2b'x'y' + c'y'^2 = f'$ par la substitution

$$X = pxx' + p'xy' + p''x'y + p'''yy', \quad Y = qxx' + q'xy' + q''x'y + q'''yy',$$

(ce que nous exprimerons d'une manière abrégée en disant : Si F se change en ff' par la substitution p, p', p'', p'''; q, q', q'', q''') la forme F sera dite *transformable* en ff', et si de plus cette transformation est telle que les six nombres

$$pq' - p'q,\ pq'' - p''q,\ pq''' - p'''q,\ p'q'' - p''q',\ p'q''' - p'''q',\ p''q''' - p'''q''$$

n'aient pas de diviseur commun, la forme F sera dite *composée* des formes f, f'.

Nous commencerons par l'hypothèse la plus générale, celle où la forme F se changerait en ff' par la substitution p, p', p'', p'''; q, q', q'', q''', et nous développerons les conséquences qui en résultent.

Cette condition est exprimée par les neuf équations suivantes :

$$Ap^2 + 2Bpq + Cq^2 = aa' \quad \ldots\ldots (1)$$
$$Ap'^2 + 2Bp'q' + Cq'^2 = ac' \quad \ldots\ldots (2)$$
$$Ap''^2 + 2Bp''q'' + Cq''^2 = a'c \quad \ldots\ldots (3)$$
$$Ap'''^2 + 2Bp'''q''' + Cq'''^2 = cc' \quad \ldots\ldots (4)$$
$$App' + B(pq' + p'q) + Cqq' = ab' \quad \ldots\ldots (5)$$
$$App'' + B(pq'' + p''q) + Cqq'' = a'b \quad \ldots\ldots (6)$$
$$Ap'p''' + B(p'q''' + p'''q') + Cq'q''' = bc' \quad \ldots\ldots (7)$$
$$Ap''p''' + B(p''q''' + p'''q'') + Cq''q''' = cb' \quad \ldots\ldots (8)$$
$$A(pp''' + p'p'') + B(pq''' + p'''q + p'q'' + p''q') + C(qq''' + q'q'') = 2bb' \ldots (9).$$

Soient D, d, d' les déterminans des formes F, f, f' respectivement; M, m, m' les plus grands communs diviseurs des nombres A, $2B$, C; a, $2b$, c; a', $2b'$, c' respectivement, M, m, m' étant pris positivement. Déterminons les six nombres A_1, B_1, C_1; A_2, B_2, C_2 de manière qu'on ait

$$A_1a + B_1b + C_1c = m, \qquad A_2a' + B_2b' + C_2c' = m'.$$

Faisons enfin $pq' - p'q = P$, $pq'' - p''q = Q$, $pq''' - p'''q = R$, $p'q'' - p''q' = S$, $p'q''' - p'''q' = T$, $p''q''' - p'''q'' = U$, et supposons que k soit leur plus grand commun diviseur (*).

Posant maintenant

$$App''' + B(pq''' + p'''q) + Cqq''' = bb' + \Delta \ldots\ldots (10),$$

(*) On peut présenter cette recherche de la manière suivante.

On tire des dernières équations que vient de poser l'auteur, en supposant connues P, Q, R, S, T, U, et par l'élimination entre les valeurs de Q, R, S, T,

$$Pq'' = Qq' - Sq, \quad Pp'' = Qp' - Sp, \quad Pq''' = Rq' - Tq, \quad Pp''' = Rp' - Tp;$$

et comme on a l'équation $pq' - p'q = 0$, il vient en substituant dans la valeur de U celles de q'', q''', p'', p''', l'équation de condition,

$$QT - RS = PU.$$

Substituant enfin les valeurs de ces mêmes quantités dans les équations (3), (4), (6), (7), (8), (9), on obtient six équations que je désignerai par
(α), (ζ), (γ), (δ), (ε), (ξ).

De (α) et (γ) on tire en éliminant S, et faisant $\sqrt{\frac{d}{d'}} = \mu$,

$$Q = \frac{a'P}{a}, \quad T = \frac{c'P}{a}.$$

Les équations (ζ), (δ) donnent $S = \frac{P}{a}(\mu b' - b)$, $R = \frac{P}{a}(\mu b' + b)$, et l'on

l'équation (9) donne

$$Ap'p'' + B(p'q'' + p''q') + Cq'q'' = bb' - \Delta \ldots\ldots (11).$$

De ces onze équations on tire les suivantes, savoir :

En élevant l'équation (5) au quarré et en retranchant le pro-

---

a facilement $R+S$, $R-S$: les équations (ε), (ξ) s'anéantissent d'elles-mêmes, et les équations (1), (2) et (3) donnent sans peine, comme dans le n° 157, $P^2D = a^2d'$; substituant dans les équations qui donnent Q, R, S, T et dans l'équation de condition, et faisant $\sqrt{\frac{d'}{D}} = n'$, $\sqrt{\frac{d}{D}} = n$; il vient

$$P = an', \; Q = a'n, \; R - S = 2bn', \; R + S = 2b'n, \; T = c'n, \; U = cn' \ldots\ldots (\Gamma).$$

Comme P, Q, R, S, T, U sont entiers, on voit que 1° n et n' sont rationnels, et partant, $\frac{d}{D}$, $\frac{d'}{D}$ des nombres carrés ; 2°. si n est une fraction, son dénominateur doit être un diviseur de m' plus grand commun diviseur entre a', $2b'$, c', et que parconséquent $m'n$ est entier ; il en est de même de mn'. Or ces équations $d = Dn^2$, $d' = Dn'^2$ donnent $dm'^2 = D(m'n)^2$, $d'm^2 = D(mn')^2$; donc D ne peut pas être plus grand que le plus grand commun diviseur entre dm'^2 et $d'm^2$.

Il est aisé de démontrer que le plus grand commun diviseur k des nombres P, Q, R, S, T, U doit diviser mn' et $m'n$. En effet, on a

$$mn' = P : \frac{a}{m} = (R - S) : \frac{2b}{m} = U : \frac{c}{m} ;$$

parconséquent

$$\frac{P}{k} : \left(\frac{R-S}{k}\right) = \frac{a}{m} : \frac{2b}{m} \text{ et } \frac{P}{k} : \frac{U}{k} = \frac{a}{m} : \frac{C}{m} ;$$

mais deux des trois nombres $\frac{a}{m}$, $\frac{2b}{m}$, $\frac{c}{m}$ sont nécessairement premiers entre eux ; donc $\frac{P}{k}$ est divisible par $\frac{a}{m}$, ainsi l'on a $\frac{Pm}{ak} = \frac{mn'}{k}$ égal à un nombre entier. On démontre de même pour $m'n$ et la réciproque, comme l'auteur (4ᵉ conclusion).

Aux six équations (Γ) doivent être ajoutées les équations (1), (2), (3) qu'on peut mettre sous une forme plus simple en éliminant deux des nombres A, B, C, alternativement ; on trouve

$$AP^2 = aa'q'^2 - 2ab'qq' + ac'q^2 \ldots BP^2 = -aa'p'q' + ab'(pq' + p'q) - ac'pq \ldots$$
$$CP^2 = aa'p'^2 - 2ab'pp' + ac'p^2 :$$

donc AP^2, $2BP^2$, CP^2 sont divisibles par mm'.

On obtiendra les 15 autres équations de l'auteur, en substituant les valeurs de p', q' : 1°. en fonction de p, p'' et de q, q'' ; 2°. en fonction de p, p''', et de q, q''', ainsi de suite. On suivra quant au reste la marche de l'auteur (*Note du Traducteur*).

duit de l'équation (1) par l'équation (2),

$$D.P^2 = d'a^2 \ldots\ldots\ldots\ldots\ldots (12);$$

en multipliant l'équation (5) par l'équation (9), l'équation (1) par l'équation (7), l'équation (2) par l'équation (6), et retranchant du premier produit la somme des deux derniers,

$$DP(R-S) = 2d'ab \ldots\ldots\ldots (13);$$

en multipliant l'équation (10) par l'équation (11), l'équation (6) par l'équation (7), et retranchant le second produit du premier,

$$DPU = d'ac - (\Delta^2 - dd') \ldots (14);$$

en ajoutant le double produit des équations (5) et (8), les quarrés des équations (10) et (11), et retranchant de leur somme les produits des équations (1) et (4), (2) et (3) et deux fois le produit des équations (6) et (7),

$$D(R-S)^2 = 4d'b^2 + 2(\Delta^2 - dd') \ldots\ldots (15);$$

en retranchant du produit de l'équation (8) par l'équation (9), la somme des produits des équations (3) et (7), (4) et (6),

$$D(R-S)U = 2d'bc \ldots\ldots\ldots\ldots (16);$$

en retranchant du quarré de l'équation (8) le produit des équations (3) et (4),

$$DU^2 = d'c^2 \ldots\ldots\ldots\ldots (17);$$

en remplaçant dans les mêmes calculs les équations (2), (5), (7), par les équations (3), (6), (8) respectivement, et réciproquement :

$$DQ^2 = da'^2 \ldots\ldots\ldots\ldots\ldots (18)$$
$$DQ(R+S) = 2da'b' \ldots\ldots\ldots\ldots (19)$$
$$DQT = da'c' - (\Delta^2 - dd') \ldots\ldots\ldots (20)$$
$$D(R+S)^2 = 4db'^2 + 2(\Delta^2 - dd') \ldots (21)$$
$$D(R+S)T = 2db'c' \ldots\ldots\ldots\ldots (22)$$
$$DT^2 = dc'^2. \ldots\ldots\ldots\ldots\ldots (23).$$

De ces équations on tire, 1°. en retranchant le quarré de l'équation (13), du produit des équations (12) et (15); 2°. en retranchant le produit des équations (12) et (17), du quarré de l'équation (14) :

$$0 = 2d'a^2(\Delta^2 - dd') \ldots\ldots 0 = (\Delta^2 - dd')^2 - 2d'ac(\Delta^2 - dd'),$$

ce qui prouve la relation $\Delta^2 - dd' = 0$, soit qu'on ait ou non $a = 0$. Cette manière de trouver l'équation $\Delta^2 = dd'$ suffit pour les recherches présentes ; mais nous aurions pu la trouver directement par une analyse plus élégante mais trop longue pour être placée ici, en déduisant directement des onze premières équations celle-ci $0 = (\Delta - dd')^2$. Nous supposerons donc qu'on ait effacé $\Delta^2 - dd'$ dans les équations (14), (15), (20), (21).

Or si l'on fait

$$A_1P + B_1(R - S) + C_1U = mn', \quad A_2Q + B_2(R + S) + C_2T = m'n,$$

où n, n' peuvent être des fractions, pourvu que mn' et $m'n$ soient entiers, on tire facilement des équations (12).....(17),

$$Dm^2n'^2 = d'(A_1a + 2B_1b + C_1c)^2 = d'm^2,$$

et des équations (18).....(23),

$$Dm'^2n^2 = d(A_2a' + 2B_2b' + C_2c')^2 = dm'^2.$$

On a donc $d = Dn^2$, $d' = Dn'^2$, d'où nous tirons une PREMIÈRE CONDITION : *les déterminans des formes* F, f, f' *sont entre eux comme des nombres quarrés* ; et une SECONDE : D *divise toujours* dm'^2 *et* $d'm^2$. Il suit donc de là que D, d, d' sont de même signe, et qu'aucune forme ne peut être transformée en le produit ff' si son déterminant est plus grand que le plus grand diviseur commun des nombres dm'^2 et $d'm^2$.

Si l'on multiplie les équations (12), (13), (14) par A_1, B_1, C_1 respectivement ; les équations (13), (15), (16), les équations (14), (16), (17) par les mêmes nombres et de la même manière ; que l'on ajoute les trois produits en y remplaçant d' par Dn'^2, on trouve, à l'aide de l'équation $A_1P + B_1(R - S) + CU_1 = mn'_1$

$$P = an', \quad R - S = 2bn', \quad U = cn'.$$

de même, en multipliant, 1°. les équations (18), (19), (20) ; 2°. les équations (19), (21), (22) ; 3°. les équations (20), (22), (23) par A_2, B_2, C_2 respectivement, on a

$$Q = a'n, \quad R + S = 2b'n, \quad T = c'n.$$

Ce qui donne une TROISIÈME CONDITION : *les nombres* a, 2b, c *sont proportionnels aux nombres* P, R — S, U ; *et en supposant*

que leur rapport est celui de 1 *à* n′, n′ *sera la racine quarrée de* $\frac{d'}{D}$: *de même, les nombres* a′, 2b′, c′ *sont proportionnels aux nombres* Q, R+S, T; *et si l'on suppose que leur rapport est celui de* 1 *à* n, n *sera la racine quarrée de* $\frac{d}{D}$.

Au reste les quantités n, n' peuvent être les racines positives ou négatives de $\frac{d}{D}$ et $\frac{d'}{D}$, d'où nous tirons une distinction qui paraît stérile au premier abord, mais dont l'usage se reconnaîtra par la suite. Nous dirons que dans la transformation de F en ff', la forme f est prise *directement* quand n est positif, *indirectement* quand n est négatif, et de même à l'égard de f'. Mais en ajoutant la condition que $k=1$, nous dirons que la forme F est composée ou directement des deux formes f, f', ou indirectement de ces deux mêmes formes, ou directement de f et indirectement de f', ou directement de f' et indirectement de f, suivant que les deux nombres n, n' seront positifs ou négatifs, ou que n sera positif et n' négatif, ou n négatif et n' positif. D'ailleurs on voit facilement que ces relations ne dépendent pas de l'ordre dans lequel ces formes sont placées.

Or nous observons que le plus grand diviseur commun k des nombres P, Q, R, S, T, U divise les nombres mn', $m'n$, ce qui résulte des valeurs établies plus haut pour ces nombres, et que parconséquent k^2 doit diviser $m^2n'^2$, m'^2n^2, et Dk^2 les nombres $d'm^2$, dm'^2; mais réciproquement tout diviseur commun de mn', $m'n$ divisera aussi k. En effet, soit e un de ces diviseurs, il divisera évidemment les nombres an', $2bn'$, cn', $a'n$, $2b'n$, $c'n$, et partant, $P, R-S, U, Q, R+S, T$, et d'après cela $2R$ et $2S$. Or si $\frac{2R}{e}$ était impair, $\frac{2S}{e}$ le serait aussi, puisque la somme est paire ainsi que la différence; leur produit serait donc impair. Mais ce produit est $\frac{4}{e^2}(b'^2n^2-b^2n'^2)=\frac{4}{e^2}(d'n^2+a'c'n^2-dn'^2-acn'^2)=\frac{4}{e^2}(a'c'n^2-acn'^2)$, et parconséquent pair, puisque e divise $a'n$, $c'n$, an', cn'. Donc $\frac{2R}{e}$ est nécessairement pair, et partant, R et S sont divisibles par e.

Donc

Donc e divisant les six nombres P, Q, R, S, T, U, divisera aussi leur plus grand commun diviseur k. Donc k est le plus grand diviseur commun entre mn' et $m'n$; d'où l'on voit facilement que Dk^2 est le plus grand commun diviseur des nombres dm'^2, $d'm^2$. C'est la QUATRIÈME CONCLUSION. Il est donc clair que toutes les fois que F sera composée de f et f', comme on a $k=1$, D sera le plus grand commun diviseur des nombres dm'^2, $d'm^2$ et réciproquement. Cette propriété aurait pu être prise comme définition de la forme composée. Ainsi la forme composée des formes f, f', a le plus grand déterminant possible parmi toutes les formes qui peuvent être transformées en le produit ff'.

Avant que nous puissions aller plus loin, il faut déterminer avec plus d'exactitude la valeur de Δ que nous avons trouvé $= \sqrt{dd} = \sqrt{D^2n^2n'^2}$, mais dont le signe n'est pas encore fixé. A cet effet, nous déduirons des équations fondamentales l'équation $DPQ=aa'\Delta$, en retranchant le produit de l'équation (1) par l'équation (2), de celui de l'équation (5) par l'équation (6); et partant, $Daa'nn'=aa'\Delta$, ou $Dnn'=\Delta$, à moins qu'un des nombres a, a' ne fût nul. Mais on tire des équations (1).....(2) absolument de la même manière, huit autres équations dans lesquelles Dnn' à gauche, Δ à droite, sont multipliés par $2ab'$, ac', $2ba'$, $4bb'$, $2bc'$, ca', $2cb'$, cc'; et comme les nombres $a, 2b, c$ ne peuvent être nuls en même temps, non plus que les nombres $a', 2b', c'$, il s'ensuit qu'on aura dans tous les cas $\Delta = Dnn'$, et que parconséquent Δ aura le même signe que D, d, d', ou un signe différent, suivant que n et n' auront le même signe, ou un signe différent.

Or les nombres aa', $2ab'$, ac', $2ba'$, $4bb'$, $2c'b$, ca', $2cb'$, cc', $2bb'+2\Delta$, $2bb'-2\Delta$ sont tous divisibles par mm'. La chose est évidente pour les neuf premiers; quant aux deux autres, on les démontrera comme nous avons démontré plus haut que R et S étaient divisibles par e. En effet, $4bb'+4\Delta$ et $4bb'-4\Delta$ sont divisibles par mm', puisque $4\Delta = \sqrt{16dd'}$, que $4d$ est divisible par m^2, $4d'$ par m'^2, partant, $16dd'$ par $m^2m'^2$ et $4\Delta = \sqrt{16dd'}$ par mm'; la somme et la différence des quotiens sont paires; et comme l'on démontre facilement que le produit des quotiens est également pair, chacun de ces quotiens l'est aussi, et parconséquent $2bb'+2\Delta$ et $2bb'-2\Delta$ sont divisibles par mm'.

Maintenant, on déduira facilement des équations fondamentales les six suivantes :

$$\begin{aligned}
AP^2 &= aa'q'^2 - 2ab'qq' + ac'q^2,\\
AQ^2 &= aa'q''^2 - 2a'bqq'' + a'cq^2,\\
AR^2 &= aa'q'''^2 - 2(bb'+\Delta)qq''' + cc'q^2,\\
AS^2 &= ac'q''^2 - 2(bb'+\Delta)q'q'' + a'cq'^2,\\
AT^2 &= ac'q'''^2 - 2bc'q'q''' + cc'q'^2,\\
AU^2 &= a'cq'''^2 - 2b'cq'''q'' + cc'q''^2.
\end{aligned}$$

Il suit de là que AP^2, AQ^2, AR^2, etc. sont divisibles par mm', d'où l'on conclut facilement que Ak^2 est divisible par mm', puisque k^2 est le plus grand commun diviseur entre P^2, Q^2, R^2, etc. ; mais en substituant pour a, $2b$, c, etc. leurs valeurs $\frac{P}{n'}$, etc., ou..... $(pq'-p'q)\frac{1}{n'}$, etc. Ces équations se changeront en six autres, dans lesquelles on aura à droite les produits de la quantité $\frac{1}{nn'}(q'q''-qq''')$ par P^2, Q^2, R^2, etc ; nous laissons à effectuer ce calcul qui est très-facile. Il suit de là qu'on a $Ann' = q'q''-qq'''$.

De la même manière on obtient six autres équations dans lesquelles A est remplacé par C, et q, q', q'', q''' par p, p', p'', p''', on parvient à l'équation $Cnn' = p'p''-pp'''$, et l'on prouve que CK^2 est divisible par mm'.

Enfin on déduit encore les six équations :

$$\begin{aligned}
BP^2 &= -aa'p'q' + ab'(pq'+p'q) - ac'pq,\\
BQ^2 &= -aa'p''q'' + a'b(pq''+p''q) - a'cpq,\\
BR^2 &= -aa'p'''q''' + (bb'+\Delta)(pq'''+p'''q) - cc'pq,\\
BS^2 &= -ac'p''q'' + (bb'-\Delta)(p'q''+p''q') - a'cp'q',\\
BT^2 &= -ac'p'''q''' + bc'(p'q'''+p'''q') - cc'p'q',\\
BU^2 &= -a'cp'''q''' + b'c(p''q'''+p'''q'') - cc'p''q'',
\end{aligned}$$

d'où l'on conclut que $2Bk^2$ est divisible par mm' ; on déduira aisément par les mêmes substitutions que ci-dessus, l'équation $2Bnn' = pq'''+p'''q-p'q''-p''q'$.

Puisque Ak^2, $2Bk^2$, Ck^2 sont divisibles par mm', il s'ensuit que Mk^2 est divisible aussi par mm' ; mais on voit par les équations fondamentales que M divise les nombres aa', $2ab'$, ac', $2ba'$,

$4bb'$, $2bc'$, ca', $2b'c$, cc'; partant, am', $2bm'$, cm', qui sont respectivement les plus grands diviseurs communs des trois premiers, des trois moyens et des trois derniers, et enfin mm' qui est le plus grand commun diviseur de ces trois nombres. Donc, lorsque F est composée de f et f', c'est-à-dire lorsque $k=1$, on a nécessairement $M=mm'$. C'est la CINQUIÈME CONCLUSION.

Si le plus grand commun diviseur des nombres A, B, C est M_1, on aura $M_1=M$, quand F sera une forme propre ou dérivée d'une forme propre, et $M_1=\frac{1}{2}M$, quand F sera une forme impropre ou dérivée d'une forme impropre. Soient de même m_1, m'_1, les plus grands diviseurs communs des nombres a, b, c; a', b', c', respectivement: on aura $m_1=m$ ou $=\frac{m}{2}$, $m'_1=m'$ ou $\frac{m'}{2}$. Or il est évident que m_1^2 divise d, que m'^2_1 divise d', que parconséquent $m_1^2 m'^2_1$ divise dd' ou Δ^2, et que $m_1 m'_1$ divise Δ. Ainsi, des six équations $BP^2=$etc., etc., il suit que $m_1 m'_1$ divise Bk^2, et partant $M_1 k^2$, car il divise aussi Ak^2 et Ck^2; donc toutes les fois que F sera composée de f et f', $m_1 m'_1$ divisera M_1 lui-même, et si, dans ce cas, les deux formes f, f' sont proprement primitives ou dérivées de formes proprement primitives; on aura $m_1 m'_1=mm'=M$; donc $M_1=M$, c'est-à-dire que F sera une forme semblable. Mais si, dans le même cas, chacune des formes f, f', ou l'une des deux seulement, f par exemple, est improprement primitive ou dérivée d'une forme improprement primitive, il suit des équations fondamentales, que les nombres aa', $2ab'$, ac', $a'b$, $2bb'$, bc', $a'c$, $2b'c$, cc' sont divisibles par M_1, et partant, $m_1 m'=\frac{1}{2}mm'=\frac{1}{2}M$; donc $M_1=\frac{1}{2}M$; ainsi la forme F est improprement primitive, ou dérivée d'une forme improprement primitive. C'est la SIXIÈME CONCLUSION.

Enfin nous observons que si les neuf équations

$$\left.\begin{array}{l} P=an',\ R-S=2bn',\ U=cn',\ Q=a'n,\ R+S=2b'n,\ T=c'n, \\ Ann'=q'q''-qq''',\ 2Bnn'=pq'''+p'''q-p'q''-p''q',\ Cnn'=p'p''-pp''' \end{array}\right\}(\Omega)$$

sont supposées avoir lieu, pourvu que n, n' ne soient pas $=0$, on s'assurera facilement, par la substitution, que toutes les équations fondamentales sont satisfaites, c'est-à-dire que la forme (A, B, C) se change, par la substitution p, p', p'', p'''; q, q',

q'', q''', en le produit des formes (a, b, c), (a', b', c'), et qu'on a en outre $b^2 - ac = n^2(B^2 - AC)$, $b'^2 - a'c' = n'^2(B^2 - AC)$. Nous laissons à l'intelligence du lecteur ce calcul, qui est trop prolixe.

236. PROBLÈME. *Étant données deux formes dont les déterminans sont égaux, ou du moins comme deux nombres quarrés, trouver une forme composée de ces deux formes.*

Soient $f = (a, b, c)$, $f' = (a', b', c')$ les formes à composer; d, d' leurs déterminans; m, m' les plus grands diviseurs communs des nombres a, $2b$, c; a', $2b'$, c' respectivement, et D le plus grand commun diviseur des nombres dm'^2, $d'm^2$, pris avec le même signe que d et d'. Alors $\frac{dm'^2}{D}$ et $\frac{d'm^2}{D}$ seront des nombres positifs premiers entre eux dont le produit sera un quarré, ainsi chacun d'eux sera un quarré (n° 21). Ainsi $\sqrt{\frac{d}{D}}$ et $\sqrt{\frac{d'}{D}}$ seront des quantités rationnelles que nous représenterons par n et n', en prenant n positif ou négatif, suivant que la forme f doit entrer directement ou indirectement dans la composition, et de même à l'égard de n'. mn' et $m'n$ seront parconséquent des entiers premiers entre eux; quant à n, n', ils peuvent être fractionnaires. Cela fait, nous observerons que an', cn', $a'n$, $c'n$, $bn' + b'n$, $bn' - b'n$ sont des nombres entiers, ce qui est évident pour les quatre premiers, et qu'on démontrera pour les deux autres, comme on a démontré que R et S étaient divisibles par e.

Soient pris maintenant quatre nombres entiers K, K', K'', K''' à volonté, pourvu qu'ils ne rendent pas zéro à-la-fois les premiers membres des quatre équations suivantes, et qu'on suppose

$$\left.\begin{array}{l} K'an' + K''a'n + K'''(bn' + b'n) = \mu q, \quad -Kan' + K'''c'n - K''(bn' - b'n) = \mu q', \\ K'''cn' - Ka'n + K'(bn' - b'n) = \mu q'', \quad -K''cn' - K'c'n - K(bn' + b'n) = \mu q''' \end{array}\right\} \text{(I)},$$

de manière que q, q', q'', q''' soient des nombres entiers premiers entre eux, ce qu'on obtiendra en prenant pour μ le plus grand commun diviseur des quatre premiers membres. On pourra alors trouver quatre nombres π, π', π'', π''' tels qu'on ait

$$\pi q + \pi' q' + \pi'' q'' + \pi''' q''' = 1,$$

et cela fait on déterminera p, p', p'', p''' par les équations suivantes:

$$\left.\begin{array}{l} \pi' an' + \pi'' a' n + \pi''' (bn' + b'n) = p, \quad -\pi an' + \pi''' c' n - \pi'' (bn' - b'n) = p', \\ \pi''' cn' - \pi a' n + \pi' (bn' - b'n) = p'', \quad -\pi'' cn' - \pi' c' n - \pi (bn' + b'n) = p''' \end{array}\right\} \text{(II)};$$

enfin en posant.

$q'q'' - qq''' = Ann'$, $pq''' + p'''q - p'q'' - p''q' = 2Bnn'$, $p'p'' - pp''' = Cnn'$, A, B, C seront des nombres entiers, et la forme $(A, B, C) = F$ sera composée des formes f et f'.

En effet, 1°. des équations (I) on déduit sans peine les suivantes :

$$\left.\begin{array}{l} q'cn' - q''c'n - q'''(bn' - b'n) = 0, \quad qcn' + q'''a'n - q''(bn' + b'n) = 0, \\ q'''an' + qc'n - q'(bn' + b'n) = 0, \quad q''an' - q'a'n - q(bn' - b'n) = 0, \end{array}\right\} \text{(III)}.$$

2°. Supposons que les nombres entiers A_1, B_1, C_1, A_2, B_2, C_2, N, N' soient déterminés de manière qu'on ait

$$A_1 a + 2B_1 b + C_1 c = m, \quad A_2 a' + 2B_2 b' + C_2 c' = m', \quad Nm'n + N'mn' = 1,$$

on en tire, par la substitution des valeurs de m, m' dans la troisième équation

$$A_1 N' an' + 2B_1 N' bn' + C_1 N' cn' + A_2 Na' n + 2B_2 Nb' n + C_2 Nc' n = 1;$$

de cette équation et des équations (III), en posant

$$\begin{array}{r} -q' A_1 N' - q'' A_2 N - q'''(B_1 N' + B_2 N) = k, \\ qA_1 N' - q''' C_2 N + q''(B_1 N' - B_2 N) = k', \\ -q''' C_1 N' + qA_2 N - q'(B_1 N' - B_2 N) = k'', \\ q'' C_1 N' + q' C_2 N + q(B_1 N' + B_2 N) = k''', \end{array}$$

on trouvera facilement

$$\left.\begin{array}{l} k'an' + k''a'n + k'''(bn' + b'n) = q, \quad -kan' + k'''c'n - k''(bn' - b'n) = q', \\ k'''cn' - kc'n + k'(bn' - b'n) = q'', \quad -k''cn' - k'c'n - k(bn' + b'n) = q''' \end{array}\right\} \text{(IV)}.$$

Lorsque $\mu = 1$, ces équations ne sont pas nécessaires, et l'on peut prendre à leur place les équations (I) elles-mêmes, dont elles sont les analogues. Or si l'on substitue dans les valeurs de Ann', $2Bnn'$, Cnn' celles de q, q', q'', q''', p, p', p'', p''', on trouvera, en réduisant, que les différens termes sont des entiers multipliés les uns par nn', les autres par dn'^2 ou $d'n^2$; et que tous les termes de la valeur de $2Bnn'$ contiennent le facteur 2; or $dn'^2 = d'n^2$ et $\frac{dn'^2}{nn'} = \frac{dn'}{n} = \sqrt{dd'}$ Donc A, B, C sont des nombres entiers.

3°. En substituant les valeurs de p, p', p'', p''', dans les six

premières des équations (Ω), on trouvera qu'elles sont satisfaites à l'aide de l'équation $\pi q+\pi' q'+\pi'' q''+\pi''' q'''=1$ et des équations (III). Les trois dernières ont déjà lieu par hypothèse ; donc la forme F se changera en ff' par la substitution p, p', p'', p''', q, q', q'', q''', et son déterminant sera D, qui est égal au plus grand commun diviseur des nombres dm'^2, $d'm^2$; donc par la quatrième conclusion du n° précédent, F sera composée de f, f'.

237. THÉORÈME. *Si la forme* F *est transformable en le produit de deux formes* f, f', *et que la forme* f' *renferme la forme* f'', F *pourra aussi se transformer en* ff''.

Conservons pour les formes F, f, f' les signes du n° 235, soit $f''=(a'', b'', c'')$, et α, β, γ, δ la transformation qui change f' en f''. On voit alors sans peine que F se change en ff'' par la substitution $\alpha p+\gamma p'$, $\beta p+\delta p'$, $\alpha p''+\gamma p'''$, $\beta p''+\delta p'''$; $\alpha q+\gamma q'$, $\beta q+\delta q'$, $\alpha q''+\gamma q'''$, $\beta q''+\delta q'''$.

Représentons, pour abréger, ces coefficiens par r, r', r'', r''' ; s, s', s'', s''', et faisons $\alpha\delta-\beta\gamma=e$, en appliquant ici les équations Ω du n° 235. On trouve

$$rs'-r's=an'e,\quad rs''-r''s-(r's''-r''s')=2bn'e,\quad r''s'''-r'''s''=cn'e,$$
$$rs''-r''s=a''n,\quad rs'''-r'''s+(r's''-r''s')=2b''n,\quad r's'''-r'''s'=e''n,$$
$$s's''-ss'''=Ann'e,\quad rs'''+r'''s-r's''-r''s'=2Bnn'e,\quad r'r''-rr'''=Cnn'e ;$$

donc en représentant par d'' le déterminant de f'', et faisant $\frac{d''}{D}=n''$, on aura $n''=n'e$ parceque $\sqrt{\frac{d'}{D}}=n'$, et que $e=\pm\sqrt{\frac{d''}{d'}}$ suivant que la forme f' renferme f'' proprement ou improprement ; ainsi dans la transformation de F en ff'' la forme f'' entrera de la même manière que f' dans la transformation de F en ff', ou d'une manière différente, suivant que e sera positif ou négatif, c'est-à-dire, suivant que f' renfermera f'' proprement ou improprement.

238. THÉORÈME. *Si la forme* F' *renferme* F, *et que* F *puisse se changer en* ff', *la forme* F' *pourra aussi se changer en* ff'.

Conservons pour les formes F, f, f' les mêmes signes que plus haut, et supposons que F' se change en F par la substitution $\alpha, \beta, \gamma, \delta$, on voit facilement que F' se changera en ff' par la substitution

$$\alpha p+\beta q,\ \alpha p'+\beta q',\ \alpha p''+\beta q'',\ \alpha p'''+\beta q''';$$
$$\gamma p+\delta q,\ \gamma p'+\delta q',\ \gamma p''+\delta q'',\ \gamma p'''+\delta q'''.$$

On prouvera en outre, par un calcul semblable à celui du n° précédent, que si F' renferme F proprement, les formes f, f' entreront dans la transformation de F' en ff' de la même manière que dans la transformation de F en ff'; et que dans le cas contraire, elles entreront d'une manière inverse.

En combinant le présent théorème avec celui du n° précédent, nous obtenons le suivant, qui est plus général :

Si une forme F *est transformable en* ff', *que* f, f' *renferment les formes* g, g' *respectivement, et que* G *renferme* F, G *sera transformable en* gg'.

En effet, par le théorème du n° présent, G se changera en ff', donc par le théorème du n° précédent, G se changera en fg' et de même en gg'. Or il est évident que si les trois formes f, f', G renferment proprement les trois formes g, g', F, G se composera de la même manière en gg' que F en ff'; de même, si les trois premières renferment improprement les trois dernières; et enfin on déterminera facilement de quelle manière G doit se composer de g, g', si une des transformations est différente des deux autres.

Si les formes F, f, f' sont équivalentes aux formes G, g, g' respectivement, les premières auront les mêmes déterminans que les dernières, et (n° 161) m et m' seront pour g, g' ce qu'ils sont pour f, f'. D'où il suit, par la quatrième conclusion du n° 235, que si F est composée de f, f', G sera aussi composée de g, g', et même que la forme g entre dans cette dernière composition comme f dans la première, si F, G; f, g sont équivalentes de la même manière, ou au contraire. De même à l'égard de f' et g'.

239. Théorème. *Si la forme* F *est composée des formes* f, f', *toute forme qui pourra se transformer en* ff' *de la même manière que* F, *renfermera proprement cette dernière.*

Conservons toujours pour F, f, f' les signes du n° 235, et supposons que la forme $F'=(A', B', C')$, dont le déterminant $=D'$ se change en ff' par la substitution $p, p', p'', p'''; q, q', q'', q'''$, et

représentons pour cette composition, par P_1, Q_1, R_1, etc. les analogues de P, Q, R, etc. Dans la première on aura

$$\left.\begin{array}{l} P_1=an'_1,\ R_1-S_1=2bn'_1,\ U_1=cn'_1,\ Q_1=c'n_1,\ R_1+S_1=2b'n_1,\ T_1=c'n_1, \\ n_1n'_1A'=q'_1q''_1-q_1q'''_1,\ 2n_1n'_1B'=p'q'''_1+p'''_1q_1-p'_1q''_1-p''_1q'_1, \\ n_1n'_1C'=p'_1p''_1-p_1p'''_1 \end{array}\right\}(\Omega'),$$

n_1 et n'_1 étant les racines de $\frac{d}{D'}$ et $\frac{d'}{D'}$, et de mêmes signes que n, n'. Soit donc $\sqrt{\frac{D}{D'}}=k$ pris positivement, on aura $n_1=kn$, $n'_1=kn'$. On déduit alors des six premières équations de Ω et Ω',

$$P_1=kP,\ Q_1=kQ,\ R_1=kR,\ S_1=kS,\ T_1=kT,\ U_1=kU;$$

donc par le lemme du n° 234, on pourra déterminer α, β, γ, δ de manière qu'on ait

$$\alpha p+\beta q=p_1,\ \alpha p'+\beta q'=p'_1, \text{ etc. } \gamma p+\delta q=q_1,\ \gamma p'+\delta q'=q'_1, \text{ etc.}$$
$$\text{et } \alpha\delta-\beta\gamma=k.$$

En substituant maintenant les valeurs de p_1, p'_1, etc., q_1, q'_1, etc. dans les trois dernières équations de Ω', on trouvera, à l'aide des équations $n_1=kn$, $n'_1=kn'$, et des trois dernières de Ω,

$$A=A'\alpha^2+2B'\alpha\gamma+C'\gamma^2,\ B=A'\alpha\beta+B'(\alpha\delta+\beta\gamma)+C'\gamma\delta,$$
$$C=A'\beta^2+2B'\beta\delta+C'\delta^2.$$

ainsi la forme F' se change en F par la substitution α, β, γ, δ, qui est propre, puisque $\alpha\delta-\beta\gamma=k$, et que k est positif.

Si donc F' est aussi composée de f, f', et de la même manière que F, on aura $D'=D$, et partant F et F' sont proprement équivalentes. Plus généralement, si G est composée de g, g' de la même manière que F l'est de f, f', et que les formes f, f' soient proprement équivalentes aux formes g, g', F et G seront proprement équivalentes.

Comme le cas où les formes à composer entrent directement dans la composition est le plus simple de tous, et que les autres s'y ramènent facilement, nous nous y attacherons principalement, ensorte que lorsque nous parlerons d'une forme composée de deux autres, on devra toujours entendre que chaque forme entre directement dans la composition; il en sera de même pour les formes transformables en produits d'autres formes.

240. THÉORÈME. *Si la forme* F *est composée des formes* ff' *et* φ *de* F *et* f'', *que* F' *le soit de* f, f'' *et* φ' *de* F', f', *les formes* φ, φ' *sont proprement équivalentes.*

I. Soient.... $f=ax^2+2bxy+cy^2$, $f'=a'x'^2+2b'x'y'+c'y'^2$,
$f''=a''x''^2+2b''x''y''+c''y''^2$.

$F=AX^2+2BXY+CY^2$, $F'=A'X'^2+2B'X'Y'+CY'^2$,
$\varphi=Gt^2+2Htu+Lu^2$, $\varphi'=G't'^2+2H't'u'+L'u'^2$,

et leurs déterminans d, d', d'', D, D', Δ, Δ', qui ont tous les mêmes signes, et sont entre eux comme des quarrés. Soit m le plus grand commun diviseur des nombres a, $2b$, c, et que m', m'', M aient la même signification par rapport aux formes f', f'', F par la conclusion 4 du n° 235, D sera le plus grand commun diviseur des nombres dm'^2 et $d'm^2$, et partant Dm''^2 celui des nombres $dm'^2m''^2$, $d'^2m^2m''^2$; $M=mm'$; Δ le plus grand commun diviseur des nombres Dm''^2, $d''M^2$, ou des nombres Dm''^2 et $d''m^2m'^2$; donc Δ est le plus grand commun diviseur des trois nombres $dm'^2m''^2$, $d'm^2m''^2$, $d''m^2m'^2$. Par la même raison Δ' est le plus grand commun diviseur des trois mêmes nombres; donc puisque Δ et Δ' doivent avoir le même signe, on a $\Delta=\Delta'$, c'est-à-dire que les formes φ, φ' ont le même déterminant.

II. Supposons maintenant que F se change en ff' par la substitution

$X=pxx'+p'xy'+p''yx'+p'''yy'$, $Y=qxx'+q'xy'+q''x'y+q'''yy'$,

et φ en Ff'' par la substitution

$$t=\pi Xx''+\pi'Xy''+\pi''x''Y+\pi'''y''Y,$$
$$u=\chi Xx''+\chi'Xy''+\chi''x''Y+\chi'''y''Y,$$

et désignons par n, n', N, ν'' les racines positives de $\frac{d}{D}$, $\frac{d'}{D}$, $\frac{D}{\Delta}$, $\frac{d''}{\Delta}$. Alors, par le n° 235, on aura dix-huit équations, dont la moitié appartiendra à la transformation de F en ff'', et l'autre moitié à la transformation de φ en Ff''; la première sera $pq'-p'q=an'$, et on peut, à l'instar, former toutes les autres, que nous omettons ici. Au reste, les quantités n, n', N, ν'' sont rationnelles, mais peuvent être fractionnaires.

III. Si l'on substitue les valeurs de X, Y dans celles de t, u, on a un résultat de la forme

$$t = rxx'x'' + r'xx'y'' + r''xx''y' + r'''xy'y'' + r^{IV}x'x''y + r^{V}x'yy'' + r^{VI}x''yy' + r^{VII}yy'y'',$$
$$u = sxx'x'' + s'xx'y'' + s''xx''y' + s'''xy'y'' + s^{IV}x'x''y + s^{V}x'yy'' + s^{VI}x''yy' + s^{VII}yy'y''.$$

Le coefficient $r = p\pi + q\pi''$, le coefficient $r' = p\pi' + q\pi'''$; les quatorze autres peuvent se former de la même manière, nous ne les plaçons pas ici, parceque chacun les trouvera sans peine. Désignons maintenant les racines quarrées positives de $\frac{d}{\Delta}$ et $\frac{d'}{\Delta}$ par ν, ν', on aura $\nu = Nn'$, $\nu' = Nn$. Cela posé, on trouvera facilement les vingt-huit équations suivantes:

$$rs' - r's = aa'\nu'', \quad rs'' - r''s = aa''\nu', \quad rs''' - r'''s = ab'\nu'' + ab''\nu',$$
$$rs^{IV} - r^{IV}s = a'a''\nu, \quad rs^{V} - r^{V}s = a'b\nu'' + a'b''\nu, \quad rs^{VI} - r^{VI}s = a''b\nu' + a''b'\nu,$$
$$rs^{VII} - r^{VII}s = bb'\nu'' + bb''\nu' + b'b''\nu + \Delta\nu\nu'\nu'', \quad r's'' - r''s' = ab''\nu' - ab'\nu'',$$
$$r's''' - r'''s' = ac''\nu', \quad r's^{IV} - r^{IV}s' = a'b''\nu - a'b\nu'', \quad r's^{V} - r^{V}s' = a'c''\nu,$$
$$r's^{VI} - r^{VI}s' = bb''\nu' + b'b''\nu - bb'\nu'' - \Delta\nu\nu'\nu'', \quad r's^{VII} - r^{VII}s' = bc''\nu' + b'c''\nu,$$
$$r''s''' - r'''s'' = ac'\nu'', \quad r''s^{IV} - r^{IV}s'' = a''b'\nu - a''b\nu',$$
$$r''s^{V} - r^{V}s'' = bb'\nu'' + b'b''\nu - bb''\nu' - \Delta\nu\nu'\nu'', \quad r''s^{VI} - r^{VI}s'' = a''c'\nu,$$
$$r''s^{VII} - r^{VII}s'' = bc'\nu'' + b''c'\nu, \quad r'''s^{IV} - r^{IV}s''' = b'b''\nu - bb'\nu'' - bb''\nu' + \Delta\nu\nu'\nu'',$$
$$r'''s^{V} - r^{V}s''' = b'c''\nu - bc''\nu', \quad r'''s^{VI} - r^{VI}s''' = b''c'\nu - bc'\nu'',$$
$$r'''s^{VII} - r^{VII}s''' = c'c''\nu, \quad r^{IV}s^{V} - r^{V}s^{IV} = a'c\nu'', \quad r^{IV}s^{VI} - r^{VI}s^{IV} = a''c\nu',$$
$$r^{IV}s^{VII} - r^{VII}s^{IV} = b'c\nu'' + b''c\nu', \quad r^{V}s^{VI} - r^{VI}s^{V} = b''c\nu' - b'c\nu'',$$
$$r^{V}s^{VII} - r^{VII}s^{V} = cc''\nu', \quad r^{VI}s^{VII} - r^{VII}s^{VI} = cc'\nu'',$$

que nous désignerons par Θ, et les neuf suivantes:

$$s's'' - ss''' = a\nu'\nu''G, \quad rs''' + r'''s - r's'' - r''s' = 2a\nu'\nu''H,$$
$$r'r'' - rr''' = a\nu'\nu''L, \quad s's^{VI} - ss^{VII} - (s'''s^{IV} - s''s^{V}) = 2b\nu'\nu''G,$$
$$rs^{VII} + sr^{VII} - r's^{VI} - r^{VI}s' + r'''s^{IV} + r^{IV}s''' - r''s^{V} - r^{V}s'' = 4b\nu'\nu H,$$
$$r'r^{VI} - rr^{VII} - (r'''r^{IV} - r''r^{V}) = 2b\nu'\nu''L, \quad s^{V}s^{VI} - s^{IV}s^{VII} = c\nu'\nu''G,$$
$$r^{IV}s^{VII} + r^{VII}s^{IV} - r^{V}s^{VI} - r^{VI}s^{V} = 2c\nu'\nu''H, \quad r^{V}r^{VI} - r^{IV}r^{VII} = c\nu'\nu''L,$$

que nous désignerons par Ψ (*).

(*) On pourrait trouver dix-huit autres équations dans lesquelles a', $2b'$, c'; a'', $2b''$, c'' remplaceraient a, $2b$, c; mais nous les omettons parcequ'elles nous sont inutiles.

IV. Il serait trop long de faire ici le calcul pour ces trente-sept équations; il suffira de le placer pour quelques-unes, afin de donner un type d'après lequel on puisse trouver les autres.

1°. $rs'-r's=p^2(\pi\chi'-\pi'\chi)+(\pi\chi''-\pi''\chi-\pi'\chi''+\pi''\chi')pq+(\pi''\chi''-\pi''\chi'')q^2=\nu''(Ap^2+2Bpq+Cq^2)=\nu''aa'\ldots\ldots$ première équation.

2°. $rs''-r''s=(pq'-p'q)(\pi\chi''-\pi''\chi)=an'a''N=aa''\nu'\ldots$. deuxième équation.

3°. $rs^{VII}-r^{VII}s=(\pi\chi'-\pi'\chi)pp'''+(\pi\chi'''-\pi'''\chi)pq'''-(\pi\chi''-\pi''\chi)p'''q+(\pi''\chi'''-\pi'''\chi'')qq'''=n''(App'''+B(pq'''+p'''q)+Cqq''')+b''N(pq'''-p'''q)=n''(bb'+\sqrt{dd'})+b''N(bn+b'n')=bb'\nu''+b'b''\nu+bb''\nu'+\Delta\nu'\nu''$, puisque $\sqrt{dd'}=\Delta\nu\nu'$ (ν.III).....huitième équation de Θ. Les autres se trouveront de la même manière.

V. Des équations Θ, il suit, comme on va le voir, que les vingt-huit nombres $rs'-r's$, $rs''-r''s$, etc. n'ont aucun diviseur commun. Nous observerons d'abord qu'avec les nombres a, $2b$, c; a', $2b'$, c'; a'', $2b''$, c''; ν, ν', ν'' on peut former vingt-sept produits de trois facteurs, tels que l'un de ces facteurs étant ν, le second sera un des nombres a', $2b'$, c', et le troisième un des nombres a'', $2b''$, c''; ou bien, le premier étant ν', le second sera l'un des nombres a, $2b$, c, et le troisième un des nombres a'', $2b''$, c''; ou enfin le premier étant ν'', le second sera l'un des nombres a, $2b$, c, et le troisième un des nombres a', $2b'$, c'. Or on s'assurera aisément, d'après les équations Θ, que chacun de ces produits est égal à l'un des nombres $rs'-r's$, etc., ou à la somme de plusieurs, ou à leur différence. Si donc ces derniers nombres avaient un commun diviseur, les vingt-sept produits en auraient un. Mais il est facile de prouver, à l'aide du n° 40, par une méthode souvent employée dans ce qui précède, que ce diviseur devrait aussi diviser les nombres $\nu m'm''$, $\nu' mm''$, $\nu'' mm'$, et partant leurs quarrés, qui sont $\frac{dm'^2m''^2}{\Delta}$, $\frac{d'm^2m''^2}{\Delta}$, $\frac{d''m^2m'^2}{\Delta}$. Mais (I) Δ est le plus grand commun diviseur des trois numérateurs; donc les fractions sont premières entre elles, et n'ont parconséquent pas de diviseur commun.

VI. Tout ce que nous avons dit jusqu'à présent regarde la transformation de φ en $ff'f''$, et est tiré de celle de la forme F

en ff', et de φ en Ff''. Mais on trouvera absolument de la même manière, par les transformations de F' en ff'' et de φ' en $F'f'$, la transformation de φ' en $ff'f''$:

$$t'=px x'x''+p'xx'y''+\text{etc.} \qquad u'=\sigma xx'x''+\sigma' xx'y''+\text{etc.}$$

On en tirera, comme plus haut, vingt-huit équations que nous désignerons par Θ', et neuf que nous désignerons par Ψ'. Or sans faire le calcul, il est aisé de voir que les équations Θ' auront les mêmes seconds membres que les équations Θ, et que les équations Ψ' ne différeront des équations Ψ que par l'accent de G, H, L. Donc, puisque tous les nombres $rs'-r's$, etc., n'ont point de commun diviseur, on pourra, par le lemme du n° 234, trouver quatre nombres entiers α, β, γ, δ tels que l'on ait

$$\alpha p+\beta\sigma=r,\ \alpha p'+\beta\sigma'=r',\ \alpha p''+\beta\sigma''=r'',\ \text{etc.}$$
$$\gamma p+\delta\sigma=s,\ \gamma p'+\delta\sigma'=s',\ \gamma p''+\delta\sigma''=s'',\ \text{etc. et } \alpha\delta-\beta\gamma=1.$$

VII. De là, en substituant les valeurs de aG, aH, aL tirées des trois premières équations Ψ, et les valeurs de aG', aH', aL' tirées des trois premières équations Ψ', on s'assure aisément que l'on a

$$a(G\alpha^2+2H\alpha\gamma+L\gamma^2)=aG',\ a(G\alpha\beta+H(\alpha\delta+\beta\gamma)+L\gamma\delta)=aH',$$
$$a(G\beta^2+2H\beta\delta+L\delta^2)=aL';$$

d'où il suit, si l'on n'a pas $a=0$, que la forme φ se change en φ' par la substitution propre α, β, γ, δ.

Mais en prenant, au lieu des trois premières équations de Ψ et Ψ', les trois suivantes ou les trois dernières, on obtiendra trois équations qui ne différeront des précédentes que parcequ'il y aura $2b$ ou c à la place de a, et comme on ne peut avoir à-la-fois a, b, $c=0$, la forme φ se changera nécessairement en φ' par la substitution α, β, γ, δ.

241. Une forme telle que φ ou φ', qui naît de la composition avec une troisième, d'une forme composée de deux autres, sera dite composée de ces trois formes, et par le n° précédent, on voit qu'il n'importe pas dans quel ordre se fait la composition. On voit que de cette manière on composera une forme d'autant d'autres formes qu'on voudra, et l'on démontrerait facilement que l'ordre dans lequel ces formes sont composées est indifférent, c'est-à-dire,

que les formes composées des mêmes formes sont toujours proprement équivalentes. Or il est évident que si les formes f, f', f'', etc. sont proprement équivalentes aux formes g, g', g'', etc., la forme composée des premières est proprement équivalente à la forme composée des dernières.

242. Les propositions précédentes renferment la composition des formes dans sa plus grande généralité; passons maintenant à des applications plus particulières, par lesquelles nous n'avons pas voulu interrompre l'ordre du sujet. Nous commencerons par reprendre le problème du n° 236, que nous limiterons par les conditions suivantes: 1°. que les formes à composer aient le même déterminant, ou qu'on ait $d = d'$; 2°. que m et m' soient premiers entre eux; 3°. que la forme cherchée soit composée directement des formes f, f'. Il suit de là que m^2 et m'^2 seront aussi premiers entre eux; donc on aura $D = d = d'$, puisque D doit être le plus grand commun diviseur des nombres dm'^2 et $d'm^2$; donc $n = n' = 1$. Comme les quatre nombres K, K', K'', K''' peuvent être pris à volonté, supposons-les $= -1, 0, 0, 0$, ce qui sera toujours permis, à moins qu'on n'ait à-la-fois $a = a' = b + b' = 0$, cas dont nous ne nous occuperons parconséquent pas ici, mais qui ne peut avoir lieu que pour les formes de déterminant positif quarré. Alors μ sera le plus grand diviseur commun aux nombres $a, a', b + b'$, et les nombres π', π'', π''' doivent être pris de manière qu'on ait $\pi' a + \pi'' a' + \pi'''(b + b') = \mu$; quant à π, il reste entièrement indéterminé. On tire de là, en substituant pour p, q, p', q', etc. leurs valeurs,

$$A = \frac{aa'}{\mu^2}, \quad B = \frac{1}{\mu}(\pi aa' + \pi' ab' + \pi'' a'b + \pi'''(bb' + D)), \text{ et } C = \frac{B^2 - D}{A} \text{ (*).}$$

(*) Si l'on avait $a = a' = 1$, $b = b'$, $c = c'$, on trouverait $p = 1$, $q = 0$, $q' = 1$, $q'' = 1$, $q = 2b$, et $(\pi' + \pi'')\, a + \pi''' b = 1$; or on a

$p = \pi' + \pi'' + 2\pi''' b = 1 \ldots . p' = \pi''' c - \pi$, $p'' = \pi''' c - \pi$, $p''' = -(\pi' + \pi'') - 2\pi b$;

et l'on satisfera à l'équation de condition en prenant $\pi''' = 1$ et $\pi' + \pi'' = 1 - 2b\pi = c$, ce qui donne

$$p' = 0, \quad p'' = 0 \quad \text{et} \quad p''' = -c.$$

On a donc $X = xx' - cyy' \ldots . Y = xy' + yx' + 2byy'$; d'ailleurs $A = 1 \ldots .$ $B = \pi a'' + (\pi' + \pi'')\, ab + \pi''' (b^2 + D) = b$, $C = c$. Résultat de *Lagrange*. (Supplément à l'Algèbre d'*Euler*, p. 642). (*Note du Traducteur.*)

Ainsi dans cette solution la valeur de A ne dépend pas des nombres π, π', π'', π''', qui peuvent être déterminés d'un nombre infini de manières; à l'égard de B, il aura des valeurs différentes quand on en donnera d'autres à ces mêmes nombres, et il sera utile de chercher la liaison de ces valeurs de B.

1°. De quelque manière qu'on détermine π, π', π'', π''', les valeurs de B qui en résultent sont congrues suivant le module A. Supposons en effet qu'en faisant $\pi = \varpi$, $\pi' = \varpi'$, $\pi'' = \varpi''$, $\pi''' = \varpi'''$, on ait $B = \beta$, et qu'en faisant $\pi = \varpi + \delta$, $\pi' = \varpi' + \delta'$, $\pi'' = \varpi'' + \delta''$, $\pi''' = \varpi''' + \delta'''$ on ait $B = \beta + \Delta$, il en résultera les deux équations de condition.

$$a\delta' + a'\delta'' + (b+b')\delta''' = 0,\quad aa'\delta + ab'\delta' + a'b\delta'' + (bb'+D)\delta''' = \mu\Delta;$$

multipliant le premier membre de la seconde équation par $a\varpi' + a'\varpi'' + (b+b')\varpi'''$, et le second par μ, et retranchant du premier produit la quantité

$$(ab'\varpi' + a'b\varpi'' + (bb'+D)\varpi''')(a\delta' + a'\delta'' + (b+b')\delta'''),$$

qui est évidemment $= 0$, en vertu de la première équation, on trouvera, réduction faite,

$$\mu^2\Delta = aa'\{\mu\delta + (\overline{b'-b}.\varpi'' + c'\varpi')\delta' + (\overline{b-b'}.\varpi' + c\varpi''')\delta'' - (c'\varpi' + c\varpi'')\delta'''\},$$

et partant, $\mu^2\Delta$ est divisible par aa', ou Δ par $\frac{aa'}{\mu^2} = A$.

2°. Si l'on rend $B = \beta$ en faisant $\pi = \varpi$, $\pi' = \varpi'$, $\pi'' = \varpi''$, $\pi''' = \varpi'''$, on peut trouver pour ces nombres d'autres valeurs qui rendent B égal à un nombre quelconque donné congru à β, suivant le module A, c'est-à-dire, telles qu'on ait $B = \beta + kA$. Observons d'abord que les nombres μ, c, c', $b - b'$ ne peuvent avoir de diviseur commun, car s'ils en avaient un, il diviserait les six nombres $a, a', b+b', c, c', b-b'$, et partant, les six nombres $a, 2b, c, a', 2b', c'$, et parconséquent m et m' qui sont premiers entre eux par hypothèse. Ainsi on peut assigner quatre nombres entiers h, h', h'', h''', tels qu'on ait $h\mu + h'c + h''c' + h'''(b-b') = 1$: cela fait, si l'on prend $kh = \delta$, $k\{h''(b+b') - h'''a'\} = \mu\delta'$, $k\{h'(b+b') + h'''a\} = \mu\delta''$, $-k(h'a' + h''a) = \mu\delta'''$; il est clair que δ, δ', δ'', δ''' sont des nombres entiers, et l'on s'assurera facilement qu'on a

$$a\delta' + a'\delta'' + (b+b')\delta''' = 0,$$

$$aa'\delta + ab'\delta' + a'b\delta'' + (bb'+D)\delta''' = aa'\frac{k}{\mu}(\mu h + ch' + c'h'' + (b-b')h''') = \mu kA.$$

La première équation fait voir que $\pi+\delta$, $\pi'+\delta'$, $\pi''+\delta''$, $\pi'''+\delta'''$ sont des valeurs de π, π', π'', π''', et la seconde, que ces valeurs rendent $B=\beta+kA$.

Il suit de là que B peut toujours être déterminé de manière à tomber entre o et $A-1$, si A est positif, ou entre o et $-A-1$, si A est négatif.

243. Des équations

$$\pi'a+\pi''a'+\pi'''(b+b')=\mu, B=\frac{1}{\mu}[\pi aa'+\pi'ab'+\pi''a'b+\pi'''(bb'+D)],$$

on tire

$$B=b+\frac{a}{\mu}(\pi a'+\pi'(b'-b)-\pi'''c)=b'+\frac{a'}{\mu}(\pi a+\pi''(b-b')-\pi'''c');$$

donc $B\equiv b\ \left(\text{mod.}\ \frac{a}{\mu}\right)$, et $B\equiv b'\ \left(\text{mod.}\ \frac{a'}{\mu}\right)$. Toutes les fois que $\frac{a}{\mu}$ et $\frac{a'}{\mu}$ seront premiers entre eux, il n'y aura entre o et $A-1$ (ou entre o et $-A-1$, si $A<0$) qu'un seul nombre qui soit congru à b, suivant le module $\frac{a}{\mu}$, et à b', suivant $\frac{a'}{\mu}$. Si on le fait $=B$, et $\frac{B^2-D}{A}=C$, la forme (A, B, C) sera composée des formes (a, b, c), (a', b', c'). Dans ce cas, il n'est pas nécessaire, pour la composition, de considérer les nombres π, π', π'', π'''. Par exemple, si l'on cherche une forme composée des deux formes $(10, 3, 11)$, $(15, 2, 7)$, $a, a', b+b'$ seront respectivement $=10$, 15, 5 et $\mu=5$; donc $A=6$, $B\equiv 3$ (mod. 2) et $\equiv 2$ (mod. 3), d'où $B=5$; et la forme $(6, 5, 21)$ sera celle qu'on cherchait. Au reste, la condition que $\frac{a}{\mu}$ et $\frac{a'}{\mu}$ soient premiers entre eux, revient à ce qu'ils n'aient pas d'autre diviseur commun que le plus grand commun diviseur des trois nombres a, a', $b+b'$, ou encore que le plus grand diviseur commun des nombres a, a', divise $b+b'$.

On doit remarquer particulièrement les cas suivans :

1°. Étant proposées deux formes (a, b, c), (a', b', c') de même déterminant D, telles que le plus grand diviseur commun des nombres $a, 2b, c$ soit premier avec celui des nombres $a', 2b', c'$, et que a

soit premier avec a'; on trouvera une forme composée de ces deux-là en faisant $A = aa'$, $B \equiv b \pmod{a}$ et $\equiv b' \pmod{a'}$, $C = \frac{B^2 - D}{A}$. Ce cas aura toujours lieu quand l'une des formes à composer est une forme principale, c'est-à-dire qu'on a $a = 1$, $b = 0$, $c = -D$. On aura alors $A = a'$, B pourra être pris $= b'$, d'où l'on tirera $C = c'$; donc *une forme quelconque est toujours composée d'elle-même et de la forme principale de même déterminant.*

2°. Si deux formes opposées proprement primitives doivent être composées, par exemple, (a, b, c) et $(a, -b, c)$, on aura $\mu = a$; d'où l'on voit facilement que la forme principale $(1, 0, -D)$ est composée de ces deux formes.

3°. Étant données tant de formes qu'on voudra (a, b, c), (a', b', c'), (a'', b'', c''), etc., proprement primitives et de même déterminant D, et dont les premiers termes a, a', a'', etc. soient des nombres premiers entre eux, on trouvera une forme (A, B, C) composée de celles-là, en prenant A égal au produit des nombres a, a', a'', etc., B congru aux nombres b, b', b'', etc., suivant les modules a, a', a'', etc. respectivement, et $C = \frac{B^2 - D}{A}$. En effet, on voit facilement que $\left(aa', B, \frac{B^2 - D}{aa'}\right)$ est composée des formes (a, b, c), (a', b', c'), que $\left(aa'a'', B, \frac{B^2 - D}{aa'a''}\right)$ est composée de cette dernière et de (a'', b'', c''), etc.

4°. Réciproquement, étant donnée une forme proprement primitive (A, B, C) de déterminant D, si l'on décompose le nombre A en facteurs premiers entre eux a, a', a'', etc., et que l'on prenne les nombres b, b', b'', etc. égaux à B, ou du moins congrus à B, suivant les modules a, a', a'', etc., $c = \frac{b^2 - D}{a}$, $c' = \frac{b'^2 - D}{a'}$ $c'' = \frac{b''^2 - D}{a''}$, etc., la forme (A, B, C) sera composée des formes (a, b, c), (a', b', c'), (a'', b'', c''), etc., ou sera décomposable en ces différentes formes. On prouve sans peine que la même proposition a lieu également quand même la forme (A, B, C) serait improprement primitive ou dérivée. De cette manière on pourra décomposer toute forme en d'autres de même déterminant, dont les

les premiers termes sont tous des nombres premiers ou des puissances de nombres premiers. Cette résolution est souvent commode pour composer plusieurs formes en une.

Soient, par exemple, à composer les trois formes (3, 1, 134), (10, 3, 41), (15, 2, 27); on décomposera la seconde en les deux (2, 1, 201), (5, —2, 81); la troisième en (3, —1, 134), (5, 2, 81); et il est clair que la forme composée des cinq formes (3, 1, 134), (2, 1, 201), (5, —2, 81), (3, —1, 134), (5, 2, 81), en quelque ordre que ce soit, sera composée des trois formes données. Mais la composition de la première et de la quatrième donne (1°.) la forme principale; la composition de la première et de la cinquième la donne aussi; donc (2°.) la forme composée définitive est (2, 1, 201).

5°. Il nous semble qu'attendu l'utilité que présente ce procédé, il n'est pas inutile de lui donner ici plus de développement. L'observation précédente prouve que pour composer tant de formes proprement primitives qu'on voudra, on peut réduire la difficulté à n'avoir à composer que des formes dont les premiers termes soient des puissances de nombres premiers. Il convient de considérer surtout le cas où l'on doit composer deux formes proprement primitives (a, b, c), (a', b', c'), dans lesquelles a et a' sont des puissances d'un même nombre premier. Soit donc $a = h^{\alpha}$, $a' = h^{\alpha'}$, h étant un nombre premier, et soit $\alpha \geqslant \alpha'$, $h^{\alpha'}$ sera le plus grand diviseur commun des nombres a, a', et s'il divise $b + b'$, on rentrera dans le cas considéré au commencement de ce numéro, et (A, B, C) sera composée des formes proposées, pourvu que l'on prenne $A = h^{\alpha + \alpha'}$, $B \equiv b \pmod{h^{\alpha - \alpha'}}$, et $\equiv b' \pmod{1}$, condition qui peut évidemment s'omettre; enfin $C = \frac{B^2 - D}{A}$. Mais si $h^{\alpha'}$ ne divise pas $b + b'$, le plus grand diviseur commun des trois nombres a, a', $b + b'$ divisera $h^{\alpha'}$, et sera une puissance de $h < h^{\alpha'}$; supposons-le $= h^{\lambda}$, il faudra déterminer les nombres π', π'', π''' de manière qu'on ait

$$\pi' h^{\alpha} + \pi'' h^{\alpha'} + \pi'''(b + b') = h^{\lambda},$$

π étant pris à volonté; et la forme (A, B, C) sera composée des formes données, si l'on prend

$$A=h^{\alpha+\alpha'-2\lambda},\ B=b+h^{\alpha-\lambda}\{\pi h^{\alpha'}-\pi'(b-b')-\pi'' c\},\ C=\frac{B^2-D}{A}.$$

Mais on voit facilement que dans ce cas π' peut être pris aussi à volonté; donc en faisant $\pi=\pi'=0$, on a $B=b-\pi''' ch^{\alpha-\lambda}$, ou plus généralement $B=kA+b-\pi''' ch^{\alpha-\lambda}$ (n° précédent). Cette formule très-simple ne renferme que π''', qui est la valeur de l'expression $\frac{h^\lambda}{b+b'}$ (mod. $h^{\alpha'}$).

Soit, par exemple, à trouver une forme composée des deux formes (16, 3, 19) et (8, 1, 37), on a $h=2$, $\alpha=4$, $\alpha'=3$, $\lambda=2$. Donc $A=8$, π''' est la valeur de l'expression $\frac{4}{4}$ (mod. 8), qui est 1, d'où $B=8k-37$, ou en faisant $k=9$, $B=-1$ et $C=37$; donc $(8, -1, 37)$ est la forme cherchée.

Étant donc proposées tant de formes qu'on voudra, dont les premiers termes sont des puissances de nombres premiers, il faut examiner si quelques-uns d'entre eux sont des puissances de mêmes nombres premiers, et comparer entre elles, par la règle que nous venons de donner, les formes auxquelles ils appartiennent. De cette manière on obtiendra des formes dont les premiers termes seront encore des puissances de nombres premiers, mais de nombres premiers différens; ainsi par l'observation (3) on pourra trouver une forme composée de ces dernières.

Par exemple, étant proposées les formes

(3, 1, 47), (4, 0, 35), (5, 0, 28), (16, 2, 9), (9, 7, 21), (16, 6, 11);

de la première et de la cinquième on tire la forme (27, 7, 7); de la seconde et de la quatrième, la forme (16, −6, 11); de cette dernière et de la sixième, la forme (1, 0, 140), qui peut être négligée. Il reste les deux formes (5, 0, 28) et (27, 7, 7), qui produisent la forme (135, −20, 4), pour laquelle on peut prendre (4, 0, 35), qui lui est proprement équivalente. Ainsi (4, 0, 35) est la résultante de la composition des six formes proposées.

Au reste, on peut tirer de là plusieurs artifices utiles dans la pratique; mais nous sommes forcés de ne pas nous arrêter plus long-temps sur ce sujet, pour passer à des choses plus difficiles.

244. Si un nombre a peut être représenté par une certaine forme f, et un nombre a' par la forme f', que d'ailleurs la forme F soit transformable en ff'; on voit sans peine que le produit aa' peut être représenté par la forme F. Il suit de là que lorsque les déterminans de ces formes sont négatifs, la forme F sera positive, si f et f' sont ou toutes deux positives, ou toutes deux négatives, et négative, si l'une est positive et l'autre négative. Arrêtons-nous particulièrement sur le cas que nous avons considéré au n° précédent, où F est composée de F, f', et où F, f, f' ont le même déterminant D; supposons encore que les représentations des nombres a, a' par les formes f, f' se fassent par des valeurs premières entre elles des indéterminées, que la première appartienne à la valeur b de l'expression $\sqrt{D}$ (mod. a), et la seconde à la valeur b' de l'expression $\sqrt{D}$ (mod. a'), et que l'on prenne $c = \frac{b^2-D}{a}$, $c' = \frac{b'^2-D}{a'}$; alors (n° 168), les formes (a, b, c), (a', b', c') seront proprement équivalentes aux formes f, f', donc F sera composée de ces deux formes; mais la forme (A, B, C) sera composée des deux mêmes formes si, μ étant le plus grand commun diviseur des nombres a, a', $b+b'$, on fait $A = \frac{aa'}{\mu^2}$, $B \equiv b \left(\text{mod. } \frac{a}{\mu}\right)$, $\equiv b' \left(\text{mod. } \frac{a'}{\mu}\right)$ et $C = \frac{B^2-D}{A}$; donc cette forme sera proprement équivalente à la forme F. Or le nombre aa' se représente par la forme $Ax^2+2bxy+Cy^2$, en faisant $x=\mu$, $y=0$, dont le plus grand diviseur commun est μ; donc aa' pourra être représenté par la forme F, de manière que les valeurs des indéterminées aient un diviseur commun μ (n° 166). Donc toutes les fois que $\mu=1$, aa' pourra être représenté par F, au moyen de valeurs premières entre elles des indéterminées, et cette représentation appartiendra à la valeur B de l'expression $\sqrt{D}$ (mod. aa'), qui est congrue à b, b', suivant les modules a, a'. La condition $\mu=1$ a lieu quand a est premier avec a', ou plus généralement, quand le plus grand commun diviseur de a, a' est premier avec $b+b'$.

245. THÉORÈME. *Si la forme* f *est comprise dans le même ordre que* g, *que* f′ *soit comprise dans le même ordre que* g′; *la forme* F *composée de* f, f′ *aura le même déterminant, et sera comprise dans le même ordre que* G *composée de* g, g′.

Soient $f=(a, b, c)$, $f'=(a', b', c')$, $F=(A, B, C)$, et les déterminans d, d', D; soit m le plus grand diviseur commun des nombres a, $2b$, c, m_1 le plus grand diviseur commun des nombres a, b, c; et que m', m'_1, M, M_1 aient les mêmes significations par rapport aux f' et F respectivement. L'ordre de la forme f sera déterminé par les nombres d, m, m_1, d'où il suit que les mêmes nombres auront lieu pour la forme g; par la même raison, les nombres d', m', m'_1, seront pour la forme g' ce qu'ils sont pour la forme f'. Or (n° 235) les nombres D, M, M_1 sont déterminés par les nombres d, m, m_1; d', m', m'_1; savoir, D est le plus grand commun diviseur des nombres dm'^2 et $d'm^2$, $M=mm'$ et $M_1=m_1m'_1$ (si l'on a en même temps $m=m_1$, $m'=m'_1$), ou $=2m_1m'_1$ (si $m=2m_1$, ou $m'=2m'_1$). Comme ces propriétés de D, M, M_1, suivent de ce que F est composé de f, f', on voit sans peine que D, M, M_1 seront pour G ce qu'ils sont pour F, et que parconséquent F et G sont de même ordre.

Nous appellerons en conséquence l'ordre qui renferme la forme F, *ordre composé* de ceux qui renferment f et f'. Ainsi, par exemple, l'ordre composé de deux ordres proprement primitifs est aussi un ordre proprement primitif, et l'ordre composé d'un ordre proprement primitif et d'un ordre improprement primitif, est un ordre improprement primitif.

C'est dans le même sens que nous pourrons dire qu'un certain ordre est *composé de plusieurs autres*.

246. PROBLÈME. *Étant proposées deux formes primitives quelconques*, f, f′, *de la composition desquelles naît la forme* F, *du genre auquel appartiennent* f et f′, *déterminer le genre auquel appartient F.*

I. Considérons d'abord le cas où une des deux formes au moins, la première f par exemple, est proprement primitive, et désignons par d, d', D, les déterminans des formes f, f', F: alors D sera le plus grand commun diviseur des nombres dm'^2, d^h; m étant $=1$,

ou $= 2$, suivant que f' est proprement ou improprement primitive : dans le premier cas, F appartiendrait à un ordre proprement primitif; dans le second, à un ordre improprement primitif. Maintenant le genre de la forme F se déterminera par ses caractères particuliers, tant à l'égard des différens diviseurs premiers impairs de D, que, dans quelques cas, à l'égard des nombres 4 ou 8. Il faudra donc déterminer chacun d'eux.

1°. Si p est un diviseur premier quelconque de D, il divisera nécessairement d et d'; ainsi la relation de la forme F avec p, se trouveront parmi les caractères des formes f, f'. Or, si le nombre a peut être représenté par la forme f, et le nombre a' par f', aa' pourra l'être par F. Si donc des résidus quadratiques de p, non divisibles par p, peuvent être représentés, tant par f que par f', il pourra y en avoir de représentés par la forme F; c'est-à-dire, que si l'une et l'autre de ces deux formes a le caractère Rp, la forme F aura le même caractère. Par une raison semblable, la forme F aura le caractère $R.p$. Si les deux formes f, f' ont le caractère $N.p$; au contraire F aura le caractère $N.p$, si l'une des formes f et f' a le caractère $R.p$, et l'autre le caractère $N.p$.

2°. Si dans le caractère complet de la forme F, il entre une relation à l'égard du nombre 4, cette relation doit entrer aussi dans les caractères des formes f, f'. En effet, cela ne peut arriver que lorsque $D \equiv 0 \pmod 4$ ou $\equiv 3 \pmod 4$; quand D est divisible par 4, dm'^2 et d' le seront aussi; donc f' ne peut pas être improprement primitive (n° 226), et partant on a $m' = 1$; donc d et d' sont divisibles par 4, et le caractère de chacune d'elles renfermera la relation à l'égard de 4. Quand $D \equiv 3 \pmod 4$, D divisera d et d', les quotiens seront des nombres quarrés, et parconséquent d et d' seront ou $\equiv 0$, ou $\equiv 3 \pmod 4$, et la relation à l'égard du nombre 4 sera comprise dans les caractères des formes f, f'. Donc il suit de là, comme dans 1°., que le caractère de la forme F sera 1,4, si les deux formes f, f' ont le caractère 1,4 ou le caractère 3.4, et qu'au contraire le caractère de la forme F sera 3,4, si l'une des formes f, f' a le caractère 1,4 et l'autre le caractère 3,4.

3°. Quand D est divisible par 8, d' l'est aussi; donc f' est pro-

prement primitive, $m'=1$, et d divisible par 8; ainsi un des caractères 1,8; 3,8; 5,8; 7,8 peut se trouver parmi les caractères de F, s'il a lieu tant pour la forme f que pour la forme f'. On s'assure facilement, comme ci-dessus, que le caractère de la forme F est 1,8, si f, f' ont le même caractère; qu'il sera 3,8, si l'une des formes f, f' a le caractère 1,8 et l'autre le caractère 3,8, ou si l'une a le caractère 5,8 et l'autre le caractère 7,8; qu'il sera 5,8 si f, f' ont pour caractères l'une 1,8, l'autre 5,8 ou 3,8 et 7,8; et enfin qu'il sera 7,8, si f, f' ont pour caractères 1,8 et 7,8, ou 3,8 et 5,8.

4°. Quand $D\equiv 2 \pmod 8$, d' sera $\equiv 0$, ou $\equiv 2 \pmod 8$; partant $m'=1$, et $d\equiv 0$ ou $\equiv 2 \pmod 8$; mais comme D est le plus grand commun diviseur de d et d', ces deux nombres ne peuvent pas être tous deux divisibles par 8. Donc dans ce cas le caractère de la forme F ne pourra être que 1 et 7,8 ou 3 et 5,8, soit que les deux formes f, f' aient l'un de ces deux caractères, soit que l'une d'elles en ayant un, l'autre ait un des caractères: 1,8; 3,8; 5,8; 7,8; d'où l'on voit facilement que le caractère de la forme F se détermine par la table suivante:

	Caractères de l'une des formes f, f'	
	1 et 7,8 ou 1,8 ou 7,8	3 et 5,8 ou 3,8 ou 3,8
Caractères de l'autre forme.	Caractères résultans pour F.	
1 et 7,8	1 et 7,8	3 et 5,8
3 et 5,8	3 et 5,8	1 et 7,8

5°. On prouve de la même manière, pour $D\equiv 6 \pmod 8$, qu'on ne peut donner à la forme F l'un ou l'autre des caractères 1 et 3,8; 5 et 7,8, à moins que quelqu'un de ces caractères n'appartienne à l'une des formes f, f', et que l'autre n'ait l'un de ces mêmes caractères ou l'un des suivans: 1,8; 3,8; 5,8; 7,8; desorte qu'on déterminera le caractère de la forme F par la table suivante:

	Caractères de l'une des formes f, f'.	
	1 et 3,8 ou 1,8 ou 3,8	5 et 7,8 ou 5,8 ou 7,8
Caractères de l'autre forme.	Caractères de la forme F.	
1 et 3,8	1 et 3,8	5 et 7,8
5 et 7,8	5 et 7,8	1 et 3,8

II. Si chacune des formes f, f' est improprement primitive, D sera le plus grand commun diviseur des nombres $4d$ et $4d'$, ou $\frac{1}{4}D$ celui de d et d'; il suit de là que d, d' et $\frac{D}{4}$ sont $\equiv 1$ (mod. 4), puisque (n° 226) d et d' le sont. Mais en posant $F=(A, B, C)$, le plus grand commun diviseur des nombres A, B, C sera 2, et celui des nombres $A, 2B, C$ sera 4; donc F est une forme dérivée de la forme improprement primitive $(\frac{1}{2}A, \frac{1}{2}B, \frac{1}{2}C)$, dont $\frac{1}{4}D$ est le déterminant, et dont le genre déterminera celui de F. Comme cette forme est improprement primitive, son caractère ne renfermera point de relations avec 4 et 8, mais seulement avec les différens diviseurs premiers impairs de $\frac{1}{4}D$. Or ces diviseurs doivent nécessairement l'être de d et d'. Si les deux facteurs d'un produit sont représentables l'un par f et l'autre par f', la moitié de ce produit le sera nécessairement par la forme $(\frac{1}{2}A, \frac{1}{2}B, \frac{1}{2}C)$; on voit facilement, d'après cela, que le caractère de cette forme, à l'égard du nombre premier p diviseur de $\frac{1}{4}D$, sera $R.p$; d'abord, si $2R.p$ et que les formes f, f' aient un même caractère à l'égard de p; ensuite si l'on a $2Np$ et que les caractères des formes f, f' soient opposés à l'égard de p. Au contraire, le caractère de cette forme sera $N.p$, si f, f' ont le même caractère et qu'on ait $2N.p$, ou s'ils en ont un différent, et qu'on ait $2R.p$.

247. Par la solution du problème précédent, il est évident que si g est une forme primitive du même ordre et du même genre que f, que g' soit une forme primitive du même ordre et du même

genre que f', la forme composée de g, g' appartient au même genre que la forme composée de f, f'. On voit par là ce que signifie *un genre composé de deux ou de plusieurs autres genres*. Or on voit encore que si f, f' ont le même déterminant, que f soit une forme d'un genre principal, et que F soit composée de f, f', F sera du même genre que f', et qu'ainsi le genre principal peut toujours être omis dans la composition avec les autres genres de même déterminant. Si, toutes choses d'ailleurs égales, f n'est pas du genre principal, et que f' soit une forme primitive, F sera certainement d'un autre genre que f'. Enfin si f, f' sont des formes proprement primitives de même genre, F sera du genre principal (n° 243 (2°.) et n° 230, à la fin). Si donc une forme proprement primitive quelconque est composée avec elle-même, la forme qui résulte de la composition, et qui sera proprement primitive et de même déterminant, sera du genre principal; mais si f et f' sont toutes deux proprement primitives, de même déterminant et de genre différent, F ne pourra pas appartenir au genre principal.

248. PROBLÈME. *Étant proposées deux formes quelconques* f, f′ *dont* F *est composée; déterminer le genre de* F *d'après ceux de* f, f′.

Soit $f=(a, b, c)$, $f'=(a', b', c')$, $F=(A, B, C)$, μ le plus grand commun diviseur des nombres a, b, c, μ' celui des nombres a', b', c', de manière que f et f' soient dérivées des formes primitives $\left(\frac{a}{\mu}, \frac{b}{\mu}, \frac{c}{\mu}\right)$, $\left(\frac{a'}{\mu'}, \frac{b'}{\mu'}, \frac{c'}{\mu'}\right)$, que nous désignerons par φ, φ'; cela posé, s'il y a au moins une des formes φ, φ' qui soit proprement primitive, le plus grand commun diviseur des nombres A, B, C sera $\mu\mu'$, et F sera dérivée de la forme primitive $\left(\frac{A}{\mu\mu'}, \frac{B}{\mu\mu'}, \frac{C}{\mu\mu'}\right)=\Phi$, et le genre de F dépendra de celui de Φ; mais on voit facilement que Φ se change en $\varphi\varphi'$ par la même substitution qui change F en ff', et que parconséquent Φ est composée de φ, φ'; donc on pourra déterminer son genre par le problème du n° 246.

Mais si f et f' sont improprement primitives, le plus grand commun diviseur des nombres A, B, C sera $2\mu\mu'$, et la forme Φ, qui

qui est encore ici composée de φ, φ', est évidemment dérivée de la forme proprement primitive $\left(\frac{A}{2\mu\mu'}, \frac{B}{2\mu\nu'}, \frac{C}{2\nu\nu'}\right)$. Le genre de cette forme pourra être déterminé par le n° 246, et comme F est dérivée de la même forme, son genre sera connu par là même.

Il est évident par cette solution, que le théorème donné au n° précédent pour les formes primitives, a lieu pour des formes quelconques, savoir, si f' et g' sont des mêmes genres que f et g respectivement, la forme composée de f, f' est du même genre que la forme composée de g, g'.

249. THÉORÈME. *Si les formes* f, f′ *sont des mêmes ordres, genres et classes que* g, g′ *respectivement, la forme composée de* f *et de* f′ *est de la même classe que la forme composée de* g, g′.

Ce théorème n'est qu'une conséquence immédiate du n° 239. On voit par là ce qu'on doit entendre par *une classe composée de deux* ou *de plusieurs classes*.

Si l'on compose une classe quelconque K avec la classe principale, la classe composée sera K elle-même; ainsi dans la composition des classes de même déterminant, on peut négliger la classe principale. Or (n° 243) il naît toujours une classe principale de la composition de deux classes opposées proprement primitives; donc toute classe ambiguë étant sa propre opposée, en composant avec elle-même une classe ambiguë proprement primitive, la résultante est la classe principale de même déterminant.

La réciproque de la dernière proposition est également vraie: *Si la résultante* H *de la composition d'une classe proprement primitive* K *avec elle-même, est la classe principale de même déterminant,* K *sera nécessairement une classe ambiguë.* En effet, si K' est une classe opposée à K, la résultante des trois classes K, K, K' sera la même que celle de H et K', c'est-à-dire, sera égale à K'; mais la résultante de K et K' est H, et la résultante de H et K est K; donc K coïncide avec K', et est par-conséquent une classe ambiguë.

Or on remarquera la proposition suivante: *Si les classes* K, L *sont opposées aux classes* K′, L′ *respectivement, la classe*

composée de K, L *sera opposée à la classe composée de* K', L'. Soient les formes f, g, f', g' des classes K, L, K', L' respectivement, F la forme composée de f, g, F' la composée de f', g'; comme f' est improprement équivalente à f et g' à g, et que F est composée directement de f, g, F sera aussi composée de f', g', mais indirectement de chacune d'elles. Donc toute forme qui équivaut improprement à F, sera composée directement des formes f', g', et partant sera proprement équivalente à F' (nos 238, 239); donc F et G seront proprement équivalentes, et les classes auxquelles elles appartiennent seront opposées.

Il suit de là que la résultante d'une classe ambiguë K avec une autre classe ambiguë L est elle-même une classe ambiguë; car elle est opposée à la résultante des classes opposées à K et L, et partant à elle-même, puisque ces classes sont elles-mêmes leurs opposées.

Observons enfin qu'étant proposées deux classes quelconques K, L de même déterminant, dont la première soit proprement primitive, on peut toujours trouver une classe M de même déterminant, telle que L soit composée de K et de M. En effet, on y parviendra en prenant pour M la classe composée de L et de la classe opposée à K. On voit aussi très-facilement que cette classe est la seule qui jouisse de cette propriété, ou que des classes différentes de même déterminant, composées avec la même classe proprement primitive, donnent des classes différentes.

La composition des classes peut se désigner commodément par le signe de multiplication $\times$, de même que l'identité des classes par le signe d'égalité. Au moyen de ces signes, la proposition que nous venons d'exposer peut être présentée de la manière suivante : Si la classe K' est opposée à K, $K \times K'$ sera la classe principale de même déterminant; donc $K \times K' \times L = L$, en prenant donc $M = K' \times L$, on aura $K \times M = L$, comme on le desirait. Mais s'il y en avait une autre M' qui jouît de la même propriété, ou qu'on eût $K \times M' = L$, on aurait $K \times K' \times M = K' \times L = M$; donc $M' = M$. Si l'on compose ensemble plusieurs classes identiques, on peut exprimer la résultante en mettant en exposant le nombre de ces classes. Ainsi K^3 désignerait la même chose que $K \times K$,

K^3, que $K \times K \times K$. On pourrait employer la même notation pour les formes, mais nous nous en abstiendrons pour éviter l'ambiguité, ayant déjà donné une signification particulière à l'expression $\sqrt{M(a, b, c)}$. Nous dirons que la classe K^2 provient de la *duplication* de la classe K, K^3 de la *triplication*, etc.

250. Si D est divisible par m^2 (en supposant m positif), il y aura un ordre de formes de déterminant D, dérivé de l'ordre proprement primitif de déterminant $\frac{D}{m^2}$ (ou deux quand D est négatif, un positif et l'autre négatif). La forme $\left(m, 0, -\frac{D}{m}\right)$ appartiendra évidemment à cet ordre (à l'ordre positif), et pourra avec raison être considérée comme la forme la plus simple de cet ordre (comme la forme $\left(-m, 0, \frac{D}{m}\right)$ dans l'ordre négatif quand D est négatif). Si en outre $\frac{D}{m^2} \equiv 1 \pmod 4$, il y aura aussi un ordre de formes de déterminant D dérivé d'un ordre improprement primitif de déterminant $\frac{D}{m^2}$, auquel appartiendra évidemment la forme $\left(2m, m, \frac{m^2-D}{2m}\right)$, qui sera la plus simple. Quand D est négatif, il y aura deux ordres, et dans le négatif la forme $\left(-2m, -m, \frac{D-m^2}{2m}\right)$ sera la plus simple. Ainsi, par exemple, si l'on veut appliquer cela au cas où $m = 1$, dans les quatre ordres de formes de déterminant 45, les suivantes seront les plus simples : (1, 0, —45), (2, 1, —22), (3, 0, —15), (6, 3, —6).

Cette observation donne naissance au problème suivant :

PROBLÈME. *Etant proposée une forme quelconque* F *de l'ordre* O, *trouver une forme primitive (positive, s'il y a lieu à distinction) qui, composée avec la forme la plus simple de l'ordre* O, *ait pour résultante* F.

Soit $F = (ma, mb, mc)$ dérivée de la forme proprement primitive $f = (a, b, c)$ de déterminant d.

1°. Si f est proprement primitive, nous observerons d'abord que quand α ne serait pas premier avec $2dm$, on pourra toujours

trouver des formes équivalentes à f, et dont les premiers termes jouissent de cette propriété. Car (n° 228) on peut trouver des nombres premiers à $2dm$, et représentables par cette forme; or soit a' un tel nombre, on aura $a' = ax^2 + 2bx\gamma + c\gamma^2$, où l'on peut supposer que α, γ soient premiers entre eux; partant, on pourra déterminer deux nombres tels qu'on ait $\alpha\delta - \beta\gamma = 1$, et la forme f se changera, par la substitution α, β, γ, δ, en une forme (a', b', c') qui lui sera proprement équivalente et jouira de la propriété précitée. Maintenant, comme F et $(a'm, b'm, c'm)$ sont équivalentes, on voit qu'il suffit de considérer le cas où a est premier avec $2dm$. Alors (a, bm, cm^2) sera une forme proprement primitive, car si a, $2bm$ et cm^2 avaient un diviseur commun, il diviserait nécessairement $2dm = 2b^2m - 2acm$; elle sera de même déterminant que F, et l'on s'assurera facilement que F se change par la substitution $1, 0, -b, -cm, 0, m, a, bm$, en le produit de la forme (a, bm, cm^2), par $(m, 0, -dm)$, qui sera la plus simple de l'ordre O, à moins que la forme F ne soit négative. Il suit de là, par la quatrième conclusion du n° 235, que F est composée de $(m, 0, -dm)$ et (a, bm, cm^2); mais quand F est négative, elle se changera, par la substitution $1, 0, b, -cm; 0, -m, -a, bm$, en le produit de la forme $(-m, 0, dm)$, qui est la plus simple de cet ordre, par la forme positive $(-a, bm, -cm^2)$, et parconséquent elle sera composée de ces deux formes.

2°. Si f est une forme improprement primitive, on peut supposer que $\frac{1}{2}a$ soit premier avec $2dm$, car si cette propriété n'a pas lieu pour la forme f, on trouvera toujours une forme qui en jouisse et qui soit proprement équivalente à f. Il suit de là que la forme $(\frac{1}{2}a, bm, 2cm^2)$ est une forme proprement primitive de même déterminant que F; on s'assurera aussi facilement que F se change, par la substitution $1, 0, \frac{1}{2}(1 \mp b), -cm; 0, \pm 2m, \pm\frac{1}{2}a, (b \pm 1)m$, en le produit des formes $(\pm 2m, \pm m, \pm\frac{1}{2}(m - dm))$, $(\pm\frac{1}{2}a, bm, \pm 2cm^2)$, et que parconséquent elle est composée de ces deux formes, dont la première est la plus simple de l'ordre O, et la seconde une forme proprement primitive positive. Les signes inférieurs doivent être pris quand F est une forme négative, et les signes supérieurs dans les autres cas.

251. PROBLÈME. *Etant proposées deux formes* F, f *de même déterminant* D *et qui appartiennent au même ordre* O, *trouver une forme proprement primitive de déterminant* D, *telle que la résultante de cette forme et de* f *soit* F.

Soit φ la forme la plus simple de l'ordre O, F' et f' des formes proprement primitives de déterminant D, qui, composées avec φ, donnent F et f' respectivement, f'' une forme proprement primitive, qui, composée avec f', donne F', alors F sera composée de trois formes φ, f', f'', ou des deux f, f''.

Ainsi toute classe d'un ordre donné peut être considérée comme composée d'une classe quelconque donnée de même ordre et d'une classe proprement primitive de même déterminant.

252. THÉORÈME. *Pour un déterminant donné, les différens genres d'un même ordre contiennent un même nombre de classes.*

Supposons que les genres G, H appartiennent au même ordre, que G soit composé de n classes K, K', K'', etc. K^{n-1}, et soit L une classe quelconque du genre H; cherchons par le n° précédent une classe proprement primitive M de même déterminant, qui, composée avec K, produise L, et désignons par L', L'', etc. L^{n-1} les classes résultantes de la composition de la classe M avec les classes K', K'', K''',... K^{n-1} respectivement. Alors de la dernière observation du n° 249, il suit que toutes les classes L, L', L'', etc. L^{n-1} sont différentes, et par le n° 248 elles appartiendront toutes au même genre. Enfin, il est visible que H ne peut contenir d'autres classes, puisque toute classe de H peut être considérée comme résultante de M et d'une autre classe de même déterminant, qui sera nécessairement du genre G. Ainsi H contient, comme G, n classes différentes.

253. Le théorème précédent suppose identité d'ordre, et ne doit pas s'étendre à des ordres différens. Ainsi, par exemple, pour le déterminant —171, il y a vingt classes positives qui se distribuent en quatre ordres; dans l'ordre proprement primitif il y a deux genres, dont chacun contient six classes; dans l'ordre improprement primitif il y a deux genres composés chacun de deux classes. L'ordre dérivé de l'ordre proprement primitif de déterminant —19 ne contient qu'un genre composé de quatre classes; enfin l'ordre

dérivé de l'ordre improprement primitif de déterminant -19 ne contient qu'un seul genre composé d'une seule classe : il en est de même des classes négatives. Il est donc utile de chercher généralement la liaison des nombres de classes dans les différens ordres.

Supposons que K, L soient deux classes de même ordre (positif) O de déterminant D, et M une classe proprement primitive de même déterminant, qui, composée avec K, donne pour résultante L, telle qu'on peut la trouver par le n° 251. Dans quelques cas il peut arriver que M soit l'unique classe proprement primitive, qui, composée avec K, produise L; dans d'autres, plusieurs classes proprement primitives différentes peuvent être douées de cette propriété. Supposons généralement qu'il y ait r classes de cette espèce M, M', M'',... M^{r-1}, qui, par leur composition avec K, donnent toutes la même classe, et désignons leur ensemble par W; soit L' une autre classe de l'ordre O, et N' une classe proprement primitive, qui, composée avec L, produise L', et désignons par W' l'ensemble des classes $N'\times M$, $N'\times M'$, $N''\times M''$... $N'\times M^{r-1}$ qui seront toutes proprement primitives et différentes entre elles. Il est facile de voir que K, par sa composition avec une classe quelconque de W', produit L', d'où l'on conclut que W et W' n'ont aucune classe commune : en outre, on prouve sans peine qu'il n'y a aucune classe proprement primitive, qui, par sa composition avec K, produise L', et qui ne soit contenue dans W'. De la même manière, si L'' est une classe de l'ordre O, on trouvera r classes proprement primitives différentes, tant entre elles qu'avec les classes W et W', et dont chacune composée avec K donnera L'', et ainsi de suite pour les autres classes; mais comme toute classe proprement primitive et positive de déterminant D composée avec K, produit une classe de l'ordre O (n° 251), on déduit facilement de là, que si le nombre de toutes les classes de l'ordre est n, le nombre de toutes les classes proprement primitives (positives) de même déterminant est rn. Nous avons ainsi une règle générale : K *et* L *étant deux classes quelconques de l'ordre* O, *et* r *le nombre des classes proprement primitives de même déterminant, dont chacune produit* L *par sa composition avec* K, *le nombre*

de toutes les classes de l'ordre proprement primitif (positif) sera r *fois plus grand que celui des classes de l'ordre* O.

Comme les classes K, L peuvent être prises arbitrairement dans l'ordre O, on peut les choisir identiques, et même il sera avantageux de se servir de la classe qui contient la forme la plus simple de cet ordre, et en prenant celle-ci pour K et L, la difficulté est réduite à assigner toutes les classes proprement primitives qui, composées avec K, reproduisent K elle-même. Nous y parviendrons au moyen du théorème suivant :

254. THÉORÈME. *Si* $F=(A, B, C)$ *est la forme la plus simple de l'ordre* O *de déterminant* D, *et* $f=(a, b, c)$ *une forme proprement primitive de même déterminant; le nombre* A^2 *pourra être représenté par la forme* f, *si* F *est la résultante d'elle-même et de* f; *et réciproquement,* F *sera composée d'elle-même et de* f, *si* A^2 *peut être représenté par* f.

1°. Si F se change en fF par la substitution p, p', p'', p'''; q, q', q'', q''', on a (n° 235) $A^3=A(aq''^2-2bqq''+cq^2)$, d'où $A^2=aq''^2-2bqq''+cq^2$.

2°. Si A^2 peut être représenté par la forme f, désignons les valeurs des indéterminées qui effectuent la représentation par q'', $-q$, ou soit $A^2=aq''^2-2bqq''+cq^2$; prenons $q''a-q(b+B)=Ap$, $-qC=Ap'$, $q''(b-B)-qc=Ap''$, $-q''C=Ap'''$, $q''a-q(b-B)=Aq'$, $q''(b+B)-qc=Aq'''$. Cela fait, on s'assure aisément que F se change en fF par la substitution p, p', p'', p'''; q, q', q'', q''', pourvu que les nombres p, p', etc. soient entiers; or, par la nature de la forme la plus simple, B est 0 ou $\frac{1}{2}A$; donc $\frac{2B}{A}$ est toujours un nombre entier; il résulte encore du même principe, que $\frac{C}{A}$ est un nombre entier; donc $q'-p$, p', $q'''-p''$, p''' sont des nombres entiers; il reste donc seulement à prouver que p et p'' sont des nombres entiers. Or on a

$$p^2+\frac{2B}{A}pq=a-\frac{q^2C}{A}, \qquad p''^2+\frac{2B}{A}p''q''=c-\frac{q''^2C}{A}.$$

Si donc $B=0$, il vient $p^2=a-\frac{q^2C}{A}$, $p''^2=c-\frac{q''^2C}{A}$, et partant p et

p'' sont entiers. Mais si $B=\frac{1}{2}A$, on a $p^2+pq=a-\frac{q^2C}{A}$, $p''^2+p''q''=c-\frac{q''^2C}{A}$, d'où l'on déduit aussi facilement que p et p'' sont entiers. Donc F est composée de f et F.

255. Ainsi le problème est réduit à assigner toutes les classes proprement primitives de déterminant D, par les formes desquelles le nombre A^2 peut être représenté. Or A^2 peut évidemment être représenté par toute forme dont le premier terme est A^2 lui-même, ou le quarré d'une partie aliquote de A; mais réciproquement si A^2 peut être représenté par une forme f, en donnant aux indéterminées de cette forme les valeurs αe, γe, dont le plus grand diviseur commun est e, la forme f se changera, par la substitution α, β, γ, δ, en une forme dont le premier terme sera $\frac{A}{e^2}$, et cette forme sera proprement équivalente à f, si β, δ sont tels qu'on ait $\alpha\delta-\beta\gamma=1$; donc toute classe par les formes de laquelle A^2 pourra être représenté, renfermera des formes dont le premier terme sera A^2 ou le quarré d'une partie aliquote de A. Tout consiste donc à trouver toutes les classes proprement primitives qui renferment des formes de cette espèce; ce qui se fait de la manière suivante: Soient a, a', a'', etc. tous les diviseurs positifs de A; on cherchera toutes les valeurs de l'expression $\sqrt{D}$ (mod. a^2) comprises entre 0 et a^2-1 inclusivement, et les représentant par b, b', b'', etc., on fera $b^2-D=a^2c$, $b'^2-D=a^2c'$, $b''^2-D=a^2c''$, etc.; désignons par V l'ensemble des formes (a^2, b, c), (a^2, b', c'), etc. On voit facilement que toute classe de déterminant D qui renfermera une forme dont le premier terme soit a^2 devra contenir une forme de V, on déterminera de la même manière toutes les formes de déterminant D, dont le premier terme est a'^2 et le second compris entre 1 et a'^2-1, nous désignerons par V' l'ensemble de ces formes. On aura de même l'ensemble V'' de formes qui commencent par a''^2, etc. On rejettera de V, V', V'', etc. toutes les formes qui ne sont pas proprement primitives, on réduira les autres en classes, et s'il y en a plusieurs qui appartiennent à la même classe, on n'en retiendra qu'une par classe. On aura de cette manière toutes les classes cherchées, et leur nombre sera à l'unité comme le nombre total des classes

classes proprement primitives positives aux nombres de classes de l'ordre O.

Exemple. Soit $D=-531$, et O l'ordre positif dérivé de l'ordre improprement primitif de déterminant -59, dans lequel la forme la plus simple est $(6, 3, 90)$. On a $A=6$, $a=1$, $a'=2$, $a''=3$, $a'''=6$. V contiendra la forme $(1, 0, 531)$; V' les formes $(4, 1, 133)$, $(4, 3, 135)$; V'' les formes $(9, 0, 59)$, $(9, 3, 60)$, $(9, 6, 63)$; enfin V''' contiendra les formes $(36, 3, 15)$, $(36, 9, 17)$, $(36, 15, 21)$, $(36, 21, 27)$, $(36, 27, 35)$, $(36, 33, 45)$. De ces douze formes il y en a six à rejeter, la deuxième et la troisième de V'', la premiere, la troisième, la quatrième et la sixième de V''', qui sont toutes des formes dérivées; on trouve que les six autres appartiennent à des classes différentes; en effet, le nombre des classes proprement primitives (positives) de déterminant -531 est 18, et le nombre des classes improprement primitives positives de déterminant -59, ou le nombre des classes de déterminant -531 dérivées de celles-ci est 3, partant le premier est au second comme 6 est à 1.

256. Cette solution sera mieux éclaircie par les observations générales suivantes :

I. Si l'ordre O est dérivé de l'ordre proprement primitif, A^2 divisera D; mais si O est dérivé de l'ordre improprement primitif ou improprement primitif lui-même, A sera pair, D sera divisible par $\frac{1}{4}A^2$ et le quotient $\equiv 1 \pmod 4$. Donc le quarré de tout diviseur de A divisera D ou au moins $4D$, et dans le second cas, le quotient sera toujours $\equiv 1 \pmod 4$.

II. Si a^2 divise D, toutes les valeurs de l'expression $\sqrt{D} \pmod{a^2}$ qui tombent entre 0 et a^2-1 seront $0, a, 2a$, etc. $a(a-1)$, et partant a sera le nombre des formes de V; mais parmi elles il n'y en aura de primitives qu'autant qu'il y a de nombres premiers avec a dans les suivans : $\frac{D}{a^2}$, $\frac{D}{a^2}-1$, $\frac{D}{a^2}-4$, ... $\frac{D}{a^2}-(a-1)^2$. Ainsi quand $a=1$, V n'aura qu'une forme $(1, 0, -D)$, qui sera toujours proprement primitive. Quand $a=2$ ou une puissance de 2, la moitié de ces nombres seront pairs, l'autre

moitié impairs; ainsi V renferme $\frac{1}{2}a$ formes proprement primitives. Quand a est un autre nombre premier p, ou une puissance de ce nombre premier, on doit distinguer trois cas: 1°. si $\frac{D}{a^2}$ n'est ni divisible par p, ni résidu quadratique de p, ces nombres seront tous premiers avec a, et partant, toutes les formes de V seront proprement primitives. 2°. Si p divise $\frac{D}{a^2}$, comme depuis 0 jusqu'à $a-1$ il y a $\frac{a}{p}$ nombres divisibles par p (0 compris), et partant $\frac{p-1}{p}a$ non-divisibles, $\frac{p-1}{p}a$ sera le nombre des formes proprement primitives que contient V. 3°. Si $\frac{D}{a^2}$ est résidu quadratique de p, et non-divisible par p, comme entre np et $(n+1)p$ il y a deux valeurs de l'expression $\sqrt{\frac{D}{a^2}}\pmod{p}$, entre 1 et a il y en aura $\frac{2a}{p}$; donc il y aura $\frac{p-2}{p}a$ nombres non-divisibles par p dans la suite $\frac{D}{a^2}, \frac{D}{a^2}-1$, etc., et partant, le nombre des formes proprement primitives de V est $\frac{p-2}{p}a$. Généralement, si l'on a $a=2^{\nu}p^{\pi}q^{\chi}r^{\rho}\ldots p, q, r$, etc. étant des nombres premiers différens, le nombre de formes proprement primitives contenues dans V sera $NPQR\ldots$ où l'on doit faire $N=1$ quand $\nu=0$, et $N=2^{\nu-1}$ si $\nu>0$; $P=p^{\pi}$ si $\frac{D}{a^2}$ n'est pas résidu quadratique de p et n'est pas divisible par p, $P=(p-1)p^{\pi-1}$ quand $\frac{D}{a^2}$ est divisible par p, ou $P=(p-2)p^{\pi-1}$ quand $\frac{D}{a^2}$ est résidu de p mais non-divisible par p. Q, R, etc. se déterminent de la même manière en q, r, etc.

III. Si a^2 ne divise pas D, on aura $\frac{4D}{a^2}$ entier et $\equiv 1 \pmod{4}$; les valeurs de l'expression $\sqrt{D}\pmod{a^2}$ seront $\frac{1}{2}a, \frac{3}{2}a, \frac{5}{2}a, a^2-\frac{1}{2}a$, partant, le nombre des formes de V sera a, et parmi les formes, il y en aura autant de proprement primitives qu'il y aura de nombres premiers à a dans la suite $\frac{D}{a^2}-\frac{1}{4}, \frac{D}{a^2}-\frac{9}{4}, \frac{D}{a^2}-\frac{25}{4}, \ldots$

$\frac{D}{a^2}-(a-\frac{1}{2})^2$. Toutes les fois que $\frac{4D}{a^2}\equiv 1$, (mod. 8), tous ces nombres seront pairs, et partant V ne renfermera aucune forme proprement primitive; mais quand $\frac{4D^2}{a^2}\equiv 5$ (mod. 8), tous ces nombres seront impairs, et partant, toutes les formes seront proprement primitives, si a est 2 ou une puissance de 2. En général, il y aura dans ce cas autant de formes proprement primitives qu'il y a de nombres premiers avec a dans la suite précédente. Le nombre de ces formes sera $NPQR...$ si $a=2^\nu p^\pi q^\varkappa r^\rho...$; N étant $=2^\nu$, et P, Q, R, etc. se déterminant comme dans le cas précédent.

Nous avons ainsi fixé le nombre des formes primitives contenues dans V, V', V'', etc. Quant à la somme de ces nombres, on trouve sans peine la règle suivante : Si $A=2^\nu P'^\alpha Q'^\beta R'^\gamma... P'$, Q', R', etc. étant des nombres premiers différens, le nombre total des formes proprement primitives contenues dans V, V', V'', etc. sera $\frac{An'a'b'c'...}{2P'Q'R'...}$, où l'on doit faire $n'=1$ dans le cas où $\nu=0$, et dans celui où $\frac{4D}{A^2}\equiv 1$ (mod. 8), $n'=2$, si $\frac{D}{A^2}$ est entier et $\nu=0$, $n'=3$, si $\frac{4D}{A^2}\equiv 5$ (mod. 8) et $\nu>0$. $a'=P'$, si P' divise $\frac{4D}{A^2}$; $a'=P'\pm 1$, quand P' ne divise pas $\frac{4D}{A^2}$, en prenant le signe + ou le signe —, suivant que $\frac{4D}{A^2}$ est non-résidu ou résidu de P'. On déduit b', c', etc. de Q', R', comme a' de P. Nous omettons, pour abréger, la démonstration.

V. Quant à ce qui regarde le nombre de classes que fournissent ces formes proprement primitives, il faut distinguer les trois cas suivans :

1°. Quand D est négatif, chaque forme proprement primitive fournit une classe particulière, excepté deux cas où l'on aurait $\frac{4D}{A^2}=-4$ ou $=-3$, c'est-à-dire, $D=-A^2$ ou $=-\frac{3A^2}{4}$. Pour démontrer ce théorème, il suffit évidemment de faire voir qu'il ne peut arriver que deux formes différentes de V, V', V'', etc. soient proprement équivalentes. Supposons donc que (h^2, i, k), (h'^2, i', k'), soient deux formes proprement primitives de V, V',

V'', etc. appartenantes à la même classe, et que la première se change en la seconde par la substitution $\alpha, \beta, \gamma, \delta$, on aura les équations

$$\alpha\delta - \beta\gamma = 1, \quad h^2\alpha^2 + 2i\alpha\gamma + k\gamma^2 = h'^2, \quad h^2\alpha\beta + i(\alpha\delta + \beta\gamma) + k\gamma\delta = i'.$$

On conclut facilement de là que γ n'est certainement pas $= 0$; car on aurait $\alpha = \pm 1$, $h^2 = h'^2$, $i' \equiv i \pmod{h^2}$, et partant, les formes (h^2, i, k), (h'^2, i', k') seraient identiques contre l'hypothèse. On voit ensuite que γ est divisible par le plus grand diviseur commun des nombres h, h'; en effet, en nommant r ce diviseur, il divise $2i$ et $2i'$ (II et III), mais sera premier avec k; en outre $i^2 - i'^2$ est divisible par r^2, puisqu'on a $i^2 - i'^2 = h^2k - h'^2k'$, et l'on en déduit facilement que $i - i'$ est divisible par r. Or on a $\alpha i' - \alpha i = \beta h'^2 + \gamma k$, donc γk et partant γ est divisible par r. Enfin on a $(\alpha h^2 + \gamma i)^2 - D\gamma^2 = h^2h'^2$. Donc en posant $\alpha h^2 + \gamma i = rp$, $\gamma = rq$, p et q seront des entiers dont le dernier ne peut être nul, et l'on a l'équation $p^2 - Dq^2 = \frac{h^2h'^2}{r^2}$. Mais $\frac{h^2h'^2}{r^2}$ est le plus petit nombre divisible à-la-fois par h^2 et h'^2, parconséquent il divisera a^2 et par suite $4D$; donc $\frac{4Dr^2}{h^2h'^2}$ sera un entier négatif que nous représenterons par $-e$, il en résultera

$$p^2 - Dq^2 = -\frac{4D}{e} \quad \text{ou} \quad 4 = \left(\frac{2rp}{hh'}\right)^2 + eq^2.$$

Dans cette équation le terme $\left(\frac{2rp}{hh'}\right)^2$ étant un quarré < 4, ne peut être que 0 ou 1; dans le premier cas on a $eq^2 = 4$ et $D = -\left(\frac{hh'}{rq}\right)^2$; donc $\frac{4D}{A^2}$ est un quarré affecté du signe $-$, et partant non $\equiv 1 \pmod{4}$; ainsi O ne sera ni un ordre improprement primitif, ni un ordre dérivé d'un ordre improprement primitif. Donc $\frac{D}{A^2}$ sera entier, d'où l'on déduit facilement que e est divisible par 4; donc $q = 1$ et $D = -\left(\frac{hh'}{r}\right)^2$, et partant $\frac{A^2}{D}$ un entier; donc on a nécessairement $D = -A^2$ ou $\frac{D}{A^2} = -1$, *première exception.* Dans le second cas, on aura $eq^2 = 3$; donc $q = 1$, $e = 3$ et

$4D=-3\left(\frac{hh'}{r}\right)^2$; donc $3\left(\frac{hh'}{rA}\right)^2$ sera un entier qui ne peut être que 3, puisqu'en le multipliant par le quarré entier $\left(\frac{rA}{hh'}\right)^2$, on a 3. Donc $4D=-3A^2$ ou $\frac{4D}{A^2}=-3$, *seconde exception.* Donc dans tous les autres cas, les différentes formes proprement primitives de V, V', etc. appartiendront à des classes différentes. Quant aux cas exceptés, il suffira, pour abréger, de mettre ici le résultat, qu'on trouve sans peine, mais dont la recherche prolongerait trop cette analyse. Dans le premier cas, les formes appartiendront deux à deux à la même classe, dans le second trois à trois; donc le nombre des formes est dans celui-là double du nombre des classes, et triple dans celui-ci.

2°. Quand D est un nombre quarré positif, les différentes formes proprement primitives de V, V', V'', etc. appartiennent sans exception à des classes différentes. Supposons en effet que (h^2, i, k) et (h'^2, i', k') soient deux formes de cette espèce, et qu'elles soient équivalentes; soit $\alpha, \beta, \gamma, \delta$ la substitution propre qui change la première en la seconde. Il est clair que tous les raisonnemens de l'observation précédente, où l'on ne suppose pas D négatif, ont également lieu ici; on aura encore $\frac{4Dr^2}{h^2h'^2}$ entier, mais positif et quarré; faisons-le $=g^2$, il en résulte $\left(\frac{2rp}{hh'}\right)^2-g^2q^2=4$, ce qui est absurde; car la différence de deux quarrés ne peut être 4, à moins que le plus petit ne soit $=0$; or cette supposition est inadmissible, puisque $\gamma=rq$ ne peut être nul, et que partant q ne peut pas l'être non plus.

3°. Quand D est positif non quarré, nous ne pouvons donner de règle générale pour comparer le nombre des classes avec celui des formes. Nous pouvons seulement affirmer que le premier sera égal au second ou une partie aliquote du second. Nous avons même découvert une certaine liaison entre le quotient de ces nombres et les plus petites valeurs qui satisfont à l'équation $t^2-Du^2=A^2$; mais il serait trop long de l'expliquer ici. Mais nous ne pouvons pas décider s'il est possible dans tous les cas de connaître ce quotient à la seule inspection des nombres D, A. Nous joignons quelques exemples qu'il sera facile de multiplier à volonté.

Pour $D=13$, $A=2$, le nombre des formes proprement primitives de V, etc. est 3, qui sont toutes équivalentes et ne donnent qu'une seule classe.

Pour $D=37$, $A=2$, le nombre des formes est 3, qui appartiennent à trois classes différentes. Pour $D=588$, $A=7$, il y a 8 formes qui fournissent quatre classes. Pour $D=867$, $A=17$, il y a dix-huit formes et deux classes. Pour $D=1445$ et $A=17$, il y a également dix-huit formes, mais elles fournissent six classes.

VI. De l'application de cette théorie générale au cas où O est l'ordre improprement primitif, il résulte que le nombre de classes contenues dans cet ordre est à celui de l'ordre proprement primitif comme 1 est au nombre de classes différentes proprement primitives que donnent les trois formes $(1, 0, -D), \left(4, 1, \frac{1-D}{4}\right), \left(4, 3, \frac{9-D}{4}\right)$ Or il en résultera une seule classe quand $D\equiv 1 \pmod 8$, parceque dans ce cas la deuxième et la troisième sont improprement primitives. Mais quand $D\equiv 5 \pmod 8$, ces trois formes seront improprement primitives et donneront autant de classes différentes si D est négatif, excepté le cas où $D=-3$, dans lequel elles appartiennent à la même classe; quant au cas où D est positif de la forme $8n+5$, il appartient à ceux pour lesquels nous n'avons pas jusqu'à présent de règle générale. Nous pouvons cependant affirmer que ces trois formes donneront ou trois classes ou une seule, jamais deux; car on voit sans peine que si les formes $(1, 0, -D)$, $\left(4, 1, \frac{1-D}{4}\right), \left(4, 3, \frac{9-D}{4}\right)$ appartiennent aux classes K, K', K'', respectivement, on aura $K.K'=K'$ (n° 243, 2°), $K'.K'=K''$ (*ibid.* 5°); donc si l'on supposait $K=K'$, on aurait aussi $K''=K$; et de même si K et K'' étaient identiques, on aurait $K'=K''$; d'ailleurs on trouve $K'.K''=K$; donc si K' et K'' étaient identiques, K et K'' le seraient aussi. Ainsi les classes K, K', K'' sont toutes différentes ou toutes identiques. Par exemple, au-dessous de 600 il y a 75 nombres de la forme $8n+5$, parmi lesquels se trouvent dix-sept déterminans auxquels se rapporte le premier cas, c'est-à-dire que le nombre de classes proprement primitives est trois fois plus grand que celui des classes improprement primitives; ces déterminans sont: 37, 101, 141, 189, 197, 269, 325, 333, 349,

373, 381, 389, 397, 405, 485, 557, 573; pour les cinquante-huit autres, le second cas a lieu, c'est-à-dire qu'il y a le même nombre de classes dans l'un et l'autre ordre.

VII. Il est presque superflu d'observer que non-seulement par la recherche précédente, on peut comparer les nombres de classes des ordres différens de même déterminant, mais qu'elle est applicable à tous les déterminans différens qui sont entre eux comme des nombres quarrés; savoir, si O est un ordre quelconque de déterminant dm^2, O' un ordre de déterminant dm'^2, O pourra être comparé avec l'ordre proprement primitif de déterminant dm^2, celui-ci avec l'ordre dérivé de l'ordre proprement primitif de déterminant d, ou, ce qui revient au même pour le nombre de classes, avec ce dernier lui-même; et par une raison semblable, l'ordre O' pourra être comparé avec le même.

257. Parmi toutes les classes d'un ordre et d'un déterminant donné, les classes ambiguës demandent un plus grand développement, et la détermination de leur nombre nous conduira à beaucoup de résultats intéressans. Or il suffit de chercher ce nombre pour l'ordre proprement primitif, puisque les autres s'y ramènent facilement. Nous y parviendrons en trouvant d'abord toutes les formes ambiguës proprement primitives (A, B, C) de déterminant D, dans lesquelles $B=0$ ou $=\frac{1}{2}A$, et en déduisant ensuite de leur nombre celui de toutes les classes ambiguës proprement primitives.

1°. Toutes les formes proprement primitives $(A, 0, C)$ de déterminant D, se trouvent évidemment en prenant pour A tous les diviseurs de D, positifs et négatifs, pour lesquels $C=-\frac{D}{A}$ est premier avec A. Ainsi quand $D=1$, il y a deux formes de cette espèce : $(1, 0, -1)$, $(-1, 0, 1)$; il y en a autant quand $D=-1$, savoir, $(1, 0, 1)$, $(-1, 0, -1)$. Quand D est un nombre premier ou une puissance d'un nombre premier avec le signe $+$ ou le signe $-$, il y a quatre formes

$$(1, 0, -D),\ (-1, 0, D),\ (D, 0, -1),\ (-D, 0, 1).$$

Généralement, quand D est divisible par n nombres premiers, il y a 2^{n+1} formes de ce genre; en effet, soit $D=\pm PQR\ldots.$,

P, Q, R, etc. étant des nombres premiers différens ou des puissances de nombres premiers différens, dont le nombre est n; les valeurs de A seront: $1, P, Q, R, \ldots PQ, PR, QR, \ldots PQR\ldots$, et en général le produit d'autant de ces nombres qu'on voudra; or, par la théorie des combinaisons, le nombre total de ces produits est 2^n, mais il faut le doubler, parceque chaque valeur de A peut être prise avec le signe $+$ ou le signe $-$.

2°. On voit de même que toutes les formes proprement primitives $(2B, B, C)$ de déterminant D s'obtiennent en prenant pour B tous les diviseurs de D, pour lesquels $C = \frac{1}{2}\left(B - \frac{D}{B}\right)$ est entier et premier avec $2B$; ainsi, comme C doit nécessairement être impair, et que partant $C^2 \equiv 1 \pmod 8$; comme d'ailleurs on a $D = B^2 - 2BC = (B-C)^2 - C^2$, on aura $D \equiv 3 \pmod 4$ si B est impair, et $\equiv 0 \pmod 8$ si B est pair. Ainsi, toutes les fois que D sera congru à l'un des nombres: $1, 2, 4, 5, 6$, suivant le module 8, il n'y aura aucune forme de cette espèce.

Quand $D \equiv 3 \pmod 4$, C est entier et impair, quel que soit le diviseur de D que l'on prenne pour B; mais pour que C n'ait pas de diviseur commun avec $2B$, B doit être pris de manière que $\frac{D}{B}$ soit premier avec B: donc pour $D = -1$ il y a deux formes de cette espèce $(2, 1, 1)$, $(-2, -1, -1)$, et en général on voit facilement que si le nombre de tous les diviseurs premiers de D est n, il y aura en tout 2^{n+1} formes.

Quand $D \equiv 0 \pmod 8$, C est entier toutes les fois que l'on prend pour B un diviseur pair de $\frac{1}{2}D$; quant à la condition qui exige que C soit premier avec $2B$, on y satisfera de deux manières, 1°. en prenant pour B tous les diviseurs impairement pairs de $\frac{1}{2}D$, pour lesquels $\frac{D}{B}$ est premier avec $\frac{B}{2}$, et dont le nombre est 2^{n+1}, si le nombre total des diviseurs de D est n, et que l'on fasse attention au double signe. 2°. En prenant pour B tous les diviseurs pairement pairs de $\frac{1}{2}D$, pour lesquels $\frac{D}{2B}$ est premier avec $\frac{1}{2}B$; leur nombre est aussi 2^{n+1}; desorte qu'on a en tout pour ce cas 2^{n+2} formes. C'est-à-dire, que si l'on pose $D = \pm 2^\mu PQR$, etc.,

μ

μ étant >2 et P, Q, R, etc. des nombres premiers ou des puissances de nombres premiers impairs dont le nombre soit n, on pourra prendre, tant pour $\frac{1}{2}B$ que pour $\frac{D}{2B}$, les nombres: 1, P, Q, R, etc. et les produits de tant de ces nombres qu'on voudra, avec le signe + ou le signe —.

On peut conclure de tout ce qui précède, que si D est divisible par n nombres premiers impairs différens (où n doit être fait $=0$ si $D=\pm 1$, ± 2, ou $\pm 2^{\mu}$), le nombre de toutes les formes proprement primitives (A, B, C) dans lesquelles $B=0$ ou $=\frac{1}{2}A$ sera 2^{n+1} quand $D\equiv 1$, ou $\equiv 5 \pmod 8$, 2^{n+2} quand $D\equiv 2$, 3, 4, 6, 7 (mod. 8) (*); enfin 2^{n+3} quand $D\equiv 0 \pmod 8$. Si l'on compare ce résultat avec celui que nous avons obtenu pour le nombre des caractères possibles des formes proprement primitives de déterminant D, on verra que dans tous les cas le premier est double du dernier. Au reste, il est évident que, pour les déterminans négatifs, il y a parmi les premières formes autant de positives que de négatives.

258. Toutes les formes trouvées dans le n° précédent appartiennent évidemment à des classes ambiguës, et réciproquement dans toute classe ambiguë proprement primitive, il doit y avoir au moins une de ces formes. En effet, dans une telle classe, il y a nécessairement des formes ambiguës, et toute forme (a, b, c) ambiguë proprement primitive de déterminant D doit trouver au moins une forme qui lui soit équivalente parmi celles du n° précédent, c'est-à-dire, une forme $\left(a, 0, -\frac{D}{a}\right)$, ou une forme $\left(a, \frac{1}{2}a, \frac{1}{4}a - \frac{D}{a}\right)$, suivant que $b\equiv 0$, ou $\equiv \frac{1}{2} \pmod a$. Ainsi le problème est réduit à trouver en combien de classes ces formes peuvent se distribuer.

(*) Il est essentiel de remarquer que la contradiction qui semble se présenter ici ne provient que de ce que n n'a pas la même signification qu'à l'article 1° de ce numéro. En effet, dans le premier cas le facteur 2 ou 2^{μ} se trouve compris dans le nombre n, tandis qu'il ne l'est pas dans le second. (*Note du traducteur.*)

Si la forme $(a, 0, c)$ est comprise parmi les formes du n° précédent, la forme $(c, 0, a)$ s'y trouvera aussi et sera toujours différente de la première, excepté dans le cas où l'on aurait $a=c=\pm 1$, et partant $D=-1$, cas que nous laisserons de côté pour quelque temps. Mais comme ces formes appartiennent à la même classe, il suffit d'en conserver une, et nous rejetterons celle dont le premier terme est plus grand que le dernier; nous écarterons aussi le cas où $a=-c=\pm 1$, c'est-à-dire, où $D=1$. De cette manière, nous pouvons réduire toutes les formes $(A, 0, C)$ à moitié, et dans celles qui resteront, on aura toujours $A<\sqrt{\pm D}$.

De la même manière, si parmi les formes du n° précédent, il se rencontre la forme $(2b, b, c)$, on y trouvera aussi la forme $(4c-2b, 2c-b, c)=\left(-\frac{2D}{b}, -\frac{D}{b}, c\right)$, qui lui est proprement équivalente, mais qui n'est pas identique avec elle, excepté dans le seul cas où l'on aurait $c=b=\pm 1$ ou $D=-1$. Il suffit de garder celle de ces deux formes dont le premier terme est le plus petit: d'où il suit que toutes les formes $(2B, B, C)$ peuvent être réduites à moitié, et que dans celles qui resteront, on aura $B<\frac{D}{B}$ ou $B<\sqrt{\pm D}$. De cette manière, nous n'avons plus que la moitié de toutes les formes du n° précédent; nous en désignerons l'ensemble par W, et il ne reste plus qu'à faire voir combien ces formes fournissent de classes. Au reste, il est évident que si D est négatif, W renfermera autant de formes positives que de formes négatives.

1°. Quand D est négatif, les différentes formes de W appartiendront à des classes différentes; car toutes les formes $(A, 0, C)$ seront réduites; de même, les formes $(2B, B, C)$ seront réduites, excepté celles dans lesquelles $C<2B$; mais dans ces formes on aura $2C<2B+C$, et comme on a $B<\frac{D}{B}$, ou $<2C-B$, ou $2B<2C$, ou $B<C$, on tire de là $2C-2B<C$, ou $C-B<\frac{C}{2}$: donc la forme $(C, C-B, C)$, qui est évidemment équivalente à la forme proposée, est une forme réduite. De cette manière, on a autant de formes réduites qu'il y a de formes dans W; on voit facilement d'ailleurs qu'il n'y en aura aucunes qui soient

identiques ni opposées, excepté dans le cas où $C-B=0$, ce qui donne $C=B$ et exige que l'un et l'autre soit ± 1, et partant que $D=-1$; or nous avons déjà écarté ce cas-là : il suit de là que le nombre total des classes ambiguës proprement primitives de déterminant D (négatif) est égal au nombre de formes de W, ou à la moitié du nombre de formes du n° précédent. Quant au cas que nous avons excepté, dans lequel $D=-1$, on a aussi le même résultat par compensation; car il y a deux classes, à la première desquelles appartiennent les formes $(1, 0, 1)$, $(2, 1, 1)$, et à la seconde les formes $(-1, 0, -1)$, $(-2, -1, -1)$. Ainsi généralement pour les déterminans négatifs, le nombre de classes ambiguës proprement primitives est égal au nombre de caractères assignables pour les formes proprement primitives de ce déterminant, et le nombre de ces classes qui sont positives en est la moitié.

2°. Quand D est un nombre positif quarré h^2, on démontre facilement que toutes les formes appartiennent à des classes différentes. Mais on peut, dans ce cas, parvenir plus simplement à la solution du problème. Comme, par le n° 210, dans toute classe ambiguë proprement primitive on doit trouver une forme réduite $(a, h, 0)$, dans laquelle a est une valeur de l'expression $\sqrt{1}$ (mod. $2h$), comprise entre 0 et $2h-1$, et que cette propriété leur est particulière, on voit qu'il y aura autant de classes ambiguës proprement primitives, qu'on peut trouver de valeurs de cette expression; or on déduit sans peine, du n° 105, que le nombre de ces valeurs est 2^n, ou 2^{n+1}, ou 2^{n+2}, suivant qu'on aura $D\equiv 1$, ou $\equiv 4$, ou $\equiv 0$ (mod. 8), n désignant le nombre des diviseurs premiers impairs de D. Donc le nombre de classes ambiguës proprement primitives est toujours égal à la moitié des formes du n° précédent, ou au nombre de caractères possibles.

3°. Quand D est positif non quarré; déduisons des formes (A, B, C) contenues dans W, d'autres formes (A, B', C') en prenant $B'\equiv B$ (mod. A) et compris entre $\sqrt{D}$ et $\sqrt{D}\mp A$ (le signe supérieur ayant lieu quand A est positif, le signe inférieur quand A est négatif), et $C'=\frac{B'^2-D}{A}$. Désignons par W' l'ensemble de toutes ces formes; elles seront évidemment toutes pro-

prement primitives, ambiguës, de déterminant D et non identiques; elles seront d'ailleurs réduites: en effet, si $A<\sqrt{D}$, B' sera évidemment $<\sqrt{D}$ et positif; en outre, $B'>\sqrt{D}\mp A$, et parconséquent $A>\sqrt{D}-B'$; donc A pris positivement est compris entre $\sqrt{D}+B'$ et $\sqrt{D}-B'$. Si $A>\sqrt{D}$, B n'est pas $=0$, puisque nous avons rejeté les formes dans lesquelles ces deux circonstances étaient réunies, mais il est $=\frac{1}{2}A$; donc B' est, en grandeur, $=\frac{1}{2}A$, et il sera positif, car on a $A<2\sqrt{D}$, partant $\pm\frac{1}{2}A$ tombera entre les limites assignées à B' et sera congru à B, suivant le module A; donc $B'=\pm\frac{1}{2}A$, donc $B'<\sqrt{D}$ ou $2B'<\sqrt{D}+B'$, et parconséquent $A<\sqrt{D}+B'$: donc enfin $\pm A$ tombera nécessairement entre les limites $\sqrt{D}+B'$ et $\sqrt{D}-B'$. En outre, W' contiendra toutes les formes réduites proprement primitives et ambiguës; en effet, si (a, b, c) est une forme de cette espèce, on aura $b\equiv 0$ ou $\equiv\frac{1}{2}a$ (mod. a); dans le premier cas, on ne pourra pas avoir $b<a$, ni partant $a>\sqrt{D}$; donc la forme $\left(a, c, -\frac{D}{a}\right)$ sera certainement contenue dans W, et partant (a, b, c), qui lui correspond, le sera dans W'; dans le second on a nécessairement $a<2\sqrt{D}$, et partant la forme $\left(a, \frac{1}{2}a, \frac{1}{4}a-\frac{D}{a}\right)$ sera contenue dans W, et la forme (a, b, c), qui lui correspond, le sera dans W'. Il suit de là que le nombre des formes de W est égal au nombre de formes réduites, ambiguës et proprement primitives de déterminant D. Mais comme dans toute classe ambiguë il y a deux formes réduites ambiguës (nos 187, 194), le nombre des classes ambiguës proprement primitives de déterminant D sera la moitié du nombre des formes de W, ou la moitié du nombre de tous les caractères assignables.

259. Le nombre des classes ambiguës improprement primitives de déterminant D, est toujours égal au nombre de celles qui sont proprement primitives. Soit K la classe principale, et K', K'', etc. les autres classes ambiguës proprement primitives de même déterminant, L une classe ambiguë improprement primitive, celle, par exemple, qui contient la forme $(2, 1, \frac{1}{2}-\frac{1}{2}D)$; la classe L résultera de la composition de K avec L elle-même, et si nous nommons L', L'', etc. les classes qui proviennent de la composi-

tion de la classe L avec les classes K', K'', etc. respectivement, ces classes seront toutes improprement primitives, ambiguës et de même déterminant D. Le théorème sera donc prouvé, aussitôt que nous aurons démontré que toutes les classes L, L', L'', etc. sont différentes, et qu'il n'y a pas d'autres classes ambiguës, improprement primitives et de déterminant D. Pour y parvenir, nous distinguerons deux cas :

1°. Quand le nombre des classes improprement primitives est égal au nombre des classes proprement primitives, chacune des premières naît de la composition de la classe L avec une classe déterminée proprement primitive; d'où il suit que L, L', L'', etc. seront nécessairement toutes différentes. Mais en désignant par Λ une classe quelconque ambiguë improprement primitive de déterminant D, on peut trouver une classe proprement primitive X, telle qu'on ait $X.L = \Lambda$, et si la classe X' est opposée à la classe X, on aura aussi $X'.L = \Lambda$, puisque L et Λ sont elles-mêmes leurs opposées; donc on a nécessairement $X = X'$, et partant X est une classe ambiguë. X se trouvera donc parmi les classes K, K', K'', etc., et Λ parmi les classes L, L', L'', etc.

2°. Quand le nombre de classes improprement primitives est trois fois moins grand que celui des classes proprement primitives, soit H la classe dans laquelle est la forme $\left(4, 1, \frac{1-D}{4}\right)$, H' celle dans laquelle est la forme $\left(4, 3, \frac{9-D}{9}\right)$; H et H' seront proprement primitives, et différentes tant entre elles qu'avec la classe principale K; on a d'ailleurs $H.H' = K$, $H^2 = H'$, $H'^2 = H$. Si maintenant Λ est une classe quelconque improprement primitive de déterminant D qui résulte de la composition de la classe L avec une classe proprement primitive X, on aura aussi $\Lambda = L.X.H$, $\Lambda = L.X.H'$, et il n'y aura que les trois classes (proprement primitives et différentes) X, $X.H$, $X.H'$ qui, composées avec L, aient Λ pour résultante. Donc si Λ est une classe ambiguë et que X' soit opposée à X, on aura, comme ci-dessus, $\Lambda = L.X'$, et partant X' sera une des trois classes X, $X.H$, $X.H'$; or si $X' = X$, X' sera une classe ambiguë; si $X' = X.H$, on aura..... $K = X.X' = X^2.H = X^2.H'^2 = (X.H')^2$; donc $X.H'$ est une classe

ambiguë ; on prouverait de même qu'en supposant $X' = X.H'$, il s'ensuivrait que $X.H$ est une classe ambiguë ; d'où l'on peut conclure que Λ se trouve nécessairement parmi les classes L, L', L'', etc. Mais on voit facilement que parmi les trois classes X, $X.H$, $X.H'$, il ne peut y en avoir qu'une ambiguë. En effet, si X et $X.H$ étaient ambiguës, ou si elles étaient identiques avec leurs opposées respectives X', $H'.X'$, on aurait $X.H = X.H'$ ou $H = H'$. La même conclusion résulterait de la supposition de l'ambiguité simultanée des classes X et $X.H'$; enfin si $X.H$ et $X.H'$ étaient ambiguës ou identiques avec leurs opposées respectives $X'.H'$, $X'.H$, il en résulterait $X.H = X'.H'$, $X.H' = X'.H$, et partant $X.X'.H^2 = X.X'.H'^2$, ou $H^2 = H'^2$ et $H = H'$. Il n'y aura donc qu'une seule classe ambiguë proprement primitive qui, composée avec L, puisse produire Λ, et parconséquent toutes les classes L, L', L'', etc. seront différentes.

Le nombre des classes ambiguës d'un ordre dérivé est évidemment égal au nombre des classes ambiguës de l'ordre primitif dont il est dérivé, et pourra ainsi se déterminer par ce qui précède.

260. PROBLÈME. *La classe proprement primitive* K, *résultant de la duplication d'une classe* k *proprement primitive de même déterminant* D, *on demande toutes les classes semblables dont la duplication donne* K.

Soit H la classe principale de déterminant D, et H', H'', H''', etc. les autres classes ambiguës de ce déterminant ; désignons par k', k'', k''', etc. les classes $k.H'$, $k.H''$, $k.H'''$, etc. ; toutes les classes k', k'', etc. seront proprement primitives et différentes entre elles, et l'on voit facilement que K naît de la duplication de chacune d'elles. Or en nommant X une classe quelconque proprement primitive de déterminant D, qui produise K par sa duplication, elle sera nécessairement comprise parmi les classes k, k', k'', etc. ; en effet, en supposant $X = kh$, dans lequel h est une forme proprement primitive de déterminant D (n° 249), on aura $k^2.h^2 = K$; mais $k^2 = K$; donc $Kh^2 = K$, et partant $h^2 = H$, h est donc ambiguë et se trouvera parmi les classes H, H', H'', etc. ; donc X se trouvera parmi les classes k, k', k'', etc. Ainsi ces classes donnent la solution complète du problème.

Au reste, il est évident que dans le cas où D est négatif, il y a parmi les classes K, K', K'', etc. autant de classes positives que de négatives.

Puisque toute classe proprement primitive de déterminant D qui résulte de la duplication d'une certaine classe, peut résulter de la duplication d'autant de classes semblables qu'il y a de classes proprement primitives ambiguës de déterminant D, il est évident que si le nombre des classes proprement primitives est r, et que le nombre des classes ambiguës proprement primitives soit n, on aura $\frac{r}{n}$ pour le nombre des classes proprement primitives de déterminant D qui peuvent résulter de la duplication de classes de la même espèce. On trouve le même résultat pour les déterminans négatifs, en restreignant la signification de r et n aux classes positives seulement. Par exemple, pour $D=-161$, le nombre des classes proprement primitives est 16, celui des classes ambiguës 4; partant, le nombre de classes proprement primitives qui peuvent résulter de la duplication d'une classe proprement primitive est nécessairement 4, et l'on trouve effectivement que toutes les classes du genre principal sont douées de cette propriété; savoir, la classe principale (1, 0, 161), qui naît de la duplication des quatre classes ambiguës; la classe (2, 1, 18), de la duplication des classes (9, 1, 18), (9, —1, 18), (11, 2, 15), (11, —2, 15); la classe (9, 1, 18), de la duplication des classes (3, 1, 54), (6, 1, 27), (5, —2, 33), (10, 3, 17); enfin la classe (9, —1, 18), de la duplication des classes (3, —1, 54), (6, —1, 27), (5, 2, 33), (10, —3, 17).

261. THÉORÈME. *La moitié des caractères assignables, pour un déterminant positif non quarré, peut n'appartenir à aucun genre proprement primitif, et pour un déterminant négatif, à aucun genre proprement primitif positif.*

Soit m le nombre de tous les genres proprement primitifs, positifs s'il y a lieu, de déterminant D; k le nombre des classes de chaque genre, km sera (n° 252) le nombre total des classes proprement primitives, n le nombre de tous les caractères différens assignables pour le déterminant D. Alors, par le n° 258, le nombre de toutes les classes ambiguës proprement primitives sera

$\frac{n}{2}$; donc par le n° précédent le nombre de toutes les classes proprement primitives qui peuvent résulter de la duplication de classes semblables est $\frac{2km}{n}$; mais (n° 247) toutes ces classes appartiennent au genre principal qui contient un nombre k de classes; si donc toutes les classes du genre principal peuvent provenir de la duplication de quelque classe, ce que nous prouverons par la suite, on aurait $\frac{2km}{n} = k$ ou $m = \frac{n}{2}$. Mais il est certain que l'on ne peut avoir $\frac{2km}{n} > k$ ni parconséquent $m > \frac{n}{2}$. Ainsi, puisque le nombre des genres proprement primitifs ne peut être plus grand que la moitié du nombre des caractères assignables, il y a au moins la moitié de ces derniers qui ne répondent à aucun genre. Au reste, il faut bien remarquer qu'il ne suit pas encore de là, que les genres proprement primitifs répondent en effet à la moitié de ces caractères; mais nous pourrons, plus bas, tirer cette vérité des propriétés les plus abstraites des nombres.

Comme pour un déterminant négatif, il y a autant de genres négatifs que de positifs, il est clair qu'il n'y a pas plus de la moitié de tous les caractères assignables qui puissent appartenir à des genres proprement primitifs négatifs, nous reviendrons plus bas sur ce sujet, ainsi que sur les genres improprement primitifs. Nous finirons en observant que le théorème n'est pas applicable aux déterminans positifs quarrés, pour lesquels on peut voir sans peine que chaque caractère répond effectivement à un genre.

262. Ainsi, lorsque pour un déterminant donné, non quarré, il ne peut y avoir que deux caractères, il n'y a qu'un genre proprement primitif (positif), qui est nécessairement le genre principal. Cela arrive pour les déterminans -1, $+2$, -2, -4, les nombres premiers de la forme $4n+1$, et les nombres premiers de la forme $4n+3$ pris négativement, enfin pour toutes les puissances impaires de nombres premiers de la forme $4n+1$, prises positivement et pour toutes les puissances des nombres premiers de la forme $4n+3$, prises positivement ou négativement, suivant que les exposans sont pairs ou impairs. Nous pouvons déduire de là une nouvelle démonstration, non-

non-seulement pour le théorème fondamental, mais encore pour les autres théorèmes de la section précédente, relatifs aux résidus -1, $+2$, -2, basée sur des principes tout-à-fait différens, et non moins élégante que la première. Nous ne nous occuperons pas du déterminant -4 et de ceux qui sont des puissances de nombres premiers, parcequ'ils n'apprennent rien de nouveau.

Pour le déterminant -1, il n'y a aucune forme positive dont le caractère soit 3,4; pour le déterminant 2, il n'y a absolument aucune forme dont le caractère soit 3 et 5,8; pour le déterminant -2, il n'y a aucune forme positive dont le caractère soit 5 et 7,8. Pour le déterminant p, si p est un nombre de la forme $4n+1$, ou pour le déterminant $-p$, si p est un nombre de la forme $4n+3$, aucune forme proprement primitive (positive dans le dernier cas) n'aura le caractère Np. Cela posé, nous démontrons comme il suit le théorème fondamental, et les autres précités:

1°. -1 est non-résidu de tout nombre positif de la forme $4n+3$. En effet, si -1 est résidu d'un tel nombre A, en faisant $-1=B^2-AC$, (A, B, C) serait une forme de déterminant -1, dont le caractère serait 3,4.

2°. -1 est résidu de tout nombre premier p de la forme $4n+1$; car le caractère de la forme $(-1, 0, p)$, comme celui de toutes les formes de déterminant p, sera Rp, donc $-1R.p$.

3°. $+2$ et -2 sont résidus de tout nombre premier p de la forme $8n+1$; car les formes $\left(8, 1, \frac{1-p}{8}\right)$, $\left(-8, 1, \frac{p-1}{8}\right)$ ou les formes $\left(8, 3, \frac{9-p}{8}\right)$, $\left(-8, 3, \frac{p-9}{8}\right)$ seront proprement primitives de déterminant p, suivant que n est impair ou pair; donc leur caractère est Rp; donc $8Rp$ et $-8Rp$; d'où (n° 98) $2Rp$ et $-2Rp$.

4°. $+2$ est non-résidu de tout nombre de la forme $8n+3$ ou $8n+5$; car s'il était résidu d'un tel nombre A, il y aurait une forme (A, B, C) de déterminant 2 dont le caractère serait 3 et 5,8.

5°. De même -2 est non-résidu de tout nombre de la forme

$8n+5$, $8n+7$; sans quoi il y aurait une forme (A, B, C) de déterminant -2 dont le caractère serait 5 et 7,8.

6°. -2 est résidu de tout nombre premier p de la forme $8n+3$. On peut prouver cette proposition de deux manières. D'abord, 2 étant $N.p$ et -1 aussi, on aura nécessairement (n° 98) $-2Rp$. Ensuite si l'on considère le déterminant $+2p$, pour lequel il y a quatre caractères assignables: $R.p$, 1 et 3,8; $R.p$, 5 et 7,8; $N.p$, 1 et 3,8; $N.p$, 5 et 7,8; la moitié au moins ne répond à aucun genre. Or la forme $(1, 0, -2p)$ a le premier caractère, la forme $(-1, 0, 2p)$ a le quatrième; donc le deuxième et le troisième doivent être rejetés. Ainsi, comme le caractère de la forme $(p, 0, -2)$, relativement au nombre 8, est 1 et 3,8, son caractère, relativement à p, ne pourra être que Rp; donc $-2Rp$.

7°. 2 est résidu de tout nombre premier p de la forme $8n+7$; on peut de même prouver cette proposition de deux manières. D'abord, -2 étant non-résidu de p et -1 aussi, on a nécessairement $+2Rp$. Ensuite, comme l'une ou l'autre des formes $\left(8, 1, \frac{1+p}{8}\right)$, $\left(8, 3, \frac{9+p}{8}\right)$ est proprement primitive de déterminant $-p$, suivant que n est pair ou impair, son caractère sera $R.p$, donc $8R.p$, et partant $2Rp$.

8°. Tout nombre premier p de la forme $4n+1$ est non-résidu de tout nombre impair q qui n'est pas résidu de p. Car il est clair que si p était résidu de q, il y aurait une forme proprement primitive de déterminant p dont le caractère serait $N.p$.

9°. De la même manière, si un nombre quelconque impair q est non-résidu d'un nombre premier p de la forme $4n+3$, $-p$ sera non-résidu de q; autrement il y aurait une forme positive, proprement primitive, et de déterminant $-p$ dont le caractère serait $N.p$.

10°. Tout nombre premier p de la forme $4n+1$ est résidu de tout autre nombre premier q qui est résidu de p. En effet, si q est aussi de la forme $4n+1$, cette proposition est une suite de la huitième; mais si q est de la forme $4n+3$, $-q$ sera résidu de p par la deuxième proposition, et partant, par la neuvième, $pR.q$.

11°. Si un nombre premier quelconque q est résidu d'un nombre premier p de la forme $4n+3$, $-p$ sera résidu de q; en effet, si q est de la forme $4n+1$, il suit de la proposition 8 que $pR.q$, et partant, par la deuxième, $-pR.q$; mais le cas où q est de la forme $4n+3$ se soustrait à cette méthode; cependant on peut facilement le traiter, par la considération du déterminant $+pq$; car, des quatre caractères assignables pour ce déterminant: $R.p, R.q$; $R.p, N.q$; $N.p, R.q$; $N.p, N.q$, il n'y en a que deux qui appartiennent à des genres, et les formes $(1, 0, -pq)$, $(-1, 0, pq)$ ayant pour caractères, la première Rp, Rq, la seconde Np, Nq, les deux autres n'appartiennent à aucun genre. Ainsi, comme le caractère de la forme $(q, 0, -p)$ est par hypothèse $R.p$, le caractère de la même forme, à l'égard du nombre q, doit être $R.q$, et partant $-pR.q$.

Si l'on suppose, dans la huitième et la neuvième proposition, que q désigne un nombre premier, et qu'on les réunisse à la dixième et à la onzième, on aura la démonstration complète du théorème fondamental de la section précédente.

263. Après avoir confirmé le théorème fondamental par une nouvelle démonstration, nous allons nous occuper de distinguer cette moitié des caractères, auxquels nous avons vu qu'il ne répond aucunes formes proprement primitives positives pour un déterminant quelconque non-quarré. Nous y parviendrons d'autant plus facilement que les élémens de cette discussion sont déjà renfermés dans les recherches des n°s 147—150. Soit e^2 le plus grand quarré qui puisse diviser le déterminant proposé D, et $D=D'e^2$, desorte que D' ne renferme aucun facteur quarré. Soient encore a, b, c, etc. tous les diviseurs premiers impairs de D', D' sera, abstraction faite du signe, le produit de ces diviseurs, ou le double de ce produit. Désignons par ω l'ensemble des caractères particuliers $N.a, N.b, N.c$, etc., seul quand $D'\equiv 1 \pmod 4$, et en y joignant le caractère 3,4, quand $D'\equiv 3$ et que e est impair ou impairement pair; ou en y joignant les caractères 3,8 et 7,8, quand $D'\equiv 3$, et que e est pairement pair; en y joignant le caractère 3 et 5,8, ou les deux 3,8 et 5,8, quand $D'\equiv 2 \pmod 8$, et que e est impair ou pair, ou les deux 5,8 et 7,8, quand $D'\equiv 6 \pmod 8$, et que e est pair ou impair. Cela posé, il ne

répondra aucun genre proprement primitif (positif) à tous les caractères complets qui renfermeront un nombre impair des caractères particuliers ω. Dans tous les cas, les caractères particuliers qui expriment la relation à l'égard de diviseurs de D qui ne sont pas diviseurs de D', n'influent pas sur la possibilité ou l'impossibilité des genres. Or, par la théorie des combinaisons, on voit aisément que l'on exclut effectivement la moitié de tous les caractères complets assignables.

La démonstration s'établit de la manière suivante :

Des principes de la section précédente, ou des théorèmes que nous venons de démontrer pour la seconde fois, on déduit sans peine que si p est un nombre premier impair et positif qui ne divise pas D, et auquel s'applique un des caractères rejetés, D' renfermera un nombre impair de facteurs qui sont non-résidus de p, et que parconséquent D', et par suite D, sera non-résidu de p. Or on voit facilement (n° 228) qu'on ne peut supposer l'existence d'un quelconque des caractères rejetés, et à-la-fois que ce caractère n'appartienne à aucun facteur d'un produit de tant de nombres premiers avec D qu'on voudra; d'où, réciproquement, il est clair que tout nombre impair positif premier avec D, auquel convient un des caractères rejetés, renfermera nécessairement un facteur premier auquel le caractère appartienne, et que partant D est non-résidu de ce nombre. Si donc il existait une forme proprement primitive (positive) de déterminant D auquel répondît ce caractère, D serait non-résidu de tout nombre positif impair premier avec lui, qui pourrait être représenté par cette forme, ce qui est contradictoire avec le théorème du n° 154.

On peut prendre pour exemple les classifications données aux n°s 230 et 231. Chacun pourra d'ailleurs en augmenter le nombre à volonté.

264. De cette manière, tous les caractères assignables pour un déterminant donné se divisent en deux espèces P, Q, dont chacune est composée d'un même nombre, et de manière qu'aucune forme proprement primitive ne puisse avoir un des caractères de Q; mais quant à P, jusqu'à présent rien n'empêche que chacun des caractères qui y sont contenus n'appartienne à des formes

semblables. A l'égard de ces deux espèces de caractères, on remarquera la proposition suivante, qui se déduit facilement de la nature même de ces caractères : *Si l'on compose un caractère de* P *avec un caractère de* Q (en feignant qu'il existe des genres qui répondent à cette espèce de caractère, et y appliquant ce qui a été dit n° 246) *on trouvera un caractère de* Q; *si l'on compose deux caractères de* P, *ou deux caractères de* Q, *le caractère résultant appartient à* P. A l'aide de ce théorème, on peut aussi exclure la moitié des caractères pour les genres négatifs et improprement primitifs, de la manière suivante :

1°. Pour le déterminant négatif D, les genres négatifs sont contraires aux genres positifs, c'est-à-dire, que les caractères de P n'appartiendront à aucun genre négatif, et que ces genres n'auront que des caractères de l'espèce Q. En effet, quand $D' \equiv 1 \pmod 4$, $-D'$ sera un nombre positif de la forme $4n+3$, et parconséquent parmi les nombres a, b, c, etc. il y en aura un nombre impair de la forme $4n+3$, de chacun desquels -1 sera non-résidu, d'où il suit que le caractère complet de la forme $(-1, 0, D)$ renferme un nombre impair des caractères particuliers de ω, ou qu'il appartient à Q. Quand $D' \equiv 3 \pmod 4$, par la même raison, entre les nombres a, b, c, etc., il n'y en aura aucun, ou il y en aura un nombre pair de la forme $4n+3$; mais comme dans ce cas le caractère complet de la forme $(-1, 0, D)$ renferme l'un ou l'autre des deux caractères particuliers 3,8 ou 7,8, il est clair que ce caractère complet appartient encore à Q. On obtient sans peine la même conclusion dans les autres cas, desorte que le caractère de la forme négative $(-1, 0, D)$ est toujours compris dans Q. Mais comme cette forme, composée avec une autre forme quelconque proprement primitive et négative, donne pour résultante une forme semblable positive, on voit facilement qu'aucune forme proprement primitive négative ne peut avoir un des caractères de P.

2°. On prouve de même, pour les genres improprement primitifs positifs, que la chose a lieu comme pour les genres proprement primitifs, ou d'une manière contraire, suivant que $D \equiv 1$ ou $\equiv 5 \pmod 8$. Car dans le premier cas, on aura aussi $D' \equiv 1$

(mod. 8); d'où l'on conclut facilement que parmi les nombres a, b, c, etc., il n'y aura aucun nombre de la forme $8n+3$, et de la forme $8n+5$, ou qu'il y en aura un nombre pair, puisque le produit de tant de nombres impairs qu'on voudra, parmi lesquels les facteurs des formes $8n+3$ et $8n+5$ sont pris ensemble en nombre impair, est toujours $\equiv 3$ ou $\equiv 5$ (mod. 8), et que le produit a, b, c, etc. doit être égal à D' ou à $-D'$. Il suit de là que le caractère complet de la forme $\left(2, 1, \frac{1-D}{2}\right)$ ne renferme aucun caractère de ω, ou en renferme un nombre pair, et que partant il appartient à P. Maintenant, comme toute forme positive, improprement primitive et de déterminant D peut être considérée comme composée de $\left(2, 1, \frac{1-D}{2}\right)$ et d'une forme positive proprement primitive et de même déterminant D, on voit qu'aucune forme positive improprement primitive ne peut avoir un des caractères de Q. Dans le second cas, où $D \equiv 5$ (mod. 8), au contraire, D' qui sera aussi $\equiv 5$ renfermera nécessairement un nombre impair de facteurs de la forme $8n+3$, et de la forme $8n+5$, d'où l'on conclut que le caractère de la forme $\left(2, 1, \frac{1-D}{2}\right)$, et partant celui de toute forme positive improprement primitive de déterminant D, appartient à Q, et qu'il n'y en a aucun qui se trouve dans P.

3°. Enfin, pour le déterminant négatif, les genres improprement primitifs négatifs sont encore contraires aux positifs; c'est-à-dire qu'ils n'auront aucun des caractères de P ou de Q, suivant que $D \equiv 1$ ou $\equiv 5$ (mod. 8), ou suivant que $-D$ est de la forme $8n+7$, ou $8n+3$. On déduit facilement cette proposition de ce que la forme $(-1, 0; D)$, dont le caractère est compris dans Q, composée avec les formes improprement primitives et négatives de même déterminant, donne des formes improprement primitives et positives; et que parconséquent, quand on exclut pour ces dernières les caractères renfermés dans Q, on doit exclure pour les premières les caractères renfermés dans P, et réciproquement.

265. Les recherches faites aux n°s 257, 258, sur le nombre des classes ambiguës, et qui servent de base à tout ce qui précède, peuvent fournir beaucoup d'autres résultats très-dignes d'attention,

que nous sommes forcés de supprimer ; cependant nous ne pouvons passer sous silence le suivant, qui est remarquable par son élégance. Nous avons fait voir que pour un déterminant positif p, qui est un nombre premier de la forme $4n+1$, il n'y avait qu'une classe ambiguë proprement primitive ; ainsi toutes les formes ambiguës proprement primitives de ce déterminant, sont proprement équivalentes entre elles. Si donc b est le nombre entier immédiatement au-dessous de $\sqrt{p}$, et que l'on fasse $p - b^2 = a'$, les formes $(1, b, -a')$, $(-1, b, a')$ seront proprement équivalentes ; et partant, comme elles sont évidemment toutes les deux réduites, l'une sera contenue dans la période de l'autre. En attribuant à la première l'indice o dans sa période, celui de la seconde sera nécessairement impair, puisque leurs termes extrêmes sont de différens signes; supposons-le $= 2m+1$. On voit facilement que si les formes dont les indices sont 1, 2, 3, etc., sont respectivement

$$(-a', b', a''),\ (a'', b'', -a'''),\ (-a''', b''', a^{IV}),\ \text{etc.};$$

celles dont les indices sont $2m$, $2m-1$, $2m-2$, $2m-3$, etc., seront

$$(a', b, -1),\ (-a'', b', a'),\ (a''', b'', -a''),\ (-a^{IV}, b''', a'''),\ \text{etc.}$$

Il suit de là que si la forme dont l'indice est m, est (A, B, C), la même sera $(-C, B, -A)$; donc $C = -A$ et $p = B^2 + A^2$; donc tout nombre de la forme $4n+1$ est décomposable en deux quarrés, proposition que nous avons déjà démontrée (n° 182), mais par des principes tout-à-fait différens. Et nous pouvons parvenir à cette décomposition d'une manière uniforme, en développant la période de la forme réduite dont le premier terme est 1, et dont le déterminant est le nombre à partager, jusqu'à ce que nous trouvions une forme dont les deux termes extrêmes soient égaux et de signe contraire. Ainsi, par exemple, pour $p = 233$, on a

$$(1, 15, -8),\ (-8, 9, 19),\ (19, 10, -7),\ (-7, 11, 16),$$
$$(16, 5, -13),\ (-13, 8, 13),$$

d'où $233 = 64 + 169$. Au reste, il est clair que la forme $(A, B, -A)$ devant être proprement primitive, A sera nécessairement impair, et partant, B pair. Comme pour un déterminant

positif p qui est un nombre premier de la forme $4n+1$, il n'y a non plus qu'une seule ambiguë dans l'ordre improprement primitif; il est clair que si g est le nombre impair immédiatement au-dessous de $\sqrt{p}$, et qu'on fasse $p-g^2=4h$, les formes réduites $(2, g, -2h)$, $(-2, g, 2h)$ sont proprement équivalentes, et partant, l'une doit être comprise dans la période de l'autre: de là, par des raisonnemens absolument semblables aux précédens, on conclut que dans la période de la forme $(2, g, -2h)$, il se trouvera une forme dont les termes extrêmes sont égaux et de signes contraires, desorte qu'on peut encore tirer de là la décomposition du nombre p en deux quarrés. Mais il est clair que les termes extrêmes seront pairs, et partant, celui du milieu impair; et comme il est constant qu'un nombre premier ne peut se décomposer que d'une seule manière en deux quarrés; la forme trouvée par cette dernière méthode sera $(B, \pm A, -B)$, ou $(-B, \mp A, B)$. Ainsi, pour l'exemple précédent, où $p=233$, on a

$(2, 15, -4)$, $(-4, 13, 16)$, $(16, 3, -14)$, $(-14, 11, 8)$, $(8, 13, -8)$,

et $233=169+64$, comme plus haut.

266. Jusqu'à présent nous avons restreint nos recherches aux fonctions du second degré qui ne renferment que deux indéterminées, et il n'a pas été nécessaire de les distinguer par une dénomination particulière; mais il est clair que ce sujet n'est qu'une section très-particulière *des fonctions algébriques rationnelles, entières et homogènes, qui renferment plusieurs inconnues*. Ces fonctions peuvent se distribuer en formes du premier, du deuxième, du troisième, etc. degré; et quant au nombre d'indéterminées, nous les distinguerons commodément en formes *binaires*, *trinaires*, *quaternaires*, etc. Ainsi, ce que nous avons appelé *forme* jusqu'à présent, prendra dorénavant le nom de *forme binaire* du second degré, et les fonctions telles que

$$Ax^2+2Bxy+Cy^2+2Dxz+2Eyz+Fz^2;$$

A, B, C, D, etc. étant des nombres entiers, s'appelleront *formes trinaires du second degré*, et ainsi de suite. Nous avions presque consacré la présente section aux formes binaires du second degré; mais comme il nous reste à faire connaître quelques-unes de leurs

plus

plus belles propriétés, qui se déduisent naturellement de la théorie des formes trinaires, nous insérons ici une courte digression sur ces dernières, et nous exposerons des premiers élémens de cette théorie, ce qui sera nécessaire pour compléter celle des formes binaires, pensant satisfaire davantage les Géomètres, que si nous les supprimions, ou si nous les déduisions de méthodes moins directes. Au reste, nous réservons pour une autre occasion l'examen plus exact de cet important sujet, tant parceque sa fertilité excéderait de beaucoup les bornes de cet ouvrage, que dans l'espoir de pouvoir lui donner par la suite plus de développemens. Mais nous écartons absolument les formes *quaternaires*, *quinaires*, etc. du second degré et celles des degrés plus élevés, et il suffira d'avoir recommandé ce champ vaste à l'attention des géomètres, où ils pourront trouver un très-beau sujet d'exercer leurs forces, et les moyens de donner à l'Arithmétique transcendante de très-beaux développemens. Nous pourrons ainsi nous contenter de distinguer les formes en binaires et ternaires.

267. Il sera avantageux, pour l'intelligence, d'établir un ordre fixe parmi les indéterminées des formes trinaires, comme nous l'avons fait pour les formes binaires, de manière à distinguer la *première*, la *seconde* et la *troisième*. Quant à la disposition des différentes parties de la forme, nous suivrons constamment aussi le même ordre, en plaçant le premier le terme qui renferme le quarré de la première inconnue, et ensuite ceux qui renferment le quarré de la seconde, le quarré de la troisième, le double produit de la seconde par la troisième, le double produit de la première par la troisième, et enfin le double produit de la première par la deuxième. Mais, comme nous abrégerons en ne dénotant pas toujours les indéterminées par des lettres particulières, nous représenterons la forme f

$$ax^2 + a'x'^2 + a''x''^2 + 2bx'x'' + 2b'xx'' + 2b''xx'$$

par le symbole $\begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix}$, quand nous n'aurons pas égard aux indéterminées.

En posant $b^2 - a'a'' = A$, $b'^2 - aa'' = A'$, $b''^2 - aa' = A''$, $ab - b'b'' = B$, $a'b' - bb'' = B'$, $a''b' - bb' = B''$, il résulte une autre

forme $F=\begin{pmatrix}A, & A', & A''\\ B, & B', & B''\end{pmatrix}$, que nous appellerons *adjointe* de la forme f. Ces relations donnent aussi les suivantes, en représentant par D le nombre

$$ab^2+a'b'^2+a''b''^2-aa'a''-2bb'b'',$$

$$B^2-A'A''=aD,\quad B'^2-AA''=a'D,\quad B''^2-AA'=a''D,$$
$$AB-B'B''=bD,\ A'B'-BB''=b'D,\ A''B''-BB'=b''D;$$

d'où il suit que la forme $\begin{pmatrix}aD, & a'D, & a''D\\ bD, & b'D, & b''D\end{pmatrix}$ est adjointe à la forme F. Nous appellerons *déterminant* de la forme f, le nombre D de la nature duquel dépendent principalement les propriétés des formes ternaires. De cette manière, le déterminant de la forme F est D^2, ou égal au quarré du déterminant de la forme à laquelle elle est adjointe.

Ainsi, par exemple, la forme ternaire $\begin{pmatrix}29, & 13, & 9\\ 7, & -1, & 14\end{pmatrix}$ a pour adjointe $\begin{pmatrix}-68, & -260, & -181\\ 217, & -111, & 133\end{pmatrix}$, et elles ont toutes deux pour déterminant, 1.

Nous excluons de nos Recherches les formes ternaires dont le déterminant est 0, que nous traiterons plus en détail dans une autre occasion, et qui ne sont ternaires qu'en apparence, se réduisant, comme on le verra, à des formes binaires.

268. Si une forme ternaire f, dont les indéterminées sont x, x', x'', et le déterminant D, se change en une forme ternaire g, dont le déterminant est E, par la substitution

$$x=\alpha y+\beta y'+\gamma y'',\ x'=\alpha' y+\beta' y'+\gamma' y'',\ x''=\alpha'' y+\beta'' y'+\gamma'' y'',$$

où les coefficiens α, β, γ, α', etc. sont supposés des nombres entiers, nous dirons, pour abréger, que la forme f se change en g par la substitution

$$\alpha,\ \beta,\ \gamma;\quad \alpha',\ \beta',\ \gamma';\quad \alpha'',\ \beta'',\ \gamma''.....(S),$$

et que f renferme g, ou que g est contenu dans f. De cette supposition dérivent six équations pour les six coefficiens de g, qu'il est inutile de transcrire ici, et d'où l'on déduit facilement les conclusions suivantes:

1°. En désignant, pour abréger, par k le nombre

$$\alpha\beta'\gamma'' + \beta\gamma'\alpha'' + \gamma\alpha'\beta'' - \gamma\beta'\alpha'' - \alpha\gamma'\beta'' - \beta\alpha'\gamma'',$$

on trouve, réduction faite, $E = k^2 D$; d'où il suit que D doit diviser E et que le quotient doit être un quarré. L'on voit ainsi que le nombre k joue ici le même rôle que le nombre $\alpha\delta - \beta\gamma$ pour les formes binaires, d'où nous pourrions présumer que le signe de k établit aussi une différence essentielle entre les transformations propres et impropres. Mais en examinant la chose de plus près, il est clair que f se change aussi en γ par la substitution

$$-\alpha, -\beta, -\gamma; \quad -\alpha', -\beta', -\gamma'; \quad -\alpha'', -\beta'', -\gamma'',$$

et que k devient alors $-k$, et que parconséquent cette substitution serait différente, et que toute forme ternaire en renfermerait une autre tant proprement qu'improprement. Ainsi nous ne ferons pas usage de cette distinction, qui devient inutile pour les formes ternaires.

2°. En désignant par F et G les formes adjointes aux formes f, γ, les coefficiens de F se déterminent par les coefficiens de f, et les coefficiens de G par ceux de g, qui se connaissent eux-mêmes par les équations que fournit la substitution S. Or la comparaison des coefficiens de F et G prouve sans peine que F renferme G et se change en elle par la substitution

$$\begin{array}{l}\beta'\gamma''-\beta''\gamma',\ \gamma'\alpha''-\gamma''\alpha',\ \alpha'\beta''-\alpha''\beta';\ \beta''\gamma-\beta\gamma'',\ \gamma''\alpha-\gamma\alpha'',\ \alpha''\beta-\alpha\beta'',\\ \beta\gamma'-\beta'\gamma,\ \gamma\alpha'-\gamma'\alpha,\ \alpha\beta'-\alpha'\beta \ldots\ldots\ldots\

4°. On prouve absolument de la même manière, que la forme G se change, par la substitution

$$\alpha, \alpha', \alpha''; \quad \beta, \beta', \beta''; \quad \gamma, \gamma', \gamma'' \ldots\ldots\ldots\ldots\ldots (S'''),$$

en la forme en laquelle se change F, en multipliant les différens coefficiens par k^2; nous désignerons cette forme par F'.

Nous dirons que la substitution S''' naît, *par transposition*, de la substitution S; alors il est évident que la substitution S résulte de la transposition de la substitution S'''; de même S' et S'' naissent de leur transposition réciproque. On peut appeler la substitution S' substitution *adjointe* à S, d'où la substitution S'' sera adjointe à la substitution S'''.

269. S'il arrive, non-seulement que la forme f renferme la forme y, mais encore que la forme g renferme la forme f, ces deux formes seront dites équivalentes, et dans ce cas on voit que D et E devant se diviser mutuellement, on a nécessairement $D = E$; et réciproquement si une forme f en renferme une autre g de même déterminant, ces deux formes seront équivalentes; en effet on aura $k = \pm 1$, et partant la forme f' en laquelle se change g par la substitution S'', sera identique avec f, et par-conséquent f sera contenue dans g. Or il est clair que dans ce cas les formes F et G adjointes aux formes f et g seront aussi équivalentes, et que la deuxième se change en la première par la substitution S'''. Enfin, si l'on suppose que les formes F, G soient équivalentes, et que la première se change en la deuxième par la substitution T, les formes f et g seront aussi équivalentes, et f se changera en g par la substitution adjointe à T, et g en f par la substitution qui naît de la transposition de la substitution adjointe à T. Car par ces deux substitutions respectives, la forme adjointe à F se change en la forme adjointe à G, et la forme G en cette même première forme; mais ces deux formes naissent de f et g, en multipliant chacun de leurs coefficiens par D; d'où l'on voit sans peine que par les mêmes substitutions f se change en g et g en f respectivement.

270. Si la forme ternaire f renferme la forme ternaire f' et celle-ci la forme f'', la forme f renfermera aussi f''. Car on voit

facilement que si f se change en f' par la substitution

$$\alpha, \beta, \gamma; \quad \alpha', \beta', \gamma'; \quad \alpha'', \beta'', \gamma'',$$

et f' en f'', par la substitution

$$\delta, \varepsilon, \zeta; \quad \delta', \varepsilon', \zeta'; \quad \delta'', \varepsilon'', \zeta'',$$

f se changera en f'' par la transformation

$$\begin{array}{lll} \alpha\delta+\beta\delta'+\gamma\delta'', & \alpha\varepsilon+\beta\varepsilon'+\gamma\varepsilon'', & \alpha\zeta+\beta\zeta'+\gamma\zeta''; \\ \alpha'\delta+\beta'\delta'+\gamma'\delta'', & \alpha'\varepsilon+\beta'\varepsilon'+\gamma'\varepsilon'', & \alpha'\zeta+\beta'\zeta'+\gamma'\zeta''; \\ \alpha''\delta+\beta''\delta'+\gamma''\delta'', & \alpha''\varepsilon+\beta''\varepsilon'+\gamma''\varepsilon'', & \alpha''\zeta+\beta''\zeta'+\gamma''\zeta''; \end{array}$$

ainsi, dans le cas où f est équivalente à f', et f' à f'', la forme f sera aussi équivalente à f''. Au reste, on voit aisément comment ces théorèmes s'étendraient à un plus grand nombre de formes.

271. Il suit évidemment de là que toutes les formes ternaires, ainsi que les formes binaires, peuvent se distribuer en classes, en rapportant à la même classe les formes équivalentes, et celles qui ne le sont pas, à des classes différentes. Ainsi les formes de déterminant différent appartiendront certainement à des classes différentes, et partant il y aura un nombre infini de classes de formes ternaires; mais les formes ternaires de même déterminant donnent un nombre de classes tantôt plus grand, tantôt plus petit, *mais toujours fini*, ce qui peut être considéré comme une propriété principale de ces formes. Avant de traiter avec plus de détail cette proposition très-importante, nous expliquerons une différence essentielle qui a lieu entre les formes ternaires.

Quelques formes ternaires sont telles, qu'on peut représenter par elles, sans distinction des nombres positifs et négatifs, par exemple, la forme $x^2+y^2-z^2$, et nous les nommerons formes *indéfinies*. Au contraire, il en existe d'autres par lesquelles on ne peut représenter de nombres négatifs, comme la forme $x^2+y^2+z^2$, et nous les nommerons formes *positives;* enfin, par d'autres, on ne peut représenter que des nombres négatifs, comme la forme $-x^2-y^2-z^2$, nous les nommerons formes *négatives*. Les formes positives et négatives s'appelleront formes *définies*. Nous allons donner les caractères auxquels on peut reconnaître à laquelle de ces espèces appartient une forme donnée.

Si l'on multiplie par a la forme

$$f=ax^2+a'x'^2+a''x''^2+2bx'x''+2b'xx''+2b''xx'$$

de déterminant D, et que l'on désigne, comme au n° 268, par A, A', A'', B, B', B'' les coefficiens de la forme adjointe à f, on trouve

$$g=af=(ax+b''x'+b'x'')^2-A''x'^2+2Bx'x''-A'x''^2;$$

multipliant ensuite par A', il vient

$$h=A'af=A'(ax+b''x'+b'x'')^2-(A'x''-Bx')^2+aDx'^2;$$

d'où il suit que $A'af$ est négatif si aD et A' le sont, et par-conséquent que le signe de f est nécessairement opposé à celui de $A'a$, c'est-à-dire que f est de même signe que a ou de signe opposé à D. Ainsi la forme f sera définie dans ce cas-là, et sera positive ou négative, suivant que a est positif ou négatif, ou suivant que D est négatif ou positif.

Mais si aD et A' sont positifs, ou que l'un des deux le soit, aucun n'étant $=0$, on voit facilement qu'en déterminant convenablement les valeurs des indéterminées, h pourra être positif ou négatif, et que partant f pourra obtenir des valeurs, tant de même signe que de signe opposé à h; donc f sera une forme indéfinie.

Pour le cas où $A'=0$, sans qu'on ait aussi $a=0$, on aura

$$af=(ax+b''x'+b'x'')^2-x'(A''x'-2Bx''),$$

en donnant à x' une valeur arbitraire, qui cependant ne soit pas $=0$, et prenant x'' tel que le signe de $\frac{A''x'}{2B}-x''$ soit le même que celui de Bx', ce qui est possible, car B n'est pas $=0$, puisqu'on aurait $B^2-A'A''=aD=0$, et partant $D=0$; alors $x'(A''x'-2Bx'')$ sera une quantité positive, et l'on voit aisément que x pourra être déterminé de manière que af obtienne une valeur négative; il est même évident que ces valeurs peuvent être prises, si l'on veut, de manière qu'elles soient toutes entières. Enfin, x' et x'' ayant des valeurs quelconques, on peut prendre x assez grand pour que af devienne positif. Donc, dans ce cas, la forme f est indéfinie.

Enfin, si $a=0$, on a

$$f=a'x'^2+2bx'x''+a''x''^2+2x(b''x'+b'x''),$$

et en prenant x', x'' à volonté, mais tels que $b''x'+b'x''$ ne soit pas zéro, il est évident que l'on peut déterminer x de manière que f obtienne des valeurs positives et négatives; donc f est une forme indéfinie.

De même que nous avons déterminé l'espèce de la forme f, d'après les nombres aD et A', nous aurions pu y parvenir au moyen des nombres aD et A'', desorte que la forme f sera définie si aD et A'' sont négatifs, et indéfinie dans tous les autres cas. On peut de même considérer les nombres $a'D$ et A, ou $a'D$ et A'', ou $a''D$ et A, ou enfin $a''D$ et A'. Il suit de là que pour une forme définie les six nombres A, A', A'', aD, $a'D$, $a''D$ sont négatifs; pour une forme positive, a, a', a'' seront positifs et D négatif, et pour une forme négative, a, a', a'' seront négatifs et D positif; ainsi, toutes les formes ternaires de déterminant donné positif peuvent se distribuer en négatives et en indéfinies, toutes les formes d'un déterminant donné négatif peuvent se distribuer en positives et en indéfinies. Enfin, il n'y a pas de formes positives de déterminant positif, ni de formes négatives de déterminant négatif. On voit facilement, d'après cela, que la forme adjointe à une forme définie est définie et même *négative*, et que la forme adjointe à une forme indéfinie est indéfinie.

Puisque tous les nombres représentables par une forme ternaire donnée le sont également par toutes les formes qui lui sont équivalentes, les formes ternaires comprises dans une même classe seront toutes positives, ou toutes négatives, ou toutes indéfinies. Ainsi ces dénominations pourront être transportées aux classes elles-mêmes.

272. Nous allons démontrer que les formes ternaires d'un déterminant donné peuvent se distribuer en un nombre fini de classes, et nous nous y prendrons comme pour les formes binaires, c'est-à-dire, que nous ferons voir d'abord comment une forme ternaire donnée peut être ramenée à une forme ternaire plus simple, et ensuite que le nombre des formes les plus simples auxquelles on parvient par ces réductions est toujours fini, quel que soit le déter-

minant. Supposons généralement que la forme $f=\begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix}$ de déterminant D, se change en la forme équivalente $g=\begin{pmatrix} m, & m', & m'' \\ n, & n', & n'' \end{pmatrix}$ par la substitution

$$\alpha, \beta, \gamma; \quad \alpha', \beta', \gamma'; \quad \alpha'', \beta'', \gamma'' \ldots\ldots\ldots\ldots (S)$$

il nous restera à déterminer α, β, γ, etc. de manière que g soit plus simple que f. Soient $F=\begin{pmatrix} A, & A', & A'' \\ B, & B', & B'' \end{pmatrix}$, $G=\begin{pmatrix} M, & M', & M'' \\ N, & N', & N'' \end{pmatrix}$ les formes adjointes à f et g, la forme F se changera en G par la substitution adjointe à S, et G en F par la substitution qui naît de la transposition de S. Nous ferons le nombre

$$\alpha\beta'\gamma'' + \alpha'\beta''\gamma + \alpha''\beta\gamma' - \alpha''\beta'\gamma - \alpha\beta''\gamma' - \alpha'\beta\gamma'' = \pm 1 = k.$$

Cela posé, observons :

1°. Que si l'on fait $\gamma=0$, $\gamma'=0$, $\alpha''=0$, $\beta''=0$, $\gamma''=1$, on a

$$m=a\alpha^2+2b''\alpha\alpha'+a'\alpha'^2, \quad m'=a\beta^2+2b''\beta\beta'+a'\beta'^2, \quad m''=a'',$$
$$n=b\beta'+b'\beta; \quad n'=b\alpha'+b'\alpha, \quad n''=a\alpha\beta+b''(\alpha\beta'+\alpha'\beta)+a'\alpha'\beta;$$

on aura en outre $\alpha\beta'-\alpha'\beta=\pm 1$. Il est évident par là, que la forme binaire (a, b'', a') de déterminant A'' se change par la substitution α, β, α', β' en la forme binaire (m, n'', m'), et qu'elle lui est même équivalente, puisque $\alpha\beta'-\alpha'\beta=\pm 1$; on aura donc $A''=M''$, ce qu'on peut aussi vérifier sans peine directement. Si donc la forme (a, b'', a') n'est pas déjà la forme la plus simple de sa classe, on pourra déterminer α, β, α', β', de manière que (m, n'', m') soit une forme plus simple ; et par la théorie des formes binaires, on sait que cette réduction peut se faire de manière que m ne soit pas plus grand que $\sqrt{-\frac{4}{3}A''}$ si A'' est négatif, ou que $\sqrt{A''}$ si A'' est positif, ou enfin de manière que $m=0$ si $A''=0$. Desorte que dans tous les cas, la valeur absolue de m peut être abaissée ou au moins au-dessous jusqu'à $\sqrt{\pm\frac{4}{3}A''}$. Ainsi la forme f peut se ramener à une autre, dans laquelle, s'il y a lieu, le premier coefficient soit plus petit, et dont la forme adjointe ait le même troisième coefficient que la forme F adjointe à f. C'est en cela que consiste la première réduction.

2°.

2°. Mais si l'on fait $\alpha = 1$, $\beta = 0$, $\gamma = 0$, $\alpha' = 0$, $\alpha'' = 0$, on aura $k = \beta'\gamma'' - \beta''\gamma' = \pm 1$, et la substitution adjointe à S deviendra

$$\pm 1, 0, 0;\quad 0, \gamma'', -\beta'';\quad 0, -\gamma', \beta',$$

par laquelle F se change en G. On a ainsi

$$m = a,\ n' = b'\gamma'' + b''\gamma',\ n'' = b'\beta'' + b''\beta',\ m' = a'\beta'^2 + 2b\beta'\beta'' + a''\beta''^2,$$
$$m'' = a'\gamma'^2 + 2b\gamma'\gamma'' + a''\gamma''^2,\ n = a'\beta'\gamma' + b(\beta'\gamma'' + \beta''\gamma') + a''\beta''\gamma'');$$
$$M' = A'\gamma''^2 - 2B\gamma'\gamma'' + A''\gamma'^2,\ N = -A'\beta''\gamma'' + B(\beta'\gamma'' + \beta''\gamma') - A''\beta'\gamma',$$
$$M'' = A'\beta''^2 - 2B\beta'\beta'' + A''\beta'^2,$$

d'où il suit que la forme binaire (A'', B, A') dont le déterminant est Da, se change par la substitution $\beta', -\gamma', -\beta'', \gamma''$, en la forme (M'', N, M') de déterminant Dm; et à cause de l'équation $\beta'\gamma'' - \beta''\gamma' = \pm 1$, ou de $Da = Dm$, ces deux formes sont équivalentes. Ainsi, à moins que la forme (A'', D, A') ne soit déjà la plus simple de sa classe, les coefficiens $\beta', \gamma', \beta'', \gamma''$ pourront être déterminés de manière que (M'', N, M') soit plus simple; et même cette réduction peut se faire de manière que M'', sans égard au signe, ne soit pas plus grand que $\sqrt{\pm \frac{4}{3} D}$; ensorte que l'on réduit la forme f à une autre qui a le même premier coefficient, mais dans la forme adjointe de laquelle le troisième coefficient est moindre, s'il y a lieu, que celui de la forme F adjointe à f. C'est en cela que consiste la seconde réduction.

3°. Si donc f est une forme ternaire à laquelle aucune de ces deux réductions ne soit applicable, c'est-à-dire, qui ne puisse par aucune se changer en une plus simple, on aura alors nécessairement $a^2 < \text{ou} = \frac{4}{3} A$, et $A^2 < \text{ou} = \frac{4}{3} aD$, sans avoir égard au signe. Donc a^4 sera $< \text{ou} = \frac{16}{9} A^2$, et partant, $a^4 < \text{ou} = \frac{64}{27} aD$, et $a^3 < \text{ou} = \frac{64}{27} D$; donc $a < \text{ou} = \frac{4}{3} \sqrt[3]{D}$, et $A^2 < \text{ou} = \frac{16}{9} \sqrt[3]{D^4}$, et parconséquent $A < \text{ou} = \frac{4}{3} \sqrt[3]{D^2}$. Ainsi, quand A et a surpassent ces limites, nécessairement l'une ou l'autre des réductions précédentes peut être appliquée à la forme f. Au reste, il ne faut pas renverser cette conclusion, puisqu'il arrive souvent qu'une forme ternaire dont le premier et le troisième coefficient sont au-dessous de ces limites, peut néanmoins être rendue plus simple par l'une ou l'autre de ces réductions.

4°. Si donc on applique alternativement la première et la seconde réduction à une forme donnée de déterminant D, c'est-à-dire qu'on lui applique la première ou la seconde, à celle qui en résulte la seconde ou la première, à celle qui en résulte de nouveau la première ou la seconde, etc., il est évident qu'on arrivera nécessairement à une forme à laquelle on ne pourra plus appliquer ni l'une ni l'autre, sans quoi on aurait deux suites de nombres entiers continuellement décroissans. Nous sommes donc parvenus à ce théorème important : *Toute forme ternaire de déterminant* D, *peut être réduite à une autre équivalente dont le premier coefficient ne soit pas plus grand que* $\frac{3}{4}\sqrt[3]{D}$, *et telle que le troisième coefficient de la forme adjointe ne soit pas plus grand que* $\frac{4}{3}\sqrt[3]{D^2}$, *sans avoir égard au signe, à moins que la forme proposée ne jouisse déjà de ces deux propriétés.*

Au reste, au lieu du premier coefficient de la forme f, et du troisième de la forme adjointe, nous aurions pu traiter absolument de la même manière, le premier coefficient de f et le second de la forme adjointe, ou le second de f et le premier ou le troisième de la forme adjointe, ou le troisième de f et le premier ou le second de la forme adjointe, et nous serions arrivés de même à notre but; mais il vaut mieux s'en tenir à une méthode unique, afin de pouvoir ramener plus facilement les opérations à un algorithme fixe. Nous observons enfin que les deux coefficiens que nous avons appris à abaisser au-dessous de limites fixes, peuvent avoir encore des limites moindres, si l'on distingue les formes finies des formes indéfinies. Mais cela n'est pas nécessaire pour ce que nous nous proposons.

273. Voici quelques exemples qui éclairciront ce qui précède.

Exemple I. Soit $f=\begin{pmatrix}19,21,50\\15,28,1\end{pmatrix}$, on aura $F=\begin{pmatrix}-825,-166,-398\\257,573,-370\end{pmatrix}$ et $D=-1$. Comme $(19, 1, 21)$ est une forme binaire réduite qui n'a pas de forme équivalente dont le premier terme soit moindre que 19, la première réduction n'est pas applicable ici; mais la forme binaire $(A'', B, A') = (-398, 257, -166)$ se change en $(-2, 1, -10)$ qui lui est équivalente, par la substitution $2, 7, 3, 11$. Ainsi, en faisant $\beta'=2$, $\gamma'=-7$, $\beta''=-3$, $\gamma''=11$, on aura pour la forme f, la substitution

$$1, 0, 0;\ 0, 2, -7;\ 0, -3, 11,$$

par laquelle on trouve qu'elle se change en $f' = \begin{pmatrix} 19, 354, 4769 \\ -1229, 301, -82 \end{pmatrix}$. Le troisième coefficient de la forme adjointe à f' est -2, et partant, celle-ci doit être regardée comme plus simple que f.

On peut appliquer à la forme f' la première réduction. La forme binaire $(19, -82, 354)$ se changeant en $(1, 0, 2)$ par la transformation $13, 4, 3, 1$, on aura pour la forme f la transformation

$$13, 4, 0;\ \ 3, 1, 0;\ \ 0, 0, 1,$$

par laquelle elle se change en la forme $\begin{pmatrix} 1, 2, 4769 \\ -95, 16, 0 \end{pmatrix} = f''$.

On peut appliquer de nouveau la seconde réduction à la forme f'' qui a pour adjointe $\begin{pmatrix} -513, -4513, -2 \\ -95, 32, 1520 \end{pmatrix}$. En effet, la forme binaire $(-2, -95, -4513)$ se change par la substitution $47, 1, -1, 0$ en $(-1, 1, -2)$, d'où f'' se change par la substitution

$$1, 0, 0;\ \ 0, 47, -1;\ \ 0, 1, 0,$$

en la forme $f''' = \begin{pmatrix} 1, 257, 2 \\ 1, 0, 16 \end{pmatrix}$. Le premier coefficient de cette forme ne peut plus être réduit par la première réduction, ni le troisième de la forme adjointe par la seconde.

Exemple II. Soit $f = \begin{pmatrix} 10, 26, 2 \\ 7, 0, 4 \end{pmatrix}$ qui a pour adjointe la forme $\begin{pmatrix} -3, -20, -244 \\ 70, -28, 8 \end{pmatrix}$, et 2 pour déterminant. On trouve successivement par l'application alternative des deux réductions,

les substitutions	par lesquelles les formes	se changent en
$1, 0, 0;\ 0, -1, 0;\ 0, 4, -1 \ldots$	$\ldots\ldots f \ldots\ldots$	$f' = \begin{pmatrix} 10, 2, 2 \\ -1, 0, -4 \end{pmatrix}$
$0, -1, 0;\ 1, -2, 0;\ 0, 0, 1 \ldots$	$\ldots\ldots f' \ldots\ldots$	$f'' = \begin{pmatrix} 2, 2, 2 \\ 2, -1, 0 \end{pmatrix}$
$1, 0, 0;\ 0, -1, 0;\ 0, 2, -1 \ldots$	$\ldots\ldots f'' \ldots\ldots$	$f''' = \begin{pmatrix} 2, 2, 2 \\ -2, 1, -2 \end{pmatrix}$
$1, 0, 0;\ 1, 1, 0;\ 0, 0, 1 \ldots$	$\ldots\ldots f''' \ldots\ldots$	$f^{IV} = \begin{pmatrix} 0, 2, 2 \\ -2, -1, 0 \end{pmatrix}$.

La forme f^{IV} ne peut être soumise à l'une ni à l'autre des deux réductions.

274. Quand on a une forme ternaire dont le premier coefficient, ainsi que le troisième de la forme adjointe, sont abaissés autant que possible par la méthode précédente, on obtiendra comme il suit une plus grande réduction.

En conservant toujours la notation du n° 172, et posant $\alpha=1$, $\alpha'=0$, $\beta'=1$, $\alpha''=0$, $\beta''=0$, $\gamma''=1$, c'est-à-dire en employant la substitution

$$1,\ \beta,\ \gamma;\quad 0,\ 1,\ \gamma';\quad 0,\ 0,\ 1,$$

on aura

$$m=a, m'=a'+2b''\beta+a\beta^2, m''=a''+2b\gamma'+2b'\gamma+a\gamma^2+2b''\gamma\gamma'+a'\gamma'^2;$$
$$n=b+a'\gamma'+b'\beta+b''(\gamma+\beta\gamma')+a\beta\gamma, n'=b'+a\gamma+b''\gamma', n''=b''+a\beta,$$

et en outre $M''=A''$, $N=B-A''\gamma'$, $N'=B'-A''\gamma-N\beta$.

Ainsi, par cette substitution les coefficiens a, A'', qui sont déjà réduits, ne changeront pas; il ne reste plus qu'à diminuer les autres coefficiens en déterminant convenablement les valeurs de β, γ, γ'.

Observons d'abord que si l'on a $A''=0$, on doit avoir aussi $a=0$; car si a n'était pas $=0$, la première réduction serait encore applicable, puisqu'à toute forme de déterminant $=0$ répond une forme équivalente telle que $(0, 0, h)$ (n° 215), et dont parconséquent le premier terme $=0$. De la même manière, si $a=0$, on aura $A''=0$, ainsi les deux nombres a et A seront tous deux nuls, ou aucun des deux ne le sera.

Dans le second cas, il est évident que β, γ, γ' peuvent être déterminés de manière que n'', N, N' ne soient pas plus grands que $\frac{1}{2}a$, $\frac{1}{2}A''$, $\frac{1}{2}A''$ respectivement. Ainsi dans le premier exemple du n° précédent, la dernière forme $\begin{pmatrix}1, & 257, & 2\\ 1, & 0, & 16\end{pmatrix}$, qui a pour adjointe $\begin{pmatrix}-513, & -2, & -1\\ 1, & -16, & 32\end{pmatrix}$, se change, par la substitution

$$1,\ -16,\ 16;\quad 0,\ 1,\ -1;\quad 0,\ 0,\ 1,$$

en la forme $f^{IV}=\begin{pmatrix}1, & 1, & 1\\ 0, & 0, & 0\end{pmatrix}$, qui a pour adjointe $\begin{pmatrix}-1, & -1, & -1\\ 0, & 0, & 0\end{pmatrix}$.

Dans le premier cas, où $a=A''=0$, et partant $b''=0$, on aura

$$m=0,\quad m'=a',\quad m''=a''+2b'\gamma'+2b'\gamma+a'\gamma'^2,$$
$$n=b+a'\gamma'+b'\beta;\quad n'=b',\quad n''=0,$$

ce qui donne $D=a'b'^2=m'n'^2$. Or on voit facilement que l'on peut prendre β et γ' de manière que n soit le résidu *minimum* absolu de b, suivant le plus grand diviseur commun des nombres a', b', c'est-à-dire, que n ne soit pas plus grand que la moitié de ce commun diviseur, abstraction faite du signe, et partant $n=0$, toutes les fois que a' et b' sont premiers entre eux; β et γ' étant ainsi déterminés, on pourra prendre γ tel que m'' ne soit pas $>b'$, à moins que l'on n'eût $b'=0$; mais alors on aurait $D=0$, cas que nous avons exclu. Ainsi, dans le second exemple, on a pour la dernière forme $n=-2-\beta+2\gamma'$, et en faisant $\beta=0$, $\gamma'=1$, il vient $n=0$, partant $m''=2-2\gamma$ et $m''=0$ en faisant $\gamma=1$. Ainsi, par la substitution

$$1,\ -2,\ 1;\quad 0,\ 1,\ 0;\quad 0,\ 0,\ 1,$$

cette forme se change en $\begin{pmatrix} 0, & 2, & 0 \\ 0, & -1, & 0 \end{pmatrix}=f^{\text{IV}}$.

275. Si l'on a une suite de formes ternaires équivalentes f, f', f'', f''', etc., et les transformations de chacune d'elles en la suivante, des transformations de f en f' et de f' en f'', on déduira (n° 270) celle de f en f''; de cette dernière et de la transformation de f'' en f''', on déduira celle de f en f''', etc. Ainsi, de cette manière on aura la transformation de f en une forme quelconque de cette suite; et comme (nos 268, 269) on déduit de la transformation d'une forme quelconque f en une autre g, la transformation de g en f, on pourra obtenir la transformation d'une forme quelconque de la suite, en la première f.

Ainsi, pour les formes du premier exemple on trouve les substitutions

$$13,\ 14,\ 0;\ 6,\ 2,\ -7;\ -9,\ -3,\ 11....$$
$$13,\ 188,\ -4;\ 6,\ 87,\ -2;\ -9,\ -130,\ 3....$$
$$13,\ -20,\ 16;\ 6,\ -9,\ 7;\ -9,\ 14,\ -11,$$

par lesquelles f' se change en f'', f''', f^{IV}, et de la dernière on déduit la suivante :

$$1,\ 4,\ 4;\quad 3,\ 1,\ 5;\quad 3,\ -2,\ 3,$$

par laquelle f^{IV} se change en f'.

De la même manière, pour l'exemple 2 du n° précédent, on trouve les substitutions

$$\begin{array}{llllllll} 1, & -1, & 1; & -3, & 4, & -3; & 10, & -14, \ 11\ldots\ldots \\ 2, & -3, & -1; & 3, & 1, & 0; & 2, & 4, \ 1, \end{array}$$

par lesquelles la forme $\begin{pmatrix} 10, & 26, & 2 \\ 7, & 0, & 4 \end{pmatrix}$ se change en $\begin{pmatrix} 0, & 2, & 0 \\ 0, & -1, & 0 \end{pmatrix}$, et cette dernière en la première respectivement.

276. THÉORÈME. *Le nombre des classes en lesquelles peuvent se distribuer les formes ternaires de déterminant donné, est toujours fini.*

I. Le nombre de toutes les formes $\begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix}$ de déterminant donné D, dans lesquelles on a $a=0$, $b''=0$, b non plus grand que la moitié du plus grand commun diviseur entre a' et b', et a'' non plus grand que b', est nécessairement toujours fini. En effet, puisqu'on a dans ce cas $D=a'b'^2$, on ne pourra prendre pour b' que $+1$, -1 et les racines des quarrés qui peuvent diviser D, s'il y en a d'autres que 1, prises positivement ou négativement, et le nombre de ces valeurs est fini; or, pour chaque valeur de b', celle de a' est déterminée, et celles de b, a'' sont évidemment limitées.

II. Il n'y aura de même qu'un nombre fini de formes $\begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix}$ de déterminant D, dans lesquelles a n'est ni $=0$ ni $>\frac{4}{3}\sqrt[3]{\pm D}$, $b''^2-aa'=A''$ ni $=0$, ni $>\frac{4}{3}\sqrt[3]{D^2}$, b'' non plus grand que $\frac{1}{2}a$, $ab-b'b''=B$ et $a'b'-bb''=B'$ non plus grands que $\frac{1}{2}A''$. Car le nombre des combinaisons des valeurs de a, b'', A'', B, B' sera nécessairement fini, et en les supposant déterminés, les autres coefficiens a', b, b', a'' de la forme et les coefficiens $A=b^2-a'a''$, $A'=b'^2-aa''$, $B''=a''b''-bb'$ de la forme adjointe seront déterminés par les équations

$$a'=\frac{b''^2-A''}{a},\quad A'=\frac{B^2-aD}{A''},\quad A=\frac{B'^2-a'D}{A''},\quad B''=\frac{BB'+b''D}{A''},$$

$$b=\frac{AB-B'B''}{D}=-\frac{Bd'+B'b''}{A''},\quad b'=\frac{A'B'-BB''}{D}=-\frac{Bb''+B'a}{A''},$$

$$a''=\frac{b'^2-A'}{a}=\frac{b^2-A}{a'}=\frac{bb'+B''}{b''}.$$

Maintenant, comme toutes ces formes s'obtiennent en choisissant parmi toutes les combinaisons de a, b'', A'', B, B' celles qui donnent des valeurs entières pour a', a'', b, b', leur nombre sera nécessairement fini.

III. Toutes les formes dont nous venons de parler (I et II) constituent un nombre de classes qui sera moindre que celui de ces formes, s'il s'en trouve parmi elles d'équivalentes. Or comme il suit de l'analyse précédente que toute forme ternaire de déterminant D est nécessairement équivalente à l'une de ces formes, les classes qu'elles déterminent renfermeront toutes les formes de déterminant D, c'est-à-dire que toutes les formes de déterminant D peuvent se distribuer en un nombre fini de classes.

277. Les règles par lesquelles toutes les formes de I et II peuvent se former, suivent naturellement de ce qui a été dit dans l'article précédent; ainsi il suffira d'en donner quelques exemples.

Pour $D=1$, les formes (I) produisent les six suivantes, par l'ambiguité des signes, $\begin{pmatrix}0, & 1, & 0\\ 0, & \pm 1, & 0\end{pmatrix}$, $\begin{pmatrix}0, & 1, & \pm 1\\ 0, & \pm 1, & 0\end{pmatrix}$; dans les formes II, a et A'' ne peuvent avoir d'autres valeurs que $+1$ et -1, et pour les quatre combinaisons qui en résultent, b'', B et B' doivent être posés $=0$, ce qui donne les quatre formes $\begin{pmatrix}1, & -1, & 1\\ 0, & 0, & 0\end{pmatrix}$, $\begin{pmatrix}-1, & 1, & 1\\ 0, & 0, & 0\end{pmatrix}$, $\begin{pmatrix}1, & 1, & -1\\ 0, & 0, & 0\end{pmatrix}$, $\begin{pmatrix}-1, & -1, & -1\\ 0, & 0, & 0\end{pmatrix}$.

De même, pour $D=-1$, il y a six formes (I)... $\begin{pmatrix}0, & -1, & 0\\ 0, & \pm 1, & 0\end{pmatrix}$, $\begin{pmatrix}0, & -1, & 1\\ 0, & \pm 1, & 0\end{pmatrix}$, et quatre formes (II)... $\begin{pmatrix}1, & -1, & -1\\ 0, & 0, & 0\end{pmatrix}$, $\begin{pmatrix}-1, & 1, & -1\\ 0, & 0, & 0\end{pmatrix}$, $\begin{pmatrix}1, & 1, & 1\\ 0, & 0, & 0\end{pmatrix}$, $\begin{pmatrix}-1, & -1, & 1\\ 0, & 0, & 0\end{pmatrix}$.

Pour $D=2$, il y a six formes (I)... $\begin{pmatrix}0, & 2, & 0\\ 0, & \pm 1, & 0\end{pmatrix}$, $\begin{pmatrix}0, & 2, & \pm 1\\ 0, & \pm 1, & 0\end{pmatrix}$, et huit formes (II)... $\begin{pmatrix}1, & -1, & 2\\ 0, & 0, & 0\end{pmatrix}$, $\begin{pmatrix}-1, & 1, & 2\\ 0, & 0, & 0\end{pmatrix}$, $\begin{pmatrix}1, & 1, & -2\\ 0, & 0, & 0\end{pmatrix}$, $\begin{pmatrix}-1, & -1, & -2\\ 0, & 0, & 0\end{pmatrix}$, $\begin{pmatrix}1, & -2, & 1\\ 0, & 0, & 0\end{pmatrix}$, $\begin{pmatrix}-1, & 2, & 1\\ 0, & 0, & 0\end{pmatrix}$, $\begin{pmatrix}1, & 2, & -1\\ 0, & 0, & 0\end{pmatrix}$, $\begin{pmatrix}-1, & -2, & -1\\ 0, & 0, & 0\end{pmatrix}$

Au reste, le nombre de classes est dans ces trois cas beaucoup moindre que le nombre des formes. En effet, on s'assure facilement

1°. Que la forme $\begin{pmatrix} 0, & 1, & 0 \\ 0, & 1, & 0 \end{pmatrix}$ se change en $\begin{pmatrix} 0, & 1, & 0 \\ 0, & -1, & 0 \end{pmatrix}$, $\begin{pmatrix} 0, & 1, & 1 \\ 0, & \pm 1, & 0 \end{pmatrix}$, $\begin{pmatrix} 0, & 1, & -1 \\ 0, & \pm 1, & 0 \end{pmatrix}$, $\begin{pmatrix} 1, & 1, & -1 \\ 0, & 0, & 0 \end{pmatrix}$, par les substitutions

1, 0, 0; 0, 1, 0; 0, 0, —1...0, 0, 1; 0, 1, —1; ±1, 1, 0
0, 0, 1; 0, 1, 1; ±1, —1, —1...1, 0, —1; 1, 1, —1; 0, —1, 1.

La forme $\begin{pmatrix} 1, & 1, & -1 \\ 0, & 0, & 0 \end{pmatrix}$ se change en $\begin{pmatrix} 1, & -1, & 1 \\ 0, & 0, & 0 \end{pmatrix}$, $\begin{pmatrix} -1, & 1, & 1 \\ 0, & 0, & 0 \end{pmatrix}$ par la seule permutation des indéterminées. Ainsi ces dix formes de déterminant 1 se réduisent aux deux : $\begin{pmatrix} 0, & 1, & 0 \\ 0, & 1, & 0 \end{pmatrix}$, $\begin{pmatrix} -1, & -1, & -1 \\ 0, & 0, & 0 \end{pmatrix}$; pour la première, on peut, si l'on veut, prendre la forme $\begin{pmatrix} 1, & 0, & 0 \\ 1, & 0, & 0 \end{pmatrix}$. Or la première forme étant indéfinie et la seconde définie, il s'ensuit que toute forme ternaire indéfinie de déterminant 1 équivaut à la forme $x^2 + 2yz$, et toute forme définie, à la forme $-x^2 - y^2 - z^2$.

2°. On trouve absolument de la même manière, que toute forme ternaire indéfinie de déterminant —1 équivaut à la forme $-x^2 + 2yz$, et toute forme définie, à la forme $x^2 + y^2 + z^2$.

3°. Pour le déterminant 2, on peut sur-le-champ rejeter des huit formes (II) la seconde, la sixième et la septième, qui proviennent de la première par la seule permutation des indéterminées; par la même raison, la cinquième, qui naît de la troisième, et la huitième, qui naît de la quatrième. Les trois qui restent avec les six formes (I) déterminent trois classes; en effet, $\begin{pmatrix} 0, & 2, & 0 \\ 0, & +1, & 0 \end{pmatrix}$ se change en $\begin{pmatrix} 0, & 2, & 0 \\ 0, & -1, & 0 \end{pmatrix}$ par la substitution.....
1, 0, 0; 0, 1, 0; 0, 0, —1, et la forme $\begin{pmatrix} 1, & 1, & -2 \\ 0, & 0, & 0 \end{pmatrix}$ en $\begin{pmatrix} 0, & 2, & 1 \\ 0, & 1, & 0 \end{pmatrix}$, $\begin{pmatrix} 0, & 2, & 1 \\ 0, & -1, & 0 \end{pmatrix}$, $\begin{pmatrix} 0, & 2, & -1 \\ 0, & 1, & 0 \end{pmatrix}$, $\begin{pmatrix} 0, & 2, & -1 \\ 0, & -1, & 0 \end{pmatrix}$, $\begin{pmatrix} 1, & -1, & 2 \\ 0, & 0, & 0 \end{pmatrix}$, par les substitutions respectives

1, 0, 1; 1, 2, 0; 1, 1, 0.....1, 0, —1; 1, 2, 0; 1, 1, 0
1, 1, 0; 1, 2, —1; 1, 1, —1.....1, 0, 0; 1, 2, 1; 1, 1, 1
1, 0, 0; 0, 1, 2; 0, 1, 1.

Ainsi

Ainsi toute forme ternaire de déterminant 2 est réductible à l'une de ces trois : $\begin{pmatrix} 0, & 2, & 0 \\ 0, & 1, & 0 \end{pmatrix}$, $\begin{pmatrix} 1, & 1, & -2 \\ 0, & 0, & 0 \end{pmatrix}$, $\begin{pmatrix} -1, & -1, & -2 \\ 0, & 0, & 0 \end{pmatrix}$; au lieu de la première on peut prendre la forme $\begin{pmatrix} 2, & 0, & 0 \\ 1, & 0, & 0 \end{pmatrix}$. Ainsi toute forme ternaire définie de déterminant 2 équivaudra nécessairement à la troisième $-x^2-y^2-2z^2$; toute forme indéfinie à la première ou à la seconde. Elle équivaudra à la première $2x^2+2yz$, si le premier, le second et le troisième coefficient sont pairs tous les trois ; car il est clair qu'une telle forme se changera en une forme semblable par une substitution quelconque, et que partant elle ne peut pas être équivalente à la seconde. Enfin elle équivaudra à la seconde $x^2+y^2-2z^2$, si le premier, le second et le troisième coefficient ne sont pas pairs tous les trois ; car il est visible, par une raison semblable, qu'une telle forme ne peut se changer par aucune transformation, en la forme $2x^2+2yz$.

On pouvait donc prévoir dans les exemples des nos 273, 274, que la forme définie $\begin{pmatrix} 19, & 21, & 50 \\ 15, & 28, & 1 \end{pmatrix}$ de déterminant -1, se réduirait à la forme $x^2+y^2+z^2$ et la forme indéfinie $\begin{pmatrix} 10, & 26, & 2 \\ 7, & 0, & 4 \end{pmatrix}$ de déterminant 2 à $2x^2-2yz$, ou, ce qui revient au même, à $2x^2+yz$.

278. Par une forme ternaire dont les indéterminées sont x, x', x'', on peut représenter des *nombres* en donnant des valeurs déterminées à x, x', x'', et des *formes binaires* par des substitutions de cette espèce : $x=mt+nu$, $x'=m't+n'u$, $x''=m''t+n''u$; m, n, m', etc. désignant des nombres déterminés, t et u les indéterminées de la forme binaire. Pour représenter d'une manière complète la théorie des formes binaires, il faudrait donner la solution des problèmes suivans.

1°. *Trouver toutes les représentations d'un nombre donné par une forme ternaire donnée.*

2°. *Trouver toutes les représentations d'une forme binaire donnée par une forme ternaire donnée.*

3°. *Distinguer si deux formes ternaires données sont équivalentes ou non, et dans le premier cas, trouver toutes les transformations de l'une en l'autre.*

4°. *Distinguer si une forme donnée renferme ou non une autre forme ternaire donnée ; et dans le premier cas, trouver toutes les transformations de la première en la seconde.*

Nous traiterons plus en détail dans un autre lieu, ces problèmes qui sont bien plus difficiles que leurs analogues dans la théorie des formes binaires ; nous nous bornerons ici à faire voir comment le premier problème peut se réduire au second, et le second au troisième, nous donnerons la solution du troisième pour quelques-uns des cas les plus simples, et qui peuvent éclairer la théorie des formes binaires. Mais nous excluons absolument le quatrième problème.

279. LEMME. *Étant proposés trois nombres entiers quelconques* a, a′, a″, *qui cependant ne soient pas tous* $= 0$, *trouver six autres nombres* B, B′, B″, C, C′, C″, *tels qu'on ait* $B'C'' - B''C' = a$, $B''C - BC'' = a'$, $BC' - B'C = a''$.

Soit α le plus grand diviseur commun des nombres a, a', a'', et les nombres entiers A, A', A'', tels que l'on ait $Aa + A'a' + A''a'' = \alpha$. Prenons à volonté trois nombres entiers Γ, Γ', Γ'', avec cette seule condition que les trois nombres $\Gamma'A'' - \Gamma''A'$, $\Gamma''A - \Gamma A''$, $\Gamma A' - \Gamma' A$ que nous représenterons par a, b', b'', et leur plus grand commun diviseur par β, ne soient pas tous $= 0$. Posant alors $a'b'' - a''b' = \alpha\beta C$, $a''b - ab'' = \alpha\beta C'$, $ab' - a'b = \alpha\beta C''$, il est clair que C, C', C'' sont entiers. Et si l'on prend des nombres entiers K, K', K'' tels que $Kb + K'b' + K''b'' = \beta$, en posant $Ka + K'a' + K''a'' = \alpha h$, et prenant $B = \alpha k - hA$, $B' = \alpha k' - hA'$, $B'' = \alpha k'' - hA''$, les valeurs de B, B', B'', C, C', C'' satisfont aux équations proposées.

En effet, on trouve $aB + a'B' + a''B'' = 0$, $bA + b'A + b''A'' = 0$, d'où $bB + b'B' + b''B'' = \alpha\beta$. Or des valeurs de C', C'', on tire

$$\alpha\beta(B'C'' - B''C') = ab'B' - a'bB' - a''bB'' + ab''B''$$
$$= a(bB + b'B' + b''B'') - b(aB + a'B' + a''B'') = a\alpha\beta;$$

donc $B'C'' - B''C' = a$; de même $B''C - BC'' = a'$, $BC' - B'C = a''$.

Nous sommes forcés au reste de supprimer ici l'analyse qui a conduit à cette solution, ainsi que la méthode par laquelle on déduit toutes les solutions d'une seule.

280. Supposons que la forme binaire $at^2 + 2btu + cu^2 = \varphi$ dont

le déterminant $= D$, soit représentée par la forme ternaire f dont les indéterminées sont x, x', x'', en posant $x = mt + nu$, $x' = m't + n'u$, $x'' = m''t + n''u$, et que la forme F dont les indéterminées sont X, X', X'', soit adjointe à f. On s'assure facilement par le calcul, ou comme conséquence du n° 268, 2°. que le nombre D est représenté par la forme F, en posant $X = m'n'' - m''n'$, $X' = m''n - mn''$, $X'' = mn' - m'n$; nous dirons que cette représentation est *adjointe* à la représentation de la forme φ par la forme f. Si les valeurs de X, X', X'' n'ont pas de commun diviseur, nous appellerons pour abréger, cette représentation *propre*, et dans le cas contraire, *impropre;* et nous transporterons aussi ces dénominations à la représentation de φ par f.

Or la recherche de toutes les représentations du nombre D par la forme F, s'appuie sur les considérations suivantes :

1°. Il n'y a aucune représentation du nombre D par F qui ne puisse se déduire de la représentation d'une certaine forme binaire de déterminant D par la forme f, c'est-à-dire, qui ne soit adjointe à une telle représentation.

Soit en effet $X = L$, $X' = L'$, $X'' = L''$ une représentation quelconque de D par F; on déterminera par le lemme précédent, les nombres m, m', m'', n, n', n'', tels que l'on ait $m'n'' - m''n' = L$, $m''n - mn'' = L'$, $mn' - m'n = L''$; et alors en représentant par $\varphi = at^2 + 2btu + cu^2$, la forme binaire en laquelle f se change par la substitution

$$x = mt + nu, \quad x' = m't + n'u, \quad x'' = m''t + n''u,$$

on voit facilement que D sera le déterminant de la forme φ, et que la représentation de D par F sera adjointe à celle de φ par f.

Exemple. Soit $f = x^2 + x'^2 + x''^2$, et partant, $F = -X^2 - X'^2 - X''^2$, $D = -209$: le nombre -209 sera représenté par F, en faisant $X = 1$, $X' = 8$, $X'' = 12$, on trouve pour les nombres m, m', m'', n, n', n'', les valeurs -20, 1, 1, -12, 0, 1 respectivement, et $\varphi = 402t^2 + 482tu + 145u^2$.

2°. Si φ, χ sont des formes binaires proprement équivalentes, toute représentation de D par F adjointe à une représentation de φ par f, sera aussi adjointe à une représentation de χ par f.

Soient p, q les indéterminées de la forme χ; supposons que φ se change en χ par la substitution propre $t=\alpha p+\beta q$, $u=\gamma p+\delta q$, et que la forme φ soit représentée par f, en faisant

$$x=mt+nu,\ x'=m't+n'u,\ x''=m''t+n''u.....(R)$$

On voit sans peine que si l'on fait

$$\begin{array}{lll} \alpha m+\gamma n=g, & \alpha m'+\gamma n'=g', & \alpha m''+\gamma n''=g'', \\ \beta m+\delta n=h, & \beta m'+\delta n'=h', & \beta m''+\delta n''=h'', \end{array}$$

la forme χ sera représentée par f, en posant

$$x=gp+hq,\ x'=g'p+h'q,\ x''=g''p+h''q.....(R')$$

et l'on trouve $g'h''-h'g''=m'n''-m''n'$, $g''h-gh''=m''n-mn''$, $gh'-g'h=mn'-m'n$, en observant que $\alpha\delta-\beta\gamma=1$. Donc la même représentation de D par F est adjointe aux représentations R et R'.

Ainsi, dans l'exemple précédent on trouve que la forme φ équivaut à la forme $\chi=13p^2-10pq+18q^2$, en laquelle elle se change par la substitution propre $t=-3p+q$, $u=5p-2q$; de là on trouve pour la représentation de χ par f: $x=4q$, $x'=-3p+q$, $x''=2p-q$, qui donne pour le nombre -209 la représentation dont nous étions partis.

3°. Si deux formes φ, χ de déterminant D, dont les indéterminées sont t, u; p, q peuvent être représentées par f, et que la même représentation de D par F soit à-la-fois adjointe à une représentation de φ par f, et à une représentation de χ par f; ces deux formes seront nécessairement équivalentes.

Supposons que φ soit représentée par la forme f, en faisant $x=mt+nu$, $x'=m't+n'u$, $x''=m''t+n''u$, et χ en faisant $x=gp+hq$, $x'=g'p+h'q$, $x''=g''p+h''q$. Supposons en outre qu'on ait $m'n''-m''n'=g'h''-g''h'=L$, $m''n-mn''=g''h-gh''=L'$, $mn'-m'n=gh'-g'h=L''$, on prendra les nombres entiers l, l', l'', tels que l'on ait $Ll+L'l'+L''l''=1$, on fera

$$\begin{array}{l} n'l''-n''l'=M,\ n''l-nl''=M',\ nl'-n'l=M'', \\ l'm''-l''m'=N;\ l''m-lm''=N',\ lm'-l'm=N'', \\ gM+g'M'+g''M''=\alpha,\ hM+h'M'+h''M''=\beta, \\ gN+g'N'+g''N''=\gamma,\ hN+h'N'+h''N''=\delta; \end{array}$$

on déduit facilement de là

$$\alpha m + \gamma n = g - l(gL + g'L' + g''L'') = g \ldots\ldots\ldots$$
$$\beta m + \delta n = h - l(hL + h'L' + h''L'') = h.$$

On trouve de même $\alpha m' + \gamma n' = g'$, $\beta m' + \delta n' = h'$, $\alpha m'' + \gamma n'' = g''$, $\beta m'' + \delta n'' = h''$; il suit de là que $mt + nu$, $m't + n'u$, $m''t + n''u$ se changent en $gp + hq$, $g'p + h'q$, $g''p + h''q$ par la substitution $t = \alpha p + \beta q$, $u = \gamma p + \delta q$ .....(S). D'où il résulte que φ se change par la substitution S, en la même forme en laquelle f se change en posant $x = gp + hq$, $x' = g'p + h'q$, $x'' = g''p + h''q$, c'est-à-dire en χ, et que partant φ est équivalente à χ. D'ailleurs on trouve $\alpha\delta - \beta\gamma = Ll + L'l' + L''l'' = 1$; donc la substitution S est propre, et les formes φ, χ sont proprement équivalentes.

On tire de ce qui précède les règles suivantes pour trouver toutes les représentations propres de D par F. On cherchera toutes les classes de formes binaires de déterminant D, et l'on prendra à volonté une forme dans chaque classe; on cherchera toutes les représentations propres par f de ces différentes formes (en rejetant celles qui ne pourraient pas se représenter par f), et de ces différentes représentations, on déduira celles du nombre D par la forme F. Il est évident (1°. et 2°.) que de cette manière on aura toutes les représentations possibles, et qu'ainsi la solution est complète; et qu'en outre (3°.) les transformations des formes prises dans des classes différentes, produisent nécessairement des représentations différentes.

281. La recherche des représentations impropres d'un nombre donné D par une forme F, se ramène facilement au cas précédent. En effet, il est évident que si D n'est divisible par aucun quarré, il n'y aura aucune représentation de cette espèce; mais si les quarrés λ^2, μ^2, ν^2 sont diviseurs de D, toutes les représentations de D par F s'obtiendront, en cherchant toutes les représentations propres des nombres $\frac{D}{\lambda^2}$, $\frac{D}{\mu^2}$, $\frac{D}{\nu^2}$, etc. par la forme F, et en multipliant les valeurs des indéterminées par λ, μ, ν, etc. respectivement.

Ainsi la recherche de toutes les représentations d'un nombre donné par une forme ternaire donnée, qui est adjointe à une autre forme ternaire, dépend du second problème; et l'on peut

ramener de la manière suivante tous les cas à celui-là, qui paraît n'être qu'un cas très-particulier. Soit D un nombre à représenter par la forme $\left(\begin{smallmatrix} g, & g', & g'' \\ h, & h', & h'' \end{smallmatrix}\right)$, dont le déterminant $=\Delta$, et qui a pour adjointe la forme $\left(\begin{smallmatrix} G, & G', & G'' \\ H, & H', & H'' \end{smallmatrix}\right)=f$; cette dernière aura pour adjointe la forme $\left(\begin{smallmatrix} \Delta g, & \Delta g', & \Delta g'' \\ \Delta h, & \Delta h', & \Delta h'' \end{smallmatrix}\right)=F$, et il est clair que les représentations du nombre ΔD par F qu'on peut trouver par la méthode précédente, sont identiques avec les représentations du nombre D par la forme proposée. On voit au reste que si les coefficiens de la forme f ont μ pour commun diviseur, tous ceux de F seront divisibles par μ^2, et parconséquent ΔD, sans quoi il n'y aurait aucune représentation; les représentations du nombre D par la forme proposée coïncident avec les représentations du nombre $\frac{\Delta D}{\mu^2}$ par la forme qui naît de F en divisant les différens coefficiens par μ^2, et cette forme sera adjointe à celle qui naît de f en divisant les différens coefficiens par μ.

Enfin observons que cette solution du premier problème n'est pas applicable au cas où $D=0$, car alors les formes de déterminant D ne peuvent pas se distribuer en un nombre fini de classes; nous résoudrons plus bas ce cas particulier par une méthode différente.

282. La recherche des représentations d'une forme binaire donnée de déterminant qui n'est pas $=0$, par une forme ternaire donnée, dépend des observations suivantes :

I. De toute représentation propre d'une forme binaire $(p, q, r)=\varphi$ de déterminant D par une forme ternaire f de déterminant Δ, on peut déduire des nombres entiers B, B' tels qu'on ait $B^2\equiv\Delta p$, $BB'\equiv-\Delta q$, $B'^2\equiv\Delta r$ (mod. D), et partant une expression de $\sqrt{\Delta}(p, -q, r)$ (mod. D).

Soit en effet $x=\alpha t+\beta u$, $x'=\alpha' t+\beta' u$, $x''=\alpha'' t+\beta'' u$ une représentation propre de la forme φ par f; x, x', x''; t, u étant les indéterminées des formes f, φ. On prendra des nombres entiers $\gamma, \gamma', \gamma''$, tels que

$$(\alpha'\beta''-\alpha''\beta')\gamma+(\alpha''\beta-\alpha\beta'')\gamma'+(\alpha\beta'-\alpha'\beta)\gamma''=k=\pm 1.$$

Soit $g=\left(\begin{smallmatrix}a, & a', & a''\\ b, & b', & b''\end{smallmatrix}\right)$ la forme en laquelle f se change par la substitution

$$\alpha,\ \beta,\ \gamma;\quad \alpha',\ \beta',\ \gamma';\quad \alpha'',\ \beta'',\ \gamma'',$$

et $G=\left(\begin{smallmatrix}A, & A', & A''\\ B, & B', & B''\end{smallmatrix}\right)$ la forme adjointe à g. Alors il est évident qu'on aura $a=p$, $b''=q$, $a'=r$, $A''=D$ et que Δ sera le déterminant de la forme g, d'où

$$B^2=\Delta p+A'D,\quad BB'=-\Delta q+B''D,\quad B'^2=\Delta r+AD.$$

Ainsi, par exemple, la forme $19t^2+6tu+41u^2$ se représente par la forme $x^2+x'^2+x''^2$, en posant $x=3t+5u$, $x'=3t-4u$, $x''=t$; d'où, en faisant $\gamma=-1$, $\gamma'=1$, $\gamma''=0$, on trouve $B=-171$, $B'=27$, ou $(-171, 27)$ pour une valeur de l'expression $\sqrt{-1}(19, -3, 41)$ (mod. 770).

Il suit de là que si $\Delta(p, -q, r)$ n'est pas résidu quadratique de D, φ ne peut être représenté proprement par aucune forme ternaire de déterminant Δ. Ainsi, dans le cas où Δ et D sont premiers entre eux, Δ doit être le nombre caractéristique de la forme φ.

II. Comme $\gamma, \gamma', \gamma''$ peuvent être déterminés d'une infinité de manières, il en résultera différentes valeurs pour B, B', et nous allons chercher quelle relation elles ont entre elles. Supposons que δ, δ', δ'' soient aussi tels que

$$(\alpha'\beta''-\alpha''\beta')\delta+(\alpha''\beta-\alpha\beta'')\delta'+(\alpha\beta'-\alpha'\beta)\delta''=k',$$

k' pouvant être $+1$ et -1, et que la forme f se change, par la substitution

$$\alpha,\ \beta,\ \delta;\quad \alpha',\ \beta',\ \delta';\quad \alpha'',\ \beta'',\ \delta'',$$

en la forme $\left(\begin{smallmatrix}m, & m', & m''\\ n, & n', & n''\end{smallmatrix}\right)=h$, dont l'adjointe est $\left(\begin{smallmatrix}M, & M', & M''\\ N, & N', & N''\end{smallmatrix}\right)=H$; alors g et h seront équivalentes ainsi que G et H; et par l'application des principes des nos 169 et 170, on trouvera que la forme H se change en la forme G par la substitution

$$k,\ 0,\ 0;\quad 0,\ k,\ 0;\quad \zeta,\ \eta,\ k,$$

en faisant

$$(\beta'\gamma''-\beta''\gamma')\delta+(\beta''\gamma-\beta\gamma'')\delta'+(\beta\gamma'-\beta'\gamma)\delta''=\zeta,$$
$$(\gamma'\alpha''-\gamma''\alpha')\delta+(\alpha\gamma''-\alpha''\gamma)\delta'+(\gamma\alpha'-\alpha\gamma')\delta''=\eta.$$

On tirera de là $B \equiv \eta k' D + kk' N$, $B' \equiv \zeta k' D + kk' N'$, et partant, comme $kk' = \pm 1$, $B \equiv N$, $B' \equiv N'$, ou $B \equiv -N$, $B' \equiv -N'$ (mod. D). Dans le premier cas, les valeurs de (B, B'), (N, N') seront dites équivalentes; dans le second, opposées. Nous dirons aussi d'une représentation de la forme φ, qu'elle *appartient* à la valeur de $\sqrt{\Delta}(p, -q, r)$, lorsqu'on peut l'en déduire par la méthode (I). Ainsi toutes les valeurs auxquelles appartient la même représentation sont équivalentes ou opposées.

III. Réciproquement, si une représentation de φ par f est $\alpha t + \beta u$, etc., et appartient à la valeur (B, B'), qu'on en déduit à l'aide de la transformation

$$\alpha, \beta, \gamma; \quad \alpha', \beta', \gamma'; \quad \alpha'', \beta'', \gamma'',$$

elle appartiendra à toute autre valeur (N, N') qui lui sera équivalente ou opposée; c'est-à-dire, qu'au lieu des nombres $\gamma, \gamma', \gamma''$, on pourra prendre d'autres nombres $\delta, \delta', \delta''$, pour lesquels l'équation

$$(\alpha'\beta'' - \alpha''\beta')\delta + (\alpha''\beta - \alpha\beta'')\delta' + (\alpha\beta' - \alpha'\beta)\delta'' = \pm 1 \ldots\ldots \Omega$$

ait lieu, et tels que les coefficiens 4 et 5 de la forme adjointe à celle en laquelle f se change par la substitution

$$\alpha, \beta, \delta; \quad \alpha', \beta', \delta'; \quad \alpha'', \beta'', \delta'',$$

soient respectivement égaux à N, N'. Soit, en effet, $\pm B = N + \eta D$, $\pm B' = N' + \zeta D$, en prenant ici et après les signes supérieurs ou inférieurs, suivant que les valeurs (B, B'), (N, N') sont équivalentes ou opposées, ζ, η seront entiers, et si la forme g se change par la substitution

$$1, 0, \zeta; \quad 0, 1, \eta; \quad 0, 0, \pm 1,$$

en la forme h. On verra sans peine que le déterminant de h est Δ, et que les coefficiens 4 et 5 de sa forme adjointe sont N, N'. Or en faisant

$$\alpha\zeta + \beta\eta \pm \gamma = \delta, \quad \alpha'\zeta + \beta'\eta \pm \gamma' = \delta', \quad \alpha''\zeta + \beta''\eta \pm \gamma'' = \delta'',$$

on verra sans peine que f se change en h par la substitution S, et que l'équation Ω est satisfaite.

283. On déduit de ces principes la méthode suivante, pour trouver toutes

toutes les représentations de la forme binaire $\varphi = pt^2 + 2qtu + ru^2$ de déterminant D, par la forme ternaire f de déterminant Δ.

I. On cherchera toutes les valeurs différentes, c'est-à-dire, non équivalentes de l'expression $\sqrt{\Delta}(p, -q, r)$ (mod. D). Ce problème a déjà été résolu (n° 233) pour le cas où Δ est premier avec D, et où la forme $(p, -q, r)$ est primitive, et les autres cas se ramènent très-facilement à celui-là. La nécessité d'abréger ne nous permet cependant pas d'insister davantage sur ce sujet. Observons seulement que lorsque Δ est premier avec D, l'expression $\Delta(p, -q, r)$ ne peut être résidu quadratique de D, à moins que φ ne soit une forme primitive : supposons en effet $\Delta p = B^2 - DA'$, $-\Delta q = BB' - DB''$, $\Delta r = B'^2 - DA$; on en déduit $(DB'' - \Delta q)^2 = (DA' + \Delta p)(DA + \Delta r)$, ou en développant et remplaçant D par $q^2 - pr$,

$$(q^2 - pr)(B''^2 - AA') - \Delta(Ap + 2B''q + A'r) + \Delta^2 = 0.$$

Si donc p, q, r avaient un commun diviseur, ce diviseur diviserait Δ^2, et parconséquent Δ ne pourrait pas être premier avec D. Ainsi φ sera une forme primitive.

II. Désignons par m le nombre de ces valeurs, et supposons qu'il s'en trouve n opposées à elles-mêmes. Alors il est évident que parmi les $m - n$ qui restent, chacune aura nécessairement son opposée, car nous supposons qu'on a toutes les valeurs non équivalentes. De chaque couple de valeurs opposées, on en rejettera une à volonté, et il en restera en tout $\frac{1}{2}(m+n)$. Ainsi, par exemple, des huit valeurs de l'expression $\sqrt{-1}$ (19, 3, 41) (mod. 770) qui sont : (39, 237), (171, −27), (269, −83), (291, −127), (−39, −237), (−171, 27), (−269, 83), (−291, 127), les quatre dernières sont à rejeter, comme opposées aux quatre premières. Au reste, il est aisé de voir que si (B, B') est une valeur opposée à elle-même, $2B$, $2B'$, et partant $2\Delta p$, $2\Delta q$, $2\Delta r$ sont divisibles par D ; donc dans le cas où Δ et D sont premiers entre eux, il faudrait que $2p$, $2q$, $2r$ fussent divisibles par D, et comme dans ce cas (I) les nombres p, q, r n'ont pas de diviseur commun, 2 doit être divisible par D, et partant la chose ne peut avoir lieu que pour $D = \pm 1$, ou $D = \pm 2$. Donc si Δ

est premier avec D, on aura $n=0$ pour les valeurs de D plus grandes que 2.

III. Cela fait, il est évident que toute représentation propre de la forme φ par f appartient nécessairement à quelqu'une des $\frac{m+n}{2}$ valeurs restantes, et à une seule; ainsi il faut parcourir ces différentes valeurs, et chercher les représentations qui appartiennent à chacune d'elles.

Pour trouver les représentations qui appartiennent à une valeur donnée (B, B'), il faut déterminer d'abord une forme ternaire $g=\left(\begin{smallmatrix} a, & a', & a'' \\ b, & b', & b'' \end{smallmatrix}\right)$ dont le déterminant soit Δ, et dans laquelle on ait $a=p$, $b''=q$, $a'=r$, $ab-b'b''=B$, $a'b'-bb''=B'$; les valeurs de b, b', a'' se déduisent de là, à l'aide des équations du n° 276, II, par lesquelles on voit facilement que lorsque D et Δ sont premiers entre eux, les nombres b, b', a'' sont nécessairement entiers, puisque les produits de ces nombres par D et Δ sont des nombres entiers; mais en général si l'un de ces trois nombres se trouve fractionnaire, ou si les formes f, g ne sont pas équivalentes, il n'y aura aucunes représentations de φ par f appartenantes à la valeur (B, B'); mais si b, b', a'' sont entiers et que les formes f, g soient équivalentes, toute transformation de f en g, comme

$$\alpha, \beta, \gamma; \quad \alpha', \beta', \gamma'; \quad \alpha'', \beta'', \gamma'',$$

donne une représentation telle que $x=\alpha t+\beta u$, $x'=\alpha' t+\beta' u$, $x''=\alpha'' t+\beta'' u$; et de cette manière il n'y a aucune représentation qui ne puisse se déduire d'une transformation. Ainsi la partie du second problème, relative aux représentations propres, est ramenée au troisième problème.

IV. Au reste, les différentes transformations de f en g produisent toujours des représentations différentes, excepté le seul cas où (B, B') est une valeur opposée à elle-même, dans lequel deux transformations ne donnent qu'une seule représentation. Supposons, en effet, que f se change aussi en g par la substitution

$$\alpha, \beta, \delta; \quad \alpha', \beta', \delta'; \quad \alpha'', \beta'', \delta'',$$

qui donne la même représentation que la précédente, et désignant

par k, k', ζ, η les mêmes nombres qu'en II, n° précédent, on aura $B=kk'B+\eta k'D$, $B'=kk'B'+\zeta k'D$; si donc chacun des nombres k, $k'=+1$ ou -1, on aura $\eta=0$, $\zeta=0$, d'où l'on déduit facilement $\delta=\gamma$, $\delta'=\gamma'$, $\delta''=\gamma''$. Ainsi ces deux transformations ne pourront être différentes que dans le cas où l'un des nombres k, k' est $+1$ et l'autre -1. Or alors $B\equiv -B$, $B'\equiv -B'$ (mod. D), c'est-à-dire que la valeur (B, B') est opposée à elle-même.

V. Il suit facilement de ce que nous avons dit (n° 271) sur les caractères des formes définies et indéfinies, que si Δ est positif, D négatif et φ une forme négative, g est une forme définie négative, et que si Δ est positif et D positif ou négatif, mais φ une forme positive, g est une forme indéfinie. Or comme f, g ne peuvent être équivalentes, à moins qu'à cet égard elles ne soient semblables, il est évident que des formes binaires de déterminant positif et les formes positives ne peuvent être représentées proprement par une forme ternaire indéfinie de déterminant positif, et que par une forme ternaire de la première ou de la deuxième espèce, on ne peut représenter que des formes binaires de la deuxième ou de la première respectivement. On peut conclure de la même manière, que par une forme ternaire définie de déterminant négatif (qui est positive), on ne peut représenter que des formes binaires positives, et par une forme ternaire indéfinie de déterminant négatif, que des formes binaires négatives et des formes de déterminant positif.

284. Comme les représentations *impropres* d'une forme binaire φ de déterminant D, par une forme ternaire f qui a pour adjointe F, sont celles d'où l'on déduit les représentations impropres du nombre D par la forme F, il est évident que φ ne peut être représenté improprement par f, à moins que D n'ait des diviseurs quarrés. Supposons que les différens diviseurs quarrés de D, non compris 1, soient e^2, e'^2, e''^2, etc., dont le nombre sera toujours fini puisque D ne peut pas être $=0$, toute représentation impropre de φ par f donnera une représentation du nombre D par F, dans laquelle les valeurs des indéterminées auront pour plus grand commun diviseur l'un des nombres e, e', e'', etc. Par cette raison, nous dirons, pour abréger, que toute représen-

tation impropre de la forme φ *dépend* du diviseur quarré e^2, ou e'^2, ou e''^2, etc. qui lui correspond. Or toutes les représentations de la forme φ dépendantes d'un diviseur quarré e^2, dont nous supposons la racine e prise positivement, se trouvent de la manière suivante. De la démonstration synthétique que nous en donnons, pour abréger, on pourra facilement déduire l'analyse qui nous y a conduits.

1°. On cherchera toutes les formes binaires de déterminant $\frac{D}{e^2}$ qui se changent en la forme φ par la substitution $T=\alpha t+\lambda u$, $U=\mu u$, T et U désignant les indéterminées d'une telle forme, t, u les indéterminées de la forme φ; α, μ des entiers positifs dont le produit est parconséquent $=e$, λ un entier positif moindre que μ, ou zéro. Ces formes, ainsi que les transformations qui leur répondent, se trouvent ainsi qu'il suit :

On égalera successivement α aux différens diviseurs positifs de e, y compris 1 et e, l'on fera $\mu=\frac{e}{\alpha}$; pour chacune des valeurs déterminées de α, μ, on donnera à λ toutes les valeurs entières depuis 0 jusqu'à $\mu-1$, et l'on aura certainement toutes les transformations. Or la forme qui se change en φ par la substitution $T=\alpha t+\lambda u$, $U=\mu u$, se trouve en cherchant la forme en laquelle φ se change par la substitution $t=\frac{T}{\alpha}-\frac{\lambda U}{e}$, $u=\frac{U}{\mu}$, et l'on obtiendra les formes qui répondent à chacune des transformations; mais il ne faudra conserver que celles dont les trois coefficiens sont entiers (*).

2°. Soit Φ une de ces formes qui se change en φ par la substitution $T=\alpha t+\lambda u$, $U=\mu u$; on cherchera toutes les représentations propres de Φ par f, s'il en existe; supposons-les représentées indéfiniment par

$$x=AT+BU,\ x'=A'T+B'U,\ x''=A''T+B''U.....(P);$$

(*) Si nous pouvions donner plus de détails sur ce problème, nous abrégerions beaucoup la solution. Il est d'abord évident que α doit être choisi de manière à ce que son quarré soit diviseur du premier coefficient de φ. Au reste, nous nous réservons de reprendre dans une autre occasion ce problème, d'où l'on peut tirer des solutions plus simples des problèmes des n°s 213, 214.

en substituant dans ces formules les valeurs de T, U, on en déduit les suivantes :

$$x = \alpha t + \beta u,\quad x' = \alpha' t + \beta' u,\quad x'' = \alpha'' t + \beta'' u \ldots\ldots (Q),$$

dans lesquelles on a de même

$$\alpha = \varkappa A,\qquad \alpha' = \varkappa A',\qquad \alpha'' = \varkappa A'',$$
$$\beta = \lambda A + \mu B,\quad \beta' = \lambda A' + \mu B',\quad \beta'' = \lambda A'' + \mu B'' \ldots\ldots (R).$$

On traitera de la même manière les autres formes, s'il y en a plusieurs, et je dis qu'on aura ainsi toutes les représentations de la forme φ dépendantes du diviseur quarré e^2.

I. Nous ne nous arrêterons pas à prouver que f se change en φ par la substitution (Q), cette partie de la proposition étant évidente; mais on déduit des valeurs de α, α', etc.

$$\alpha'\beta'' - \alpha''\beta' = (A'B'' - A''B')e,\quad \alpha''\beta - \alpha\beta'' = (A''B - AB'')e,$$
$$\alpha\beta' - \alpha'\beta = (AB' - A'B)e;$$

et comme (P) est une représentation propre, il s'ensuit que le plus grand commun diviseur de ces trois nombres est e, et que la représentation (Q) dépend du diviseur e^2.

II. Nous allons maintenant faire voir que de toute représentation donnée de la forme φ, on peut déduire une représentation propre d'une forme de déterminant $\frac{D}{e^2}$ contenue parmi les formes trouvées par la première règle; c'est-à-dire, que des valeurs données de α, α', α'', β, β', β'', on peut déduire des valeurs entières de $\varkappa$, λ, μ qui satisfassent aux conditions prescrites, et des valeurs de A, B, A', B', A'', B'' qui satisfassent aux équations (R), et cela d'une seule manière. Il est clair d'abord par les trois premières équations (R), que l'on doit prendre pour $\varkappa$ le plus grand commun diviseur des nombres α, α', α'' pris positivement, puisque $A'B'' - A''B'$, $A''B - AB''$, $AB' - A'B$ ne devant pas avoir de diviseur commun A, A', A'' n'en auront pas non plus. Donc A, A', A'' seront déterminés, ainsi que μ qui doit être égal à $\frac{e}{\varkappa}$, et sera nécessairement un nombre entier. Soient trois nombres entiers k, k, k', tels qu'on ait $kA + k'A' + k''A'' = 1$, les trois dernières équations

(*R*) donnent, en faisant $kB + k'B' + k''B'' = m$,

$$k\beta + k'\beta' + k''\beta'' = \lambda + m\mu,$$

d'où il suit qu'il n'y a qu'une seule valeur de λ comprise entre 0 et $\mu - 1$; les valeurs de B, B', B'', sont alors déterminées, et il ne reste qu'à démontrer qu'elles sont entières. Or on aura

$$B = \frac{1}{\mu}(\beta - A\lambda) = \frac{1}{\mu}\{\beta(1 - kA) - A(k'\beta' + k''\beta'')\} + Am$$

$$= \frac{1}{\mu}\{k''(A''\beta - A\beta'') - k'(A\beta' - A'\beta)\} + Am$$

$$= \frac{1}{e}\{k''(\alpha''\beta - \alpha\beta'') - k'(\alpha\beta' - \alpha'\beta)\} + Am.$$

Donc B est nécessairement entier. On le démontrera de même pour B', B''. Il suit de ces raisonnemens qu'il n'y a aucune représentation impropre de φ par f dont on ne puisse déduire une représentation propre d'une forme φ par f, et dont on puisse en déduire plusieurs. Donc la méthode précédente donnera toutes les représentations cherchées, et n'en donnera que de différentes.

En appliquant la même méthode aux autres diviseurs quarrés de D, on trouvera toutes les représentations impropres possibles de φ par f.

Au reste, on voit aisément par cette solution, que le théorème énoncé à la fin du n° précédent pour les représentations propres, a lieu également pour les représentations impropres, c'est-à-dire, qu'en général aucune forme binaire positive de déterminant négatif ne peut être représentée par une forme ternaire négative, etc. En effet, soit une forme φ, qui par ce théorème ne puisse être représentée proprement par f; les formes de déterminant $\frac{D}{e^2}, \frac{D}{e'^2}$, etc. qui renferment φ, ne pourront non plus être représentées par f, puisque leur déterminant sera affecté de même signe que celui de φ; et lorsque ces déterminans sont positifs, toutes les formes sont positives ou négatives, suivant l'espèce de la forme φ.

285. Nous ne pouvons placer ici que peu de détails sur les questions qui font le sujet du troisième problème, auquel nous avons réduit les deux autres, c'est-à-dire sur la manière de juger si deux formes ternaires de même déterminant sont équivalentes,

ou non ; et dans le premier cas, de trouver toutes les transformations de l'une en l'autre; parceque la solution complète, telle que nous l'avons donnée pour les formes binaires, est sujette à beaucoup de difficultés. Aussi nous bornerons ici notre recherche à quelques cas particuliers pour lesquels nous avons fait cette digression.

I. Pour le déterminant $+1$, nous avons fait voir plus haut que toutes les formes ternaires se distribuent en deux classes, dont l'une contient toutes les formes indéfinies, et l'autre toutes les formes définies (négatives). Il suit de là que deux formes quelconques de déterminant $+1$ sont équivalentes si elles sont toutes deux définies ou toutes deux indéfinies, mais qu'elles ne le sont pas si l'une est indéfinie et l'autre définie. (Cette seconde partie de la propoposition a lieu pour un déterminant quelconque). De la même manière, deux formes indéfinies de déterminant -1 sont équivalentes, si elles sont toutes deux définies ou toutes deux indéfinies. — Deux formes définies de déterminant 2 seront toujours équivalentes; deux formes indéfinies le seront aussi, à moins que dans l'une les trois premiers coefficiens ne soient pairs, et qu'ils ne les soient pas tous dans l'autre. — Nous pourrions donner plusieurs propositions particulières de la même manière, si nous avions plus haut (n° 277) calculé un plus grand nombre d'exemples.

II. On pourra aussi pour tous ces cas, f, f' désignant deux formes ternaires équivalentes, trouver une transformation de l'une en l'autre. Car pour chaque classe nous avons assigné un assez petit nombre de formes, à l'une desquelles toute forme de cette classe peut être ramenée; nous avons aussi appris à réduire toutes ces formes à une seule. Soit F cette forme de la même classe que f, f', on pourra par les moyens indiqués, trouver les transformations de f, f' en F, et partant, de F en f, f'. Ainsi par le n° 270, on pourra déduire les transformations de f en f' et de f' en f.

III. Ainsi il ne resterait plus qu'à montrer comment d'une seule transformation de f en f', on peut tirer toutes les transformations possibles; ce problème dépend d'un autre plus simple qui consiste à trouver toutes les transformations de la forme f en elle-même. En

effet, si f se change en elle-même par plusieurs substitutions (τ), (τ'), (τ''), etc., et en f' par la substitution (t), il est aisé de voir qu'en combinant par la méthode du n° 270, la transformation (t) avec (τ), (τ'), (τ''), il en résulte des transformations par lesquelles f se change en f'. En outre, on peut prouver facilement par le calcul, que toute transformation de f en f' peut se déduire de cette manière, de la combinaison de la transformation (t) de f en f' avec une, et une seule transformation de la forme f en elle-même, et que parconséquent la combinaison de la transformation (t) avec les différentes transformations de f en elle-même, donne toutes les transformations de f en f', et ne donnera qu'une fois chacune d'elles.

Nous bornerons ici notre recherche au cas où f est une forme définie dont les coefficiens 4, 5, 6 sont $=0$ (*). Soit donc $f=\begin{pmatrix} a, & a', & a'' \\ 0, & 0, & 0 \end{pmatrix}$, et représentons une substitution quelconque qui change f en elle-même, par

$$\alpha,\ \beta,\ \gamma;\quad \alpha',\ \beta',\ \gamma';\quad \alpha'',\ \beta'',\ \gamma'',$$

on aura les équations

$$\left.\begin{array}{l} a\alpha^2+a'\alpha'^2+a''\alpha''^2=a,\ a\beta^2+a'\beta'^2+a''\beta''^2=a',\ a\gamma^2+a'\gamma'^2+a''\gamma''^2=a'' \\ a\alpha\beta+a'\alpha'\beta'+a''\alpha''\beta''=0,\ a\alpha\gamma+a'\alpha'\gamma'+a''\alpha''\gamma''=0,\ a\beta\gamma+a'\beta'\gamma'+a''\beta''\gamma''=0 \end{array}\right\}(\omega)$$

Or on doit distinguer trois cas:

1°. Quand a, a', a'', qui doivent avoir le même signe, sont tous inégaux, nous supposerons $a<a'$, $a'<a''$; si l'ordre de grandeur était différent, on trouverait de même les conclusions analogues. La première des équations (ω) exige nécessairement que l'on ait $\alpha'=\alpha''=0$, et partant $\alpha=\pm 1$; les équations 4, 5 donnent alors $\beta=0$, $\gamma=0$; l'équation 2 donne $\beta''=0$ et $\beta'=\pm 1$, et l'équation 6 exige qu'on ait $\gamma'=0$; donc par l'équation 3, $\gamma''=\pm 1$; desorte que, à cause de l'ambiguité des signes, il y a en tout huit transformations différentes.

(*) Les autres cas où la forme f est définie, peuvent se ramener à celui-là; mais si elle est indéfinie, il faut employer une méthode tout-à-fait différente, et le nombre des transformations est infini.

2°. Quand parmi les nombres a, a', a'' il y en a deux égaux, a' et a'', par exemple, supposons d'abord $a<a'$. Alors, de la même manière que dans le cas précédent, on aura $\alpha'=0$, $\alpha''=0$, $\alpha=\pm 1$, $\beta=0$, $\gamma=0$; les équations 2, 3, 6 deviennent $\beta'^2+\beta''^2=1$, $\gamma'^2+\gamma''^2=1$, $\beta'\gamma'+\beta''\gamma''=0$; d'où l'on tire $\beta'=0$, $\beta''=\pm 1$, $\gamma'=\pm 1$, $\gamma''=0$, ou $\beta'=\pm 1$, $\beta''=0$, $\gamma'=0$, $\gamma''=\pm 1$. Mais si $a>a'$, les équations 2 et 3 donnent $\beta=0$, $\gamma=0$ et $\beta'=0$, $\beta''=\pm 1$, $\gamma'=\pm 1$, $\gamma''=0$, ou $\beta'=\pm 1$, $\beta''=0$, $\gamma'=0$, $\gamma''=\pm 1$; l'une ou l'autre supposition donnent, par les équations 4 et 5, $\alpha'=0$, $\alpha''=0$, et par l'équation 1, $\alpha=\pm 1$. Ainsi dans les deux cas il y a seize transformations différentes. Les deux autres cas où $a=a''$, ou bien $a=a'$ se résolvent de la même manière, pourvu qu'on change α, α', α'', pour le premier cas, en β, β', β''; pour le second, en γ, γ', γ'' respectivement.

3°. Quand les nombres a, a', a'' sont égaux, les équations 1, 2, 3 exigent que des nombres α, α', α'', ainsi que des nombres β, β', β'', et des nombres γ, γ', γ'' deux soient égaux à zéro et le troisième égal à ± 1; or, par les équations 4, 5, 6, on voit qu'il ne peut y avoir qu'un seul nombre $=\pm 1$ parmi α, β, γ, ou α', β', γ', ou α'', β'', γ''. Il ne reste que six combinaisons.

$$\left.\begin{array}{|c|c|c|c|c|c|}\alpha & \alpha & \alpha' & \alpha' & \alpha'' & \alpha''=\pm 1\\ \beta' & \beta'' & \beta & \beta'' & \beta & \beta'=\pm 1\\ \gamma'' & \gamma' & \gamma'' & \gamma & \gamma' & \gamma=\pm 1\end{array}\right\}, \text{ et les six autres coefficiens } =0;$$

desorte que par l'ambiguité des signes il y a en tout quarante-huit transformations. — Le même tableau renferme aussi les cas précédens; mais des six colonnes il ne faut prendre que la première, quand a, a', a'' sont tous inégaux; la première et la seconde, quand $a'=a''$; la première et la troisième, quand $a=a'$; la première et la sixième, quand $a=a''$.

Il suit de là que si la forme $f=ax^2+a'x'^2+a''x''^2$ se change en la forme équivalente f' par la substitution

$$x=\delta y+\varepsilon y'+\zeta y'', \quad x'=\delta' y+\varepsilon' y'+\zeta' y'', \quad x''=\delta'' y+\varepsilon'' y'+\zeta'' y'',$$

toutes les transformations de f en f' sont contenues dans le tableau suivant:

$$\begin{vmatrix} x & x \\ x' & x'' \end{vmatrix} \begin{vmatrix} x' & x' \\ x & x'' \end{vmatrix} \begin{vmatrix} x'' & x'' \\ x & x' \end{vmatrix} = \pm(\delta y + \varepsilon y' + \zeta y'')$$
$$\begin{vmatrix} x' & x'' \\ x'' & x' \end{vmatrix} \begin{vmatrix} x & x' \\ x'' & x \end{vmatrix} \begin{vmatrix} x'' & x \\ x' & x \end{vmatrix} = \pm(\delta' y + \varepsilon' y' + \zeta' y'')$$
$$\begin{vmatrix} x'' & x' \\ x' & x'' \end{vmatrix} \begin{vmatrix} x' & x \\ x'' & x \end{vmatrix} \begin{vmatrix} x'' & x \\ x' & x \end{vmatrix} = \pm(\delta'' y + \varepsilon'' y' + \zeta'' y''),$$

avec cette différence que l'on doit employer les six colonnes lorsque $a=a'=a''$; la première et la seconde, quand $a'=a''$; la première et la troisième, quand $a=a'$; la première et la sixième, quand $a=a''$; enfin la première seule, quand a, a', a'' sont tous inégaux, et il y aura dans le premier cas quarante-huit transformations, seize dans le second, le troisième et le quatrième, et huit dans le cinquième.

Après avoir exposé succinctement les premiers élémens des formes ternaires, nous allons passer à quelques applications particulières, parmi lesquelles le problème suivant mérite la première place.

286. Problème. *Etant donnée une forme binaire* F=(A, B, C) *de déterminant* D *appartenant au genre principal, trouver une forme binaire* f *qui donne* F *par sa duplication.*

1°. On cherchera une représentation propre de la forme $(A, -B, C)=F'$ par la forme ternaire x^2-2yz; supposons qu'elle soit

$$x=\alpha T+\beta U, \quad y=\alpha' T+\beta' U, \quad z=\alpha'' T+\beta'' U.$$

Il est aisé de voir, par la théorie précédente, que la chose est toujours possible. En effet, F étant, par hypothèse, du genre principal, on pourra trouver une valeur de l'expression $\sqrt{(A, B, C)}$ (mod. D) (233, 6°), et parconséquent une forme ternaire φ de déterminant 1, dans laquelle la forme $(A, -B, C)$ entre comme partie, et dont l'on voit facilement que tous les coefficiens sont entiers. Il est également clair que la forme φ doit être indéfinie, puisque, par hypothèse, F n'est certainement pas une forme négative; donc φ sera équivalente à la forme x^2-2yz; on pourra parconséquent assigner une transformation de x^2-2yz en φ, qui fournira une représentation propre de F' par la forme x^2-2yz; d'ailleurs on aura $A=\alpha^2-2\alpha'\alpha''$, $-B=\alpha\beta-\alpha'\beta''-\alpha''\beta'$, $C=\beta^2-2\beta'\beta''$; d'où l'on voit qu'en faisant $\alpha\beta'-\alpha'\beta=a$,

$\alpha'\beta''-\alpha''\beta'=b$, $\alpha''\beta-\alpha\beta''=c$, ces nombres n'auront pas de commun diviseur, et qu'on aura $D=b^2-2ac$.

2°. De là et à l'aide de la dernière observation du n° 235, on peut facilement conclure que F, par la substitution $2\beta'$, β, β, β''; $2\alpha'$, α, α, α'', se change en le produit de la forme $(2a, -b, c)$ par elle-même, et par la substitution β', β, β, $2\beta''$; α', α, α, $2\alpha''$, en le produit de la forme $(a, -b, 2c)$ par elle-même. Or le plus grand commun diviseur des nombres $2a$, $2b$, $2c$ est 2; si donc c est impair, $2a$, $2b$, c n'auront pas de commun diviseur, et la forme $(2a, -b, c)$ sera une forme proprement primitive. De même si a est impair $(a, -b, 2c)$ sera une forme proprement primitive; dans le premier cas, F naît de la duplication de la forme $(2a, -b, c)$, et dans le deuxième, de la duplication de la forme $(a, -b, 2c)$. (Voyez Conclus. 4, n° 235). Or un de ces cas arrivera nécessairement. En effet, si a, c étaient tous deux pairs, b serait nécessairement impair; or on s'assure aisément que l'on a $\beta''a+\beta b+\beta' c=0$, $\alpha''a+\alpha b+\alpha' c=0$; donc βb et αb, et partant α et β seraient tous les deux pairs; A et C le seraient donc aussi, ce qui est contre l'hypothèse, puisque F est une forme du genre principal, et parconséquent de l'ordre proprement primitif. Au reste il peut arriver que a et c soient impairs, et dans ce cas on a deux formes qui produisent F par leur duplication.

Soit proposée, par exemple, la forme $F=(5, 2, 31)$ de déterminant -151; on trouve $(55, 22)$ pour valeur de l'expression $\sqrt{(5, 2, 31)}$; donc la forme ternaire $\varphi=\begin{pmatrix}5, & 31, & 4\\ 11, & 0, & -2\end{pmatrix}$. Or par les règles du n° 272, on trouve la forme $\begin{pmatrix}1, & 1, & -1\\ 0, & 0, & 0\end{pmatrix}$ équivalente à φ, et qui se change en elle par la substitution

$$2, 2, 1;\quad 1, -6, -2;\quad 0, 3, 1.$$

De là, à l'aide des transformations consignées n° 277, on trouve que $\begin{pmatrix}1, & 0, & 0\\ -1, & 0, & 0\end{pmatrix}$ se change en φ par la substitution

$$5, -7, -2;\quad 2, -1, 0;\quad 1, -9, -3;$$

ainsi $a=11$, $b=-17$, $c=20$. Et comme a est impair, F naît

de la duplication de la forme (11, 17, 40), et se change en le produit de cette forme par elle-même, par la substitution —1, —7, —7, —18; 2, 3, 3, 2.

287. Nous ajouterons les observations suivantes sur le problème précédent.

1°. Si une forme F se change, par la substitution p, p', p'', p'''; q, q', q'', q''', en le produit des deux formes (h, i, k), (h', i', k'), toutes deux étant prises directement, comme nous le supposons toujours, on déduira facilement de la troisième conclusion du n° 235 les équations

$$\begin{aligned} p''hn' - p'h'n - p(in' - i'n) &= 0, \\ (p'' - p')(in' + i'n) - p(kn' - k'n) + p'''(hn' - h'n) &= 0, \\ p'kn' - p''k'n - p'''(in' - i'n) &= 0, \end{aligned}$$

et trois autres qu'on obtient en remplaçant dans celles-ci p, p', p'', p''' par q, q', q'', q'''. n et n' sont les racines quarrées positives des quotiens qui résultent de la division des déterminans des formes (h, i, k), (h', i', k') par celui de la forme F. Si donc ces formes sont identiques ou qu'on ait $n = n'$, $h = h'$, $i = i'$, $k = k'$, les équations précédentes deviennent $(p'' - p')\,hn = 0$, $(p'' - p')\,in = 0$; $(p'' - p')\,kn = 0$; donc on a nécessairement $p' = p''$, et absolument de la même manière, $q' = q''$; ainsi, en donnant aux formes (h, i, k), (h', i', k') les mêmes indéterminées t et u, et désignant par T, U les indéterminées de la forme F, F se changera en $(ht^2 + 2itu + ku^2)^2$, par la substitution

$$T = pt^2 + 2p'tu + p'''u^2, \quad U = qt^2 + 2q'tu + q'''u^2.$$

2°. Si la forme F naît de la duplication de la forme f, elle naîtra aussi de la duplication de toute forme contenue dans la même classe que f, ou la classe de la forme F naîtra de la duplication de la classe de la forme f (n° 238). Ainsi dans l'exemple du n° précédent, (5, 2, 31) naîtra aussi de la duplication de la forme (11, —5, 16), proprement équivalente à (11, 17, 40). Une fois qu'on connaît une classe de la duplication de laquelle résulte la classe de la forme F, on les trouvera toutes, s'il y en a plusieurs, à l'aide du problème du n° 260. Dans notre exemple, il n'y a pas d'autre classe positive de cette espèce, parcequ'il

n'y a qu'une seule classe ambiguë proprement primitive et positive de déterminant — 151, qui est la classe principale. Comme de la composition de la seule classe ambiguë négative (—1, 0, —151) avec la classe (11, —5, 16), il résulte la classe (—11, —5, —16); celle-ci sera la seule classe négative dont la duplication donne la classe (5, 2, 31).

3°. Comme la solution du problème du n° précédent prouve que toute classe de formes binaires qui est proprement primitive, positive et qui appartient au genre principal, résulte de la duplication d'une classe proprement primitive de même déterminant, le théorème du n° 261, par lequel nous étions certains qu'il y avait au moins la moitié de tous les caractères assignables pour un déterminant D non quarré, auxquels ne répondît aucun genre proprement primitif-positif, reçoit par là plus de développement; puisque nous voyons qu'il y a *moitié* de ces caractères auxquels répondent des genres, et *moitié* auxquels il n'en répond aucun (Voyez la démonstration de ce théorème). Donc, puisque nous avons distribué (n° 263) tous ces caractères assignables en deux espèces P et Q, composées d'un même nombre, desquelles la dernière, Q, ne pouvait répondre aux formes proprement primitives positives, tandis qu'il était incertain si chaque caractère de l'espèce P répondait effectivement à quelque genre; maintenant il ne reste aucun doute qu'il n'y a aucun caractère de cette espèce auquel ne réponde un genre.

On déduit facilement aussi de là, pour le déterminant négatif dans l'ordre proprement primitif négatif, à l'égard duquel nous avons prouvé (n° 264, 1°) qu'il n'y avait d'admissibles que les caractères Q, qu'ils le sont tous effectivement. Soit en effet K un des caractères de Q, f une forme quelconque de l'ordre proprement primitif négatif de déterminant D, et K' son caractère, K' appartiendra à l'espèce Q; donc le caractère composé de K et K', d'après le n° 246, appartiendra à l'espèce P, et partant il y a des formes positives proprement primitives de déterminant D, qui lui répondent; en composant donc une de ces formes avec la forme f, il en naîtra une proprement primitive négative de déterminant D dont le caractère sera K.

On prouverait absolument de la même manière, pour l'ordre improprement primitif, que les caractères démontrés *seuls* possibles (n° 264, 2° et 3°) sont *tous* possibles, qu'ils soient de l'espèce P ou de l'espèce Q.

Ces théorèmes, si nous ne nous trompons étrangement, doivent être rangés parmi les plus beaux de la théorie des formes binaires, surtout parceque, malgré leur grande simplicité, ils sont tellement cachés qu'il n'est pas possible d'en donner la démonstration rigoureuse, sans le secours d'un grand nombre d'autres recherches.

Nous passons maintenant à une autre application de la digression précédente, savoir, la décomposition, tant des nombres que des formes binaires en trois quarrés. Nous résoudrons d'abord le problème suivant :

288. PROBLÈME. M *étant un nombre positif, trouver les conditions auxquelles doivent satisfaire les formes binaires primitives négatives de déterminant* $-M$, *qui sont résidus quadratiques de* M, *ou pour lesquelles* 1 *est le nombre caractéristique.*

Désignons par ω l'ensemble de tous les caractères particuliers que donnent les relations du nombre 1 aux différens diviseurs premiers impairs de M, et au nombre 8 ou 4, quand il divise D. Ces caractères seront évidemment Rp, Rp', Rp'', etc., p, p', p'', etc. étant les diviseurs premiers, et 1,4 ou 1,8, suivant que 4 ou 8 divise M. Employons en outre les lettres P et Q dans le même sens qu'au n° précédent ou qu'au n° 263. Nous distinguerons les cas suivans :

1°. Quand M est divisible par 4, ω sera le caractère complet, et il est clair (n° 233, 5°) que 1 ne peut être nombre caractéristique que de formes dont le caractère est ω. Mais il est manifeste que ω est le caractère de la forme principale $(1, 0, M)$, que parconséquent il est de l'espèce P, et qu'ainsi il ne peut appartenir à aucune forme proprement primitive négative, et comme il n'y a pas de forme improprement primitive pour ce déterminant, il n'y a pas de formes primitives négatives qui soient dans ce cas résidus de M.

2°. Quand $M \equiv 3 \pmod 4$, les mêmes raisonnemens ont lieu, avec cette seule différence que dans ce cas l'ordre improprement

primitif négatif existe, dans lequel les caractères de l'espèce P seront possibles ou impossibles, suivant que $M \equiv 3$ ou $\equiv 7$ (mod. 8). (Voyez n° 264, 3°.) Si donc $M \equiv 3$ (mod. 8), il y aura dans cet ordre un genre dont ω sera le caractère, ainsi 1 sera nombre caractéristique de toutes les formes qui y seront contenues. Si $M \equiv 7$ (mod. 8), aucune forme négative ne pourra jouir de cette propriété.

3°. Quand $M \equiv 1$ (mod. 4), ω n'est pas le caractère complet, il faut y ajouter la relation à 4. Mais il est clair que ω doit nécessairement entrer dans le caractère de la forme dont 1 est nombre caractéristique, et que réciproquement toute forme dont le caractère est ω; 1,4 ou ω; 3,4, aura 1 pour nombre caractéristique. Or, ω; 1,4 est le caractère du genre principal, qui appartient à P et est parconséquent impossible dans l'ordre proprement primitif négatif. Par la même raison, le caractère ω; 3,4 appartiendra à Q (n° 263); donc il y aura dans l'ordre proprement primitif négatif un genre qui lui répondra et dont toutes les formes auront 1 pour nombre caractéristique.

Dans ce cas, non plus que dans le suivant, il n'y a pas d'ordre improprement primitif.

4°. Quand $M \equiv 2$ (mod. 4), il faut joindre à ω la relation au nombre 8, pour avoir le caractère complet. Ces relations sont 1 *et* 3,8 ou 5 *et* 7,8, quand $M \equiv 2$ (mod. 8), et 1 *et* 7,8 ou 3 *et* 5,8, quand $M \equiv 6$ (mod. 8). Pour le premier cas, le caractère ω; 1 *et* 3,8 appartient évidemment à P, et partant le caractère ω; 5 *et* 7,8 appartient à Q; donc il répond à ce dernier caractère un genre proprement primitif négatif. Par la même raison, pour le second cas, il y a dans l'ordre proprement primitif négatif un genre dont les formes sont douées des propriétés précitées; le caractère de ce genre est ω; 3 *et* 5,8.

Il résulte de tout cela qu'il n'y a de formes primitives de déterminant $-M$, dont le nombre caractéristique soit 1, que quand M est congru à l'un des nombres 1, 2, 3, 5, 6, suivant le module 8, et cela dans un seul genre qui sera impropre quand $M \equiv 3$, desorte qu'il n'en existe aucune lorsque $M \equiv 0$, 4 ou 7 (mod. 8). Au reste, il est évident que si $(-a, -b, -c)$ est une forme

primitive négative qui ait $+1$ pour nombre caractéristique, (a, b, c) sera une forme primitive positive dont le nombre caractéristique sera -1. On voit par là que dans les cinq premiers cas (quand $M\equiv 1, 2, 3, 5, 6$), il existe un genre primitif positif dont le nombre caractéristique est -1, genre impropre si $M\equiv 3$, et que dans les trois autres (quand $M\equiv 0, 4, 7$) il n'en existe aucune.

289. A l'égard des représentations propres des formes binaires par la forme ternaire $x^2+y^2+z^2=f$, on peut déduire ce qui suit de la théorie générale exposée au n° 282.

1°. La forme binaire φ ne peut être représentée par la forme f, à moins qu'elle ne soit primitive, positive, et que son nombre caractéristique ne soit -1 (déterminant de la forme f). Ainsi aucune forme de déterminant positif, ou même de déterminant négatif $-M$, si $M\equiv 0$ (mod. 4) ou $\equiv 7$ (mod. 8), ne pourra être représentée proprement par f.

2°. Mais si $\varphi=(p, q, r)$ est une forme primitive positive de déterminant $-M$, et que -1 soit son nombre caractéristique, il sera aussi celui de son opposée $(p, -q, r)$, et alors chaque valeur de l'expression $\sqrt{-(p, -q, r)}$ fournira des représentations de φ par f, c'est-à-dire que les coefficiens de la forme ternaire g de déterminant -1 (n° 283) seront nécessairement entiers, que g sera une forme définie et partant équivalente à f (n° 285, I).

3°. Le nombre des représentations qui appartiennent à la même valeur de l'expression $\sqrt{-(p, -q, r)}$ est égal dans tous les cas, excepté dans ceux où $M=1$ ou 2, au nombre de transformations de f en g (n° 283, III), et sera parconséquent (n° 285) égal à 48. Il suit de là que lorsque l'on connaîtra une représentation appartenante à une valeur donnée, on trouvera les 47 autres, tant en permutant les valeurs de x, y, z entre elles de toutes les manières possibles, qu'en les affectant de différens signes. Ainsi les quarante-huit représentations ne donnant qu'une seule décomposition de la forme φ en trois quarrés, si l'on ne considère que les quarrés, et non l'ordre et les signes des racines.

4°.

4°. Soit μ le nombre des diviseurs premiers impairs de M; on déduit sans peine du n° 233, que le nombre de toutes les valeurs différentes de l'expression $\sqrt{-}(p, -q, r)$ (mod. M) est 2^{μ}, dont on ne doit considérer que la moitié (quand $M > 2$): ainsi le nombre de toutes les représentations propres de la forme φ par f sera $48 \cdot 2^{\mu-1} = 3 \cdot 2^{\mu+3}$; mais le nombre des décompositions en trois quarrés n'est que $2^{\mu-1}$

Exemple. Soit $\varphi = 19t^2 + 6tu + 41u^2$, et partant $M = 770$; on a ici à considérer (n° 283) les quatre valeurs suivantes et l'expression $\sqrt{-}(19, -3, 41)$ (mod. 770):

$$(39, 237),\ (171, -27),\ (269, -83),\ (291, -127).$$

Pour trouver les représentations qui appartiennent à la valeur (39, 237), on détermine d'abord la forme ternaire $g = \begin{pmatrix} 19, & 41, & 2 \\ 3, & 6, & 3 \end{pmatrix}$, en laquelle on trouve que f se change, à l'aide des méthodes précédentes (n°s 272 et 275), par la substitution

$$1, -6, -0;\quad -3, -2, -1;\quad -3, -1, -1.$$

D'où résulte pour la représentation de φ par f,

$$x = t - 6u,\quad y = -3t - 2u,\quad z = -3t - u.$$

Pour abréger, nous nous dispensons d'écrire les 47 autres représentations qui naissent de celle-là par permutation et changement de signes. Mais ces 48 représentations ne donnent qu'une seule décomposition en trois quarrés,

$$t^2 - 12tu + 36u^2,\quad 9t^2 + 12tu + 4u^2,\quad 9t^2 + 6u + u^2.$$

Absolument de la même manière on tire:

de la valeur (171, — 27) la décomposition $(3t+5u)^2+(3t-4u)^2+t^2$
de la valeur (269, — 83) la décomposition $(t+6u)^2+(3t+u)^2+(3t-2u)^2$
de la valeur (291, —127) la décomposition $(t+3u)^2+(3t+4u)^2+(3t-4u)^2$.

Chacune de ces décompositions répond à 48 représentations. Mais ces 192 représentations ou ces quatre décompositions sont les seules, parceque, 770 n'étant divisible par aucun quarré, il ne peut y avoir de représentations impropres.

290. Nous ajouterons quelque chose de particulier à l'égard des

formes de déterminant -1 et -2, qui sont sujettes à quelques exceptions. Observons d'abord généralement que si φ, φ' sont deux formes binaires équivalentes quelconques, (Θ) une transformation de la première en la seconde, en combinant avec (Θ) une représentation quelconque de la forme φ par une certaine forme ternaire f, on obtient une représentation de la forme φ' par f; en outre, que de cette manière, les représentations propres de φ conduisent à des représentations propres de φ', les représentations différentes de φ à des représentations différentes de φ', et qu'en opérant de même sur toutes les premières, on obtiendra toutes les dernières. Tout cela se prouve facilement par le calcul. Ainsi l'une des formes φ' peut se représenter par f d'autant de manières que l'autre.

1°. Soit d'abord $\varphi = t^2 + u^2$, et φ' une autre forme binaire de déterminant -1 qui sera parconséquent équivalente à φ; supposons que φ se change en φ' par la substitution $t = \alpha t' + \beta u'$, $u = \gamma t' + \delta u'$. La forme φ se représente par la forme ternaire $f = x^2 + y^2 + z^2$, en posant $x = t$, $y = u$, $z = 0$. En permutant x, y, z, il en résulte six représentations, et de chacune d'elles on en déduit quatre en changeant les signes de t et de u, desorte qu'il y a en tout vingt-quatre représentations différentes qui répondent à une seule décomposition en trois quarrés et qui sont évidemment les seules. On conclut de là que la forme φ' ne peut se décomposer que d'une seule manière en trois quarrés, qui sont:

$$(\alpha t' + \beta u')^2, \quad (\gamma t' + \delta u')^2, \text{ et } 0,$$

cette décomposition équivaut à vingt-quatre représentations.

2°. Soit $\varphi = t^2 + 2u^2$, et φ' une autre forme quelconque de déterminant -2, en laquelle φ se change par la substitution $t = \alpha t' + \beta u'$, $u = \gamma t' + \delta u'$; on conclura, comme dans le cas précédent, que φ et parconséquent φ' ne peut être décomposé que d'une seule manière en trois quarrés, savoir, φ en $t^2 + u^2 + u^2$, et φ' en

$$(\alpha t' + \beta u')^2 + (\gamma t' + \delta u')^2 + (\gamma t' + \delta u')^2;$$

on voit facilement que cette décomposition revient à vingt-quatre représentations.

Il suit de là que les formes binaires de déterminant -1 et

-2 s'accordent parfaitement avec les autres, quant au nombre des représentations par la forme ternaire $x^2+y^2+z^2$; en effet, comme dans les deux cas on a $\mu=0$, la formule donnée au numéro précédent, 4°, conduit à vingt-quatre représentations. Cela vient de ce que les deux exceptions auxquelles elles sont sujettes se compensent mutuellement.

Nous omettons, pour abréger, d'appliquer à la forme $x^2+y^2+z^2$ la théorie générale des représentations impropres exposée au n° 284.

291. La recherche des représentations d'un nombre donné positif M, par la forme $x^2+y^2+z^2$, est d'abord ramenée, par le n° 281, à la recherche des représentations du nombre $-M$ par la forme $-x^2-y^2-z^2=f$. Or on trouve ces dernières par les procédés du n° 280, ainsi qu'il suit :

1°. On cherchera toutes les classes de formes binaires de déterminant $-M$, dont les formes peuvent être représentées proprement par la forme $X^2+Y^2+Z^2=F$, qui a f pour adjointe. Quand $M\equiv 0$, 4 ou 7 (n° 288) il n'existe point de telles classes, et parconséquent le nombre M ne peut pas être décomposé en trois quarrés qui n'aient pas de diviseur commun (*). Mais quand $M\equiv 1$, 2, 5 ou 6, il y aura un genre positif proprement primitif, et quand $M\equiv 3$, un genre improprement primitif, qui renfermera toutes ces classes dont nous représenterons le nombre par k.

2°. De chacune de ces classes on tirera à volonté une forme ; soient ces formes φ, φ', φ'', etc. On cherchera les représentations propres de chacune d'elles par F, le nombre en sera $3.2^{\mu+3}k=K$, μ étant le nombre des facteurs premiers impairs de M. Chaque représentation de cette espèce, telle que

$$X=mt+nu,\quad Y=m't+n'u,\quad Z=m''t+n''u,$$

(*) Cette impossibilité se manifeste d'elle-même ; en effet, la somme de trois quarrés impairs est évidemment $\equiv 3$ (mod. 8) ; la somme de deux impairs et d'un pair est $\equiv 2$ ou $\equiv 6$; la somme d'un pair et de deux impairs est $\equiv 1$ ou $\equiv 5$; enfin la somme de trois pairs est $\equiv 0$ ou $\equiv 4$; mais dans le dernier cas, la représentation est évidemment impropre.

donnera une représentation de M par $x^2+y^2+z^2$, qui sera

$$x=m'n''-m''n',\quad y=m''n-mn'',\quad z=mn'-m'n,$$

et l'ensemble de ces représentations, que nous désignerons par Ω, renfermera nécessairement toutes les représentations de M.

3°. Ainsi il ne reste plus qu'à examiner si dans Ω il peut se trouver des représentations identiques, et comme (n° 280, 3°) les représentations qui sont dérivées de formes différentes sont nécessairement différentes, tout se réduit à chercher si, parmi celles qui se déduisent de la même forme, de φ, par exemple, il peut y en avoir d'identiques. Or il est évident, au premier coup-d'œil, que si, parmi les représentations de φ, on trouve la suivante :

$$X=mt+nu,\quad Y=m't+n'u,\quad Z=m''t+n''u.....(r),$$

on y trouvera aussi

$$X=-mt-nu,\quad Y=-m't-n'u,\quad Z=-m''t-n''u.....(r'),$$

et que de chacune on déduit la même représentation de M, que nous désignerons par (R); examinons donc si la représentation (R) peut encore résulter d'autres représentations de la forme φ. On voit par le n° 280, 3°, en y faisant $\chi=\varphi$, et supposant que toutes les transformations propres de φ en elle-même soient données par les formules $t=\alpha t+\beta u$, $u=\gamma t+\delta u$, que toutes les représentations de la forme φ, dont (R) peut résulter, seront exprimées par

$$x=(\alpha m+\gamma n)t+(\beta m+\delta n)u,\quad y=(\alpha m'+\gamma n')t+(\beta m'+\delta n')u;$$
$$z=(\alpha m''+\gamma n'')t+(\beta m''+\delta n'')u;$$

mais il résulte de la théorie exposée n° 179, sur les transformations des formes binaires de déterminant négatif, qu'excepté les cas où l'on a $M=1$ ou $M=3$, il n'y a jamais que deux transformations propres de la forme φ en elle-même : 1, 0, 0, 1 et -1, 0, 0, -1. On doit remarquer en effet que la forme φ étant primitive, le nombre désigné par m au n° 179 est ici 1 ou 2, et qu'ainsi le premier cas a nécessairement lieu, excepté pour les valeurs 1 et 2 du déterminant. Donc (R) ne peut provenir que des seules représentations r et r', et parconséquent toute représentation propre du nombre M est contenue deux fois dans Ω,

mais ne peut l'être davantage. Le nombre des représentations propres différentes de M est donc $\frac{1}{2}K = 3.2^{\mu+2}k$.

Pour ce qui regarde les cas exceptés, le nombre des transformations de φ en elle-même sera (n° 179) 4 pour $M = 1$, et 6 pour $M = 3$: et en effet, on voit facilement que le nombre des représentations de 1 et 3 sont $\frac{1}{4}K$ et $\frac{1}{6}K$ respectivement, puisque chacun de ces nombres ne peut se décomposer que d'une manière en trois quarrés, savoir, 1 en $1+0+0$, et 3 en $1+1+1$. La décomposition de 1 donne six représentations, celle de 3 en donne huit. Or, pour $M = 1$, on a $K = 24$ (puisque $\mu = 0$ et $k = 1$); pour $M = 3$, on a $K = 48$ (puisque $\mu = 1$ et $k = 1$).

Au reste, observons que si h désigne le nombre de classes du genre principal, qui (n° 252) est égal au nombre de classes de tout autre genre proprement primitif, on aura $k = h$ pour $M \equiv 1, 2, 3, 5, 6 \pmod 1$; mais $k = \frac{1}{3}h$ pour $M \equiv 3$, excepté le seul cas où $M = 3$, dans lequel $k = h = 1$. Ainsi, pour les nombres de la forme $8n+3$, le nombre des représentations est en général $2^{\mu+2}h$, puisque dans le cas où $M = 3$, les deux exceptions le comprennent.

292. Nous avons distingué les décompositions en trois quarrés, tant pour les nombres que pour les formes binaires, des représentations par la forme $x^2+y^2+z^2$, en ne considérant dans les premières que la grandeur des quarrés, et dans les dernières, en outre de la grandeur des racines, leur ordre et les signes qui les affectent; de manière que nous regardons comme différentes les deux représentations $x = a, y = b, z = c$, et $x = a', y = b', z = c'$ tant que l'on n'a pas $a = a', b = b', c = c'$; tandis que les décompositions $a^2+b^2+c^2$, $a'^2+b'^2+c'^2$ n'en font qu'une seule, si les premiers quarrés sont égaux aux derniers, sans faire attention à leur ordre. Il suit de là,

1°. Que la décomposition du nombre M en trois quarrés $a^2+b^2+c^2$ équivaut à quarante-huit représentations, si aucun n'est nul, et qu'ils soient tous inégaux; à vingt-quatre, si l'un des quarrés est nul et que les autres soient inégaux, ou qu'aucun ne soit nul et que deux soient égaux. Mais si deux quarrés sont nuls, ou que l'un d'eux soit nul, tandis que les deux autres sont égaux, ou enfin qu'ils soient tous trois égaux, la décomposition

équivaudra à six, à douze ou à huit représentations. Or cela ne peut arriver que dans les cas particuliers où $M=1$, ou 2, ou 3 respectivement, tant que les représentations doivent être propres. Excluons ces trois cas; désignons par E le nombre total des décompositions du nombre M en trois quarrés qui n'aient de commun diviseur, et supposons que parmi ces décompositions il y en ait e dans lesquelles un des quarrés soit nul, et e' dans lesquelles deux des quarrés soient égaux: on peut regarder les premières comme des décompositions en deux quarrés, et les dernières comme des décompositions en un quarré et le double d'un quarré. Alors le nombre total des représentations du nombre M par $x^2+y^2+z^2$ sera

$$24(e+e')+48(E+e-e')=48E-24(e+e').$$

Mais de la théorie des formes binaires on déduit facilement que e sera ou $=0$, ou $=2^{\mu-1}$, suivant que -1 est non-résidu, ou résidu quadratique de M, et que e' sera $=0$, ou $=2^{\mu-1}$, suivant que -2 est non-résidu ou résidu de M, μ étant le nombre des facteurs premiers impairs de M (n° 182); nous supprimons le développement de cette conséquence: il suit de là que l'on a

$E=2^{\mu-2}.k$ si -1, et -2 sont non-résidus de M;

$E=2^{\mu-2}(k+1)$, si l'un des deux est résidu, et l'autre non-résidu;

$E=2^{\mu-2}(k+2)$, si -1 et -2 sont résidus de M.

Ces formules ne sont pas applicables aux cas où $M=1$ ou 2, car elles donnent $E=\frac{3}{4}$, tandis que l'on doit avoir $E=1$; mais pour $M=3$ on trouve $E=1$, parceque les exceptions se compensent.

Toutes les fois que M est un nombre premier, on a $\mu=1$, et partant,

$E=\frac{1}{2}(k+2)$, si $M\equiv 1$ (mod. 8).
$E=\frac{1}{2}(k+1)$, si $M\equiv 3$ ou $\equiv 5$ (mod. 8). (nos 108 et 116).

Legendre a découvert par induction ces théorèmes particuliers, et les a consignés dans le Mémoire que nous avons déjà cité souvent avec éloge. (*Hist. de l'Acad. de Paris*, 1785, *p.* 530 et *suivantes*). S'ils sont présentés sous une forme un peu différente, c'est que ce savant géomètre n'a pas distingué l'équivalence propre

de l'équivalence impropre, et a parconséquent mêlé avec les autres les formes opposées.

2°. Pour trouver toutes les décompositions d'un nombre donné M en trois quarrés premiers entre eux, il n'est pas nécessaire de chercher toutes les représentations propres des formes φ, φ', φ'', etc. En effet, on voit d'abord facilement que les quarante-huit représentations de la forme $\varphi = (p, q, r)$ qui appartiennent à la même valeur de l'expression $\sqrt{-(p, -q, r)}$, donnent la même décomposition du nombre M, et que parconséquent il suffit d'avoir une de ces représentations, ou, ce qui revient au même, de connaître les différentes décompositions (*) de la forme φ en trois quarrés. Il en est de même des formes φ', φ'', etc. En outre, si φ appartient à une classe non-ambiguë, on pourra ne pas s'occuper de la forme qui serait tirée de la classe opposée, c'est-à-dire que de deux classes opposées, il suffit d'en considérer une. Comme il est en effet indifférent de prendre telle ou telle forme dans chaque classe, supposons que dans la classe opposée à celle où est φ, on ait choisi la forme opposée à φ, que nous désignerons par φ'. On voit alors au premier abord, que si les décompositions propres de la forme φ sont représentées indéfiniment par

$$(gt+hu)^2+(g't+h'u)^2+(g''t+h''u)^2,$$

les décompositions de la forme φ' le seront par

$$(gt-hu)^2+(g't-h'u)^2+(g''t-h''u)^2,$$

qui donnent les mêmes décompositions du nombre M que les premières. Enfin, dans le cas où la forme φ est d'une classe ambiguë, sans être de la classe principale, ni équivalente à la forme $(2, 0, \frac{1}{2}M)$ ou à la forme $(2, 1, \frac{1}{2}(M+1))$ (suivant que M est pair ou impair), on pourra omettre la moitié des valeurs de l'expression $\sqrt{-(p, -q, r)}$; mais pour abréger nous ne donnerons pas plus de détails sur cette simplification. — Au reste, on peut employer ces simplifications, même quand on veut avoir les représentations propres de M par $x^2+y^2+z^2$, puisque l'on déduit facilement celles-ci dès qu'on a les décompositions.

(*) On doit toujours sous-entendre décompositions *propres*, en transportant cette expression des représentations aux décompositions.

Cherchons, par exemple, toutes les manières de décomposer en trois quarrés le nombre 770, par lequel $\mu=3$, $e=e'=0$, et partant $E=2k$; par la classification des formes binaires positives de déterminant -770, classification que chacun peut faire à l'aide de ce qui a été dit n° 231, et que nous pouvons nous dispenser d'inscrire ici, on trouve qu'il y a trente-deux classes qui sont toutes proprement primitives et peuvent se distribuer en huit genres, desorte qu'on a $k=4$ et $E=8$. Le genre dont le nombre caractéristique est -1 doit avoir, à l'égard des nombres 5, 7, 11, les caractères particuliers $R5$; $N7$; $N11$: d'où (n° 263) l'on conclut facilement que le caractère de ce genre, à l'égard du nombre 8, doit être 1 *et* 3,8. Or le genre dont le caractère est 1 *et* 3,8; $R.5$; $N.7$; $N.11$, comprend quatre classes, pour représentantes desquelles nous prendrons les formes

$$(6, 2, 129),\ (6, -2, 129),\ (19, 3, 41),\ (19, -3, 41);$$

mais nous rejetons la seconde et la quatrième classes, comme opposées à la première et à la troisième. Or nous avons déjà donné (n° 289) les quatre décompositions de la forme (19, 3, 41), il en résulte pour les décompositions du nombre 770 en trois quarrés

$$9+361+400,\ 16+25+729,\ 81+400+289,\ 576+169+25;$$

on trouve de la même manière, pour la forme $6t^2+4tu+129u^2$, les quatre décompositions

$$(t-8u)^2+(2t+u)^2+(t+8u)^2,\ (t-10u)^2+(2t+5u)^2+(t+2u)^2,$$
$$(2t-5u)^2+(t+10u)^2+(t+2u)^2,\ (2t+7u)^2+(t-8u)^2+(t-4u)^2,$$

qui résultent des valeurs respectives

$$(48, 369),\ (62, -149),\ (92, -159),\ (202, 61)$$

de l'expression $\sqrt{-(6, -2, 129)}$, et donnent les décompositions du nombre 770 en

$$225+256+289,\ 1+144+625,\ 64+81+625,\ 16+225+529.$$

Ces huit décompositions sont les seules que l'on puisse avoir.

Quant à ce qui regarde celles dans lesquelles les quarrés ont des diviseurs communs, l'application de la théorie générale du n° 281 est trop facile pour qu'il soit nécessaire que nous nous y arrêtions.

293.

293. Les recherches précédentes servent aussi à démontrer que *tout nombre entier positif est toujours décomposable en trois nombres triangulaires;* théorème célèbre trouvé par *Fermat*, mais dont la démonstration manquait jusqu'à présent (*). Il est évident que toute décomposition du nombre M en trois nombres triangulaires

$$\tfrac{1}{2}x(x+1)+\tfrac{1}{2}y(y+1)+\tfrac{1}{2}z(z+1),$$

conduit à une décomposition du nombre $8M+3$ en trois quarrés impairs

$$(2x+1)^2+(2y+1)^2+(2z+1)^2,$$

et réciproquement. Mais par la théorie précédente, tout nombre entier positif $8M+3$ est décomposable en trois quarrés, qui seront nécessairement impairs (n° 291, *note*), et le nombre des décompositions dépend, tant de celui des facteurs premiers de $8M+3$, que de celui des classes suivant lesquelles peuvent être distribuées les formes binaires dont le déterminant est $-(8M+3)$. Nous supposons que le nombre $\frac{1}{2}x(x+1)$ soit regardé comme triangulaire, quelque valeur entière que l'on donne à x; si l'on voulait exclure zéro des nombres triangulaires, il faudrait énoncer le théorème de la manière suivante: *Tout nombre entier positif est triangulaire, ou décomposable en deux ou en trois nombres triangulaires.* Il faut faire le même changement dans le théorème suivant, si l'on veut exclure zéro du nombre des quarrés.

On démontre par les mêmes principes cet autre théorème de *Fermat: Tout nombre entier positif est décomposable en quatre quarrés.* En effet, si l'on retranche d'un nombre de la forme $4n+1$, un quarré pair; d'un nombre de la forme $4n+2$, un quarré arbitraire; d'un nombre de la forme $4n+3$, un quarré impair; les restes seront décomposables en trois quarrés. Quant aux nombres de la forme $4n$, on peut les représenter par $4^{\mu}N$, N étant nécessairement de l'une des trois formes ci-dessus; or quand on aura décomposé le nombre N, en quatre quarrés, le nombre $4^{\mu}N$ le sera aussi. D'un nombre de la forme $8n+3$, on pourrait encore re-

(*) Voyez les Additions de l'auteur, à la fin.

trancher le quarré d'un nombre pairement pair ; d'un nombre de la forme $8n+7$, le quarré d'un nombre impairement pair ; d'un nombre de la forme $8n+4$, le quarré d'un nombre impair, et le reste sera décomposable en trois quarrés. Au reste, ce théorème a déjà été démontré par *Lagrange* (*Nouveaux Mémoires de l'Acad. de Berlin*, 1770, *p.* 123). La démonstration de cet illustre géomètre, qui est entièrement différente de la nôtre, a été exposée avec plus de détails par *Euler* (*Acta Ac. Petr. Vol. II, p.* 48).

Les autres théorèmes de *Fermat*, qui font, pour ainsi dire, la continuation des précédens, savoir: que tout nombre entier est décomposable en cinq nombres pentagones, six nombres hexagones, sept heptagones, manquent jusqu'à présent de démonstration et paraissent exiger d'autres principes.

294. THÉORÈME. a, b, c *étant des nombres premiers entre eux, dont aucun n'est* $=0$, *ni divisible par un quarré, l'équation* $ax^2+by^2+cz^2=0\ldots.(\omega)$ *n'admettra pas de solutions entières* (*excepté la solution* $x=y=z=0$, *que nous ne considérons pas*), *à moins que* $-bc$, $-ac$, $-ab$ *ne soient résidus quadratiques de* a, b, c *respectivement, et que ces derniers ne soient affectés de signes différens; mais si ces conditions ont lieu, l'équation* (ω) *sera résoluble en nombres entiers.*

Si (ω) est résoluble en nombres entiers, elle le sera par des valeurs de x, y, z qui n'auront pas de diviseur commun; car toutes les valeurs qui satisferont à l'équation (ω), y satisferont encore après avoir été divisées par leur plus grand commun diviseur. Supposons donc que l'on ait $ap^2+bq^2+cr^2=0$, et que p, q, r soient premiers entre eux, ils le seront aussi deux à deux. En effet, si q et r avaient un commun diviseur μ, ce nombre serait premier avec p; mais μ^2 divise ap^2, donc il diviserait a, contre l'hypothèse : par la même raison, p et r, p et q sont premiers entre eux ; $-ap^2$ peut donc être représenté par la forme binaire by^2+cz^2, en attribuant à y, z des valeurs premières entre elles et qui seront celles de q et de p ; ainsi le déterminant $-bc$ de cette forme est résidu quadratique de ap^2, et parconséquent de a (n° 154). On aura de la même manière $-acRb$, $-abRc$. Quant à la condition qui exige que a, b, c n'aient pas le même signe, elle est si évidente qu'elle n'a pas besoin d'explication.

Pour démontrer la proposition inverse, qui constitue la seconde partie du théorème, nous commencerons par donner le moyen de trouver une forme équivalente à la forme $\begin{pmatrix} a, & b, & c \\ o, & o, & o \end{pmatrix}$, et telle que les deuxième, troisième et quatrième coefficiens soient divisibles par abc, et de là nous déduirons la solution de l'équation (ω).

1°. On cherchera trois nombres entiers A, B, C qui n'aient pas de diviseur commun, et tels que A soit premier avec b et c, B avec a et c, C avec a et b, tandis que $aA^2+bB^2+cC^2$ sera divisible par abc, ce qui se fait de la manière suivante : Soient H, K, L respectivement des valeurs des expressions

$$\sqrt{-bc} \pmod{a}, \quad \sqrt{-ac} \pmod{b}, \quad \sqrt{-ab} \pmod{c},$$

valeurs qui seront nécessairement premières avec a, b, c respectivement. On prendra à volonté les trois nombres entiers h, k, l, pourvu qu'ils soient respectivement premiers avec a, b, c (on peut, par exemple, les prendre tous égaux à 1). Cela posé, on déterminera A, B, C de manière qu'on ait

$$A \equiv kc \pmod{b} \text{ et } \equiv lL \pmod{c}, \quad B \equiv la \pmod{c} \text{ et } hH \pmod{a},$$
$$C \equiv hb \pmod{a} \text{ et } \equiv kK \pmod{b};$$

on aura alors

$$aA^2+bB^2+cC^2 \equiv h^2(bH^2+cb^2) \equiv h^2(bH^2-bH^2) \equiv o \pmod{a},$$

c'est-à-dire que $aA^2+bB^2+cC^2$ est divisible par a; on prouvera de la même manière, qu'il est divisible par b et par c, et par-conséquent par abc. On voit en outre que A est premier avec b et c, B avec a et c, C avec a et b. S'il arrivait que les valeurs de A, B, C eussent un diviseur commun μ, μ serait nécessairement premier avec a, b, c, et partant avec abc; donc en divisant ces valeurs par μ, on en obtiendra de nouvelles qui n'auront pas de diviseur commun, et qui satisferont à la condition de rendre $aA^2+bB^2+cC^2$ divisible par abc, et par-conséquent à toutes les conditions.

2°. A, B, C étant ainsi déterminés, Aa, Bb, Cc n'auront pas non plus de commun diviseur; en effet a étant premier avec Bb et Cc, il s'ensuivrait que le plus grand commun diviseur supposé, que nous désignerons par μ, serait premier avec a; on

prouvera de même que μ est premier avec b et c; donc il devrait diviser A, B, C, contre l'hypothèse. On pourra donc trouver trois nombres α, β, γ, tels que l'on ait $\alpha Aa+\beta Bb+\gamma Cc=1$: on cherchera six nombres α', β', γ'; $\alpha'', \beta'', \gamma''$ tels qu'on ait

$$\beta'\gamma''-\beta''\gamma'=Aa,\ \gamma'\alpha''-\gamma''\alpha'=Bb,\ \alpha'\beta''-\alpha''\beta'=Cc;$$

la forme f se changera, par la substitution

$$\alpha,\ \alpha',\ \alpha''\ ;\quad \beta,\ \beta',\ \beta''\ ;\quad \gamma,\ \gamma',\ \gamma'',$$

en une certaine forme $g=\begin{pmatrix} m, & m', & m'' \\ n, & n', & n'' \end{pmatrix}$ qui lui sera équivalente, et dans laquelle m', m'', n seront divisibles par abc. Posons en effet

$$\beta''\gamma-\beta\gamma''=A',\quad \gamma''\alpha-\gamma\alpha''=B',\quad \alpha''\beta-\alpha\beta''=C',$$
$$\beta\gamma'-\beta'\gamma=A'',\quad \gamma\alpha'-\gamma'\alpha=B'',\quad \alpha\beta'-\alpha'\beta=C'';$$

on aura

$$\alpha'=B''Cc-C''Bb,\quad \beta'=C''Aa-A''Cc,\quad \gamma'=A''Bb-B''Aa,$$
$$\alpha''=C'Bb-B'Cc,\quad \beta''=A'Cc-C'Aa,\quad \gamma''=B'Aa-A'Bb;$$

et en substituant ces valeurs dans les équations

$$m'=a\alpha'^2+b\beta'^2+c\gamma'^2, m''=a\alpha''^2+b\beta''^2+c\gamma''^2, n=a\alpha'\alpha''+b\beta'\beta''+c\gamma'\gamma'',$$

on trouve, suivant le module a,

$$m'\equiv bcA''^2(B^2b+C^2c)\equiv 0,\quad m''\equiv bcA'^2(B^2b+C^2c)\equiv 0,$$
$$n\equiv bcA'A''(B^2b+C^2c)\equiv 0,$$

c'est-à-dire, que m', m'', n sont divisibles par a: on démontre de même qu'ils sont divisibles par b et par c, et ainsi par abc.

3°. Faisons, pour abréger, le déterminant des formes f, g, c'est-à-dire, le nombre $-abc=d$, $md=M$, $m'=M'd$, $m''=M''d$, $n=Nd$, $n'=N'$, $n''=N''$; il est clair que f se change, par la substitution

$$\alpha d,\ \alpha',\ \alpha''\ ;\quad \beta d,\ \beta',\ \beta''\ ;\quad \gamma d,\ \gamma',\ \gamma''\ldots\ldots\ldots(S),$$

en la forme ternaire $g'=\begin{pmatrix} Md, & M'd, & M''d \\ Nd, & N'd, & N''d \end{pmatrix}$ de déterminant d^3, qui est parconséquent contenue dans f. Or je dis que cette forme est nécessairement équivalente à la forme $g''=\begin{pmatrix} d, & 0, & 0 \\ d, & 0, & 0 \end{pmatrix}$. En effet, il est évident que $g'''=\begin{pmatrix} M, & M', & M'' \\ N, & N', & N'' \end{pmatrix}$ est une forme ternaire

de déterminant 1 ; or, comme par hypothèse a, b, c n'ont pas tous les trois le même signe, f est une forme indéfinie, d'où l'on conclut facilement que g' et g'' sont aussi des formes indéfinies ; donc g'' sera équivalente à la forme $\begin{pmatrix} 1, & 0, & 0 \\ 1, & 0, & 0 \end{pmatrix}$ (n° 277), et l'on pourra trouver une transformation (S') de la première en la seconde. Mais d'ailleurs la transformation (S') change g' en g'' ; donc g'' sera contenue dans f, et de la combinaison des substitutions (S), (S'), on déduira une transformation de f en g''. Représentons-la par

$$\delta, \delta', \delta''; \quad \varepsilon, \varepsilon', \varepsilon''; \quad \zeta, \zeta', \zeta'';$$

il est évident qu'il en résultera deux solutions de l'équation (ω) :

$$x=\delta', \ y=\varepsilon', \ z=\zeta' \quad \text{et} \quad x=\delta'', \ y=\varepsilon'', \ z=\zeta'':$$

on voit aussi que les valeurs ne peuvent être toutes égales à zéro en même temps, puisque l'on doit avoir

$$\delta\varepsilon'\zeta''+\delta'\varepsilon''\zeta+\delta''\varepsilon\zeta'-\delta\varepsilon''\zeta'-\delta'\varepsilon\zeta''-\delta''\varepsilon'\zeta=d.$$

Exemple. Soit $7x^2-15y^2+23z^2=0$ l'équation proposée ; elle est résoluble, puisqu'on a $345R7$, $-161R15$, $105R23$. On trouve pour valeurs de H, K, L les nombres 3, 7, 6, et faisant $h=k=l=1$, on en déduit $A=98$, $B=-39$, $C=-8$. De là résulte la substitution

$$3, 5, 22; \quad -1, 2, -28; \quad 8, 25, -7,$$

par laquelle f se change en $\begin{pmatrix} 1520, & 14490, & -7245 \\ -2415, & -1246, & 4735 \end{pmatrix}=g$. On trouve pour la substitution (S)

$$7245, 5, 22; \quad -2415, 2, -28; \quad 19320, 25, -7,$$

et

$$g''=\begin{pmatrix} 3670800, & 6, & -3 \\ -1, & -1246, & 4735 \end{pmatrix};$$

on trouve enfin que g'' se change en $\begin{pmatrix} 1, & 0, & 0 \\ 1, & 0, & 0 \end{pmatrix}$, par la substitution (S')

$$3, 5, 1; \quad -2440, -4066, -813; \quad -433, -722, -144,$$

qui, combinée avec (S), donne la suivante :

$$9, 11, 12; \quad -1, 9, -9; \quad -9, 4, 3,$$

par laquelle f se change en g''. Nous avons donc une double solution de l'équation proposée, savoir : $x=11$, $y=9$, $z=4$; $x=12$, $y=-9$, $z=3$. La dernière devient plus simple, en divisant les valeurs par leur diviseur commun 3, et elle donne $x=4$, $y=-3$, $z=1$.

295. La seconde partie du théorème du n° précédent peut encore être traitée de la manière suivante. Conservons aux lettres H, K, L la même signification que dans le n° précédent; on cherchera un entier h tel qu'on ait $ah\equiv L \pmod{c}$, et l'on fera $ah^2+b=ci$. Il est aisé de voir que i est entier, et que $-ab$ est le déterminant de la forme binaire $\varphi=(ac, ah, i)$. Cette forme ne sera certainement pas positive, puisque a, b, c n'étant pas tous de même signe, ab et ac ne peuvent pas être tous deux positifs. Or -1 sera son nombre caractéristique, ce qui peut se démontrer synthétiquement de la manière suivante : Si l'on détermine les entiers e, e' de manière à avoir

$e\equiv 0 \pmod{a}$ et $\equiv K \pmod{b}$, $ce'\equiv H \pmod{a}$ et $\equiv hK \pmod{b}$,

(e, e') sera une valeur de l'expression $\sqrt{-(ac, ah, i)}$; en effet, suivant le module a, on aura

$$e^2\equiv 0\equiv -ac,\ ee'\equiv 0\equiv -ah,\ c^2e'^2\equiv H^2\equiv -bc\equiv -c^2i \text{ ou } e'^2\equiv -i;$$

et suivant le module b,

$$e^2\equiv K^2\equiv -ac,\ cee'\equiv hK^2\equiv -ach \text{ ou } ee'\equiv -ah,$$
$$c^2e'^2\equiv h^2K^2\equiv -ach^2\equiv -c^2i \text{ ou } e'^2\equiv -i;$$

mais puisque les trois mêmes congruences ont lieu à-la-fois pour les modules a et b, elles ont lieu aussi suivant le module ab.

On conclut facilement de là, par la théorie des formes binaires, que φ est représentable par la forme $\left(\begin{smallmatrix}-1, & 0, & 0\\ 1, & 0, & 0\end{smallmatrix}\right)$. Supposons donc

$$act^2+2ahtu+iu^2=-(\alpha t+\beta u)^2+2(\gamma t+\delta u)(\varepsilon t+\zeta u);$$

on aura, en multipliant par c,

$$a(ct+hu)^2+bu^2=-c(\alpha t+\beta u)^2+2c(\gamma t+\delta u)(\varepsilon t+\zeta u);$$

donc si l'on donne à t et u des valeurs telles que l'on ait $\gamma t+\delta u=0$ ou $\varepsilon t+\zeta u=0$, on aura une solution de l'équa-

tion (ω), à laquelle parconséquent on peut satisfaire de deux manières, en faisant

$$x=\delta c-\gamma h, y=\gamma, z=\alpha\delta-\beta\gamma, \text{ ou } x=\zeta c-\varepsilon h, y=\varepsilon, z=\alpha\zeta-\beta\varepsilon.$$

On voit en même temps que ni les premières ni les secondes valeurs ne peuvent être ensemble $=0$; en effet, si l'on avait $\delta c-\gamma h=0$ et $\gamma=0$, il s'ensuivrait aussi $\delta=0$, et partant $\varphi=-(at+\beta u)^2$, d'où $ab=0$, contre l'hypothèse : on démontrerait de même pour les autres.

Dans l'exemple que nous avons donné, on trouve pour la forme φ celle-ci (161, —63, 24); en outre (7, —51) est une valeur de l'expression $\sqrt{-\varphi}$ (mod. 105), et la représentation de la forme φ par la forme $\begin{pmatrix} -1, & 0, & 0 \\ 1, & 0, & 0 \end{pmatrix}$ est

$$\varphi=-(13t-4u)^2+2(11t-4u)(15t-5u),$$

d'où résultent les solutions $x=7$, $y=11$, $z=-8$; $x=20$, $y=15$, $z=-5$, ou en divisant par 5, et ne faisant pas attention au signe de z, $x=4$, $y=3$, $z=1$.

Des deux méthodes que nous venons de donner pour résoudre l'équation (ω), la seconde est préférable, parceque le plus souvent on n'emploie que de petits nombres; mais la première, qui peut s'abréger par différens artifices que nous passerons sous silence, paraît plus élégante, surtout parceque les nombres a, b, c sont traités de la même manière, et que leur permutation ne change rien au calcul. La même chose n'a pas lieu dans la seconde, où le calcul devient souvent plus commode en prenant pour a le plus petit, pour c le plus grand des trois nombres, comme nous l'avons fait dans notre exemple.

296. Le théorème élégant que nous avons exposé dans les nos précédens, a été trouvé par *Legendre* (*Hist. de l'Acad. de Paris*, 1785, *p.* 507), qui en a donné une belle démonstration, mais entièrement différente des deux nôtres. Cet excellent géomètre a cherché en même temps à tirer de là une démonstration des propositions qui reviennent au *théorème fondamental* de la section précédente, démonstration que nous avons déjà annoncé (n° 151) ne pas nous paraître remplir le but qu'il s'était proposé.

Il est donc à propos d'exposer ici en peu de mots cette démonstration, qui est très-élégante, et d'y joindre les motifs de notre jugement.

Il commence par observer que *si trois nombres* a, b, c *sont* $\equiv 1 \pmod 4$, *l'équation* $ax^2+by^2+cz^2=0 \ldots . (\omega)$ *n'est pas résoluble*. En effet, on voit facilement que la valeur de $ax^2+by^2+cz^2$ deviendrait nécessairement $\equiv 1, 2, 3 \pmod 4$, à moins que l'on ne donnât à x, y, z des valeurs paires : donc si (ω) était résoluble, ce ne pourrait être que par des valeurs paires, ce qui est absurde, puisque toutes les fois que trois nombres satisfont à l'équation (ω), ils y satisferont encore après qu'ils auront été divisés par leur plus grand commun diviseur, et que par cette opération il résulterait au moins un nombre impair. Or les différens cas du théorème à démontrer se rapportent aux suivans :

I. p et q désignant des nombres premiers de la forme $4n+3$ positifs et inégaux, on ne peut pas avoir en même temps pRq et qRp. En effet, si cela était possible, il est évident qu'en posant $1=a$, $-p=b$, $-q=c$, toutes les conditions nécessaires pour la résolution de l'équation $ax^2+by^2+cz^2=0$ seraient remplies (n° 294). Mais d'après l'observation précédente, cette équation n'admet aucune solution, donc la supposition ne peut subsister. De là suit sur-le-champ la proposition 7 du n° 131.

II. Si p est un nombre premier de la forme $4n+1$, et q un nombre premier de la forme $4n+3$, on ne peut avoir en même temps qRp, pNq, autrement on aurait $-pRq$, et l'équation $x^2+py^2-qz^2=0$ serait résoluble, tandis que l'observation précédente prouve qu'elle ne l'est pas. De là suivent les quatrième et cinquième cas du n° 131.

III. Si p et q sont des nombres premiers de la forme $4n+1$, on ne peut avoir en même temps pRq et qNp; en effet, prenons un autre nombre premier de la forme $4n+3$, qui soit résidu de q, et dont p soit non-résidu. Alors, par les cas traités dans l'instant (II), on aura qRr et rNp : si donc on avait pRq et qNp, il en résulterait $qrRp$, pRq, $pqNr$, et partant $-pqRr$. Donc l'équation $px^2+qy^2-rz^2=0$ serait résoluble,

contre

contre l'observation précédente, et partant, la supposition ne peut subsister. De là, suivent le premier et deuxième cas du n° 131.

On peut présenter ce cas d'une manière plus simple. Soit r un nombre premier de la forme $4n+3$, dont p soit non-résidu; on aura rNp, et partant, puisque l'on suppose pRq, qNp, on aura aussi $qrRp$; d'ailleurs on a $-pRq$, $-pRr$ et parconséquent $-pRqr$, donc l'équation $x^2+py^2-qrz^2=0$ serait résoluble, contre l'observation précédente, etc.

IV. Si p est un nombre premier de la forme $4n+1$, et q un nombre premier de la forme $4n+3$, on ne peut pas avoir en même temps pRq et qNp. En effet, prenons un nombre premier r de la forme $4n+1$, qui soit non-résidu des deux nombres p et q: on aura (II) qNr, et (III) pNr; donc $pqRr$. Si l'on avait donc pRq, qNp, il s'ensuivrait aussi $prNq$, $-prRq$, $qrRp$. L'équation $px^2-qy^2+rz^2=0$ serait donc résoluble, ce qui est absurde. On tire de là le troisième et le sixième cas du n° 131.

V. p et q étant deux nombres premiers de la forme $4n+3$, on ne peut pas avoir en même temps pNq, qNp; supposons en effet que la chose ait lieu, et prenons un nombre premier r de la forme $4n+1$ qui soit non-résidu de p et de q; on aura $qrRp$, $prRq$; or (II) on a pNr et qNr; et partant, $pqRr$ et $-pqRr$. L'équation $-px^2-qy^2+rz^2=0$ serait donc possible, contre l'observation précédente. De là se déduit le huitième cas du n° 131.

297. En examinant attentivement cette démonstration, on verra facilement que les deux premiers cas sont démontrés de manière à ne permettre aucune objection : mais les autres s'appuient sur l'existence de nombres auxiliaires, et cette existence n'étant pas prouvée, la méthode perd toute sa force. Quoique ces suppositions soient si spécieuses, qu'au premier abord elles semblent ne pas exiger de démonstration, et qu'elles ramènent bien certainement le théorème à démontrer au plus haut degré de probabilité; cependant, quand on recherche la rigueur géométrique, il est impossible de les admettre gratuitement. Pour ce qui regarde la supposition des quatrième et cinquième cas, qu'il existe un nombre r de la forme $4n+1$ qui soit non-résidu des deux autres nombres

premiers p et q; il est facile de conclure de la section IV, que tous les nombres moindres que $4pq$, et premiers avec lui, qui sont au nombre de $2(p-1)(q-1)$, peuvent être distribués en quatre classes égales, dont l'une contient les non-résidus de p et de q, et les trois autres les nombres qui sont résidus de p ou de q seulement, ou de tous les deux : d'ailleurs, dans chaque classe, moitié des nombres seront de la forme $4n+1$, et l'autre de la forme $4n+3$. Parmi ces nombres, il y en aura donc $\frac{1}{4}(p-1)(q-1)$ qui seront non-résidus de p et de q, et de la forme $4n+1$. Représentons-les par g, g', g'', etc., et tous les autres qui sont au nombre de $\frac{3}{4}(p-1)(q-1)$ par h, h', h'', etc. Il est évident que tous les nombres de la forme

$$4pqt+g,\ 4pqt+g',\ 4pqt+g'',\ \text{etc}.....(G)$$

seront à-la-fois non-résidus de p et de q, et de la forme $4n+1$. Or, pour établir la démonstration, il ne reste plus qu'à faire voir qu'il y a nécessairement des nombres premiers compris sous les formes (G); cette assertion paraît d'autant plus plausible, que ces formes jointes aux formes

$$4pqt+h,\ \ 4pqt+h',\ \ 4pqt+h''+\text{etc}.....(H),$$

renferment tous les nombres premiers à p et q, et parconséquent tous les nombres absolument premiers (excepté 2, p et q), et qu'il n'y a pas de raison pour que la suite des nombres premiers ne soit pas distribuée également entre ces formes, de manière que la huitième partie appartienne à (G), et les autres à (H). Cependant on voit sans peine combien un tel raisonnement est éloigné de la rigueur géométrique. *Legendre* avoue lui-même qu'il lui semble assez difficile de démontrer qu'il y a nécessairement des nombres premiers compris sous la forme $kt+l$, k et l étant deux nombres premiers entre eux, et t un nombre indéterminé, et il indique une autre méthode qui conduirait peut-être au but proposé. Mais il nous semblerait nécessaire de faire beaucoup de recherches préliminaires, avant de parvenir par cette dernière voie à une démonstration rigoureuse. — Il suppose encore (III, seconde méthode) qu'il existe un nombre premier r, de la forme $4n+3$, dont un nombre premier donné p, de la forme $4n+1$, soit non-résidu; mais il n'a rien ajouté pour

confirmer sa supposition. Nous avons démontré (n° 129) qu'il existe nécessairement des nombres premiers dont p soit non-résidu; mais notre méthode ne paraît pas pouvoir démontrer l'existence de tels nombres, qui soient en même temps de la forme $4n+3$ (ce qui est exigé ici, et non dans notre première démonstration). Au reste, nous pouvons facilement démontrer, comme il suit, la légitimité de cette supposition. Par le n° 287, il y aura un genre positif de formes binaires de déterminant $-p$ dont le caractère sera 3,4; Np: soit (a, b, c) une telle forme, et a impair (ce que l'on peut supposer). Alors a sera de la forme $4n+3$, et il sera premier ou divisible par un facteur premier de r de la forme $4n+3$. D'ailleurs on aura $-pRa$, et partant, $-pRr$, d'où pNr. Mais il faut remarquer que les propositions des n°s 263, 287 s'appuient sur le théorème fondamental, et que parconséquent c'est faire un cercle vicieux que d'établir sur elles une partie de la démonstration de ce théorème. — La supposition de la première méthode du troisième cas est encore beaucoup plus gratuite, ensorte qu'il est inutile de nous y arrêter.

Qu'il nous soit permis d'ajouter une observation à l'égard du cinquième cas, qui n'est pas assez prouvé par la méthode précédente, mais qui n'échappe pas à la suivante. Si l'on avait à-la-fois pNq, qNp, on aurait $-pRq$, $-qRp$; d'où l'on conclut facilement que -1 est nombre caractéristique de la forme $(p, 0, q)$, qui parconséquent, d'après la théorie des formes ternaires peut être représentée par la forme $x^2+y^2+z^2$. Soit

$$pt^2+qu^2=(\alpha t+\beta u)^2+(\alpha' t+\beta' u)^2+(\alpha'' t+\beta'' u)^2,$$

ou

$$\alpha^2+\alpha'^2+\alpha''^2=p,\ \beta^2+\beta'^2+\beta''^2=q,\ \alpha\beta+\alpha'\beta'+\alpha''\beta''=0;$$

par les deux premières équations, α, α', α'', β, β', β'' doivent être tous impairs; mais alors la troisième ne peut subsister.

Le deuxième cas peut se traiter d'une manière semblable.

298. Problème. a, b, c *étant des nombres quelconques dont cependant aucun n'est* $=0$, *trouver les conditions nécessaires pour que l'équation* $ax^2+by^2+cz^2=0\ldots.(\omega')$ *soit résoluble.*

Soient α^2, β^2, γ^2 les plus grands quarrés qui puissent diviser

bc, ac, ab respectivement, et soit fait

$$\alpha a = \beta\gamma A, \quad \beta b = \alpha\gamma B, \quad \gamma c = \alpha\beta C.$$

A, B, C seront entiers et premiers entre eux; l'équation (ω') sera résoluble ou non, suivant que l'équation $AX^2+BY^2+CZ^2=0$ le sera ou ne le sera pas, ce qui pourra se déterminer par le n° 294.

1°. Soit fait $bc=H\alpha^2$, $ac=K\beta^2$, $ab=L\gamma^2$, H, K, L sont des entiers délivrés de facteurs quarrés, et l'on a $H=BC$, $K=AC$, $L=AB$; donc $HKL=(ABC)^2$, et partant $ABC=AH=BK=CL$ est nécessairement un nombre entier. Soit m le plus grand commun diviseur des nombres H et AH, et $H=gm$, $AH=hm$; g sera premier avec h et avec m, puisque H est libre de tout facteur quarré. Or on a $h^2m=gA^2H=gKL$, donc g divisera h^2m, ce qui est impossible à moins que l'on n'ait $g=\pm 1$, et partant $H=\pm m$, $A=\pm h$; donc A est entier : on démontrera de même que B et C le sont.

2°. Puisque $H=BC$ ne renferme pas de facteurs quarrés, B et C sont nécessairement premiers entre eux. De même A et B, B et C sont premiers entre eux.

3°. Enfin il est évident que si l'on satisfait à l'équation (ω) en faisant $X=P$, $Y=Q$, $Z=R$, on satisfera à l'équation (ω') en faisant $x=\alpha P$, $y=\beta Q$, $z=\gamma R$, et réciproquement si l'on satisfait à l'équation (ω') en faisant $x=p$, $y=q$, $z=r$, on satisfera à l'équation (ω) en faisant $X=\beta\gamma p$, $Y=\alpha\gamma q$, $Z=\alpha\beta r$. Ainsi toutes deux sont résolubles, ou aucune ne l'est.

299. Problème. *Étant proposée la forme ternaire*

$$ax^2+a'x'^2+a''x''^2+2bx'x''+2b'xx''+2b''xx'=f,$$

trouver si zéro peut être représenté par elle, en donnant aux indéterminées des valeurs qui ne soient pas toutes égales à zéro.

I. Quand $a=0$, on peut prendre à volonté les valeurs de x', x'', et il est clair que l'équation

$$a'x'^2+2bx'x''+a''x''^2=-2x(b'x''+b''x'),$$

donne toujours pour x une valeur déterminée et rationnelle. Toutes

les fois qu'il en résulte une fraction, il suffit de multiplier les valeurs de x, x', x'' par le dénominateur de la fraction, et l'on obtient une solution entière. On doit seulement exclure les valeurs de x', x'' qui rendraient $b'x''+b''x'=0$, à moins qu'elles ne rendissent aussi $a'x'^2+2bx'x''+a''x''^2=0$, auquel cas x peut être pris arbitrairement. On voit en même temps que de cette manière on obtient toutes les solutions possibles. Au reste, le cas où $b'=b''=0$ sort de nos considérations; car x n'entre plus dans la forme, c'est-à-dire que f est une forme binaire, et que l'on peut juger par la théorie des formes binaires si zéro est représentable par elle.

II. Mais quand a n'est pas $=0$, l'équation $f=0$ revient à

$$(ax+b''x'+b'x'')^2-A''x'^2+2Bx'x''-A'x''^2=0,$$

en posant $b''^2-aa'=A''$, $ab=b'b''=B$, $b'^2-aa''=A'$.

Or quand $A''=0$, et que l'on n'a pas $B=0$, il est évident que si $ax+b''x'+b'x''$ et x'' sont pris arbitrairement, x et x' obtiennent des valeurs rationnelles, et si elles ne sont pas entières, un multiplicateur convenable donnera des entiers. Il n'y a que lorsque l'on prend $x''=0$, que $ax+b''x'+b'x''$ n'est plus arbitraire; il doit être aussi $=0$. La valeur de x' peut être prise arbitrairement et produira des valeurs rationnelles pour x. Quand on a à-la-fois $A''=0$, $B=0$, il est clair que dans le cas où A' est un quarré k^2, l'équation $f=0$ est décomposable en deux équations linéaires (dont l'une ou l'autre doit avoir lieu),

$$ax+b''x'+(b'+k)x''=0, \quad ax+b''x'+(b'-k)x''=0;$$

mais si, dans la même hypothèse, A' n'est pas un quarré, il est évident que la solution de l'équation proposée dépend des équations $x''=0$, $ax+b''x'=0$, qui doivent avoir lieu en même temps.

Au reste, il est à peine nécessaire d'observer que la méthode du paragraphe I s'appliquerait de même quand $a'=0$, ou $a''=0$, et celle du paragraphe II, quand $A'=0$.

III. Mais quand on n'a ni $a=0$, ni $A''=0$, l'équation $f=0$ peut se mettre sous la forme

$$A''(ax+b''x'+b'x'')^2-(A''x'-Bx'')^2+Dax''^2=0,$$

en désignant par D le déterminant de la forme f, ou par Da le nombre $B^2 - A'A''$.

Quand $D = 0$, la solution est semblable à celle de la fin du cas précédent, savoir, si A'' est un quarré $= k^2$, l'équation proposée se réduit aux deux

$$kax + (kb'' - A'')x' + (kb' + B)x'' = 0,$$
$$kax + (kb'' + A'')x' + (kb' - B)x'' = 0;$$

mais si A'' n'est pas un quarré, on doit avoir

$$ax + b''x' + b'x'' = 0, \quad A''x' - Bx'' = 0.$$

Quand D n'est pas $= 0$, on est ramené à l'équation..... $A''t^2 - u^2 + aDv^2 = 0$, dont la possibilité se reconnaît par le n° précédent. Si cette dernière ne peut être résolue que par les valeurs $t = 0$, $u = 0$, $v = 0$, la proposée n'admettra pas d'autre solution que $x = 0$, $x' = 0$, $x'' = 0$; mais si elle est susceptible d'autres solutions, on déduira d'une quelconque d'entre elles, au moyen des équations

$$ax + b''x' + b'x'' = t, \quad A''x' - Bx'' = u, \quad x'' = v,$$

des valeurs au moins rationnelles de x, x', x''. Si ces valeurs renferment des fractions, on pourra toujours en tirer des entiers à l'aide d'un multiplicateur convenable.

Cela posé, quand on a une solution en nombres entiers de l'équation $f = 0$, on peut réduire le problème au premier cas, et obtenir, comme on l'a fait, toutes les solutions. Soient α, α', α'' les valeurs supposées de x, x', x'' respectivement, délivrées de facteurs communs; on prendra (n°s 40, 279) les nombres entiers β, β', β'', γ, γ', γ'' tels qu'on ait

$$\alpha(\beta'\gamma'' - \beta''\gamma') + \alpha'(\beta''\gamma - \beta\gamma'') + \alpha''(\beta\gamma' - \beta'\gamma) = 1;$$

la forme f se changera, par la substitution

$$x = \alpha y + \beta y' + \gamma y'', \quad x' = \alpha' y + \beta' y' + \gamma' y'', \quad x'' = \alpha'' y + \beta'' y' + \gamma'' y'' \ldots (S),$$

en la forme

$$g = cy^2 + c'y'^2 + c''y''^2 + 2dy'y'' + 2d'yy'' + 2d''yy'.$$

On aura évidemment $c = 0$, et g équivalente à f; d'où il suit que des solutions de l'équation $g = 0$ on déduira, à l'aide de la

substitution (S), toutes les solutions de l'équation $f=0$ en nombres entiers. Or nous avons vu (I) que toutes les solutions de l'équation $g=0$ sont contenues sous les formules

$$y=-z(c'p^2+2dpq+c''q^2),\ y'=2z(d''p^2+d'pq),\ y''=2z(d''pq+d'q^2),$$

p et q étant des nombres entiers indéterminés, et z un nombre indéterminé qui peut être fractionnaire, pourvu que y, y', y'' restent entiers. En substituant ces valeurs dans (S), on aura toutes les solutions de l'équation $f=0$ en nombres entiers.

Ainsi, par exemple, si $f=x^2+x'^2+x''^2+4x'x''+2xx''+8xx'$, et que l'on ait la solution $x=1$, $x'=-2$, $x''=1$, en faisant β, β', β'', γ, γ', $\gamma''=0$, 1, 0, 0, 0, 1, il en résulte... $g=y'^2+y''^2-4y'y''+12yy''$. Toutes les solutions de l'équation $g=0$ en nombres entiers seront renfermées dans les formules

$$y=-z(p^2-4pq+q^2),\quad y'=12zpq,\quad y''=12zq^2,$$

et partant toutes celles de l'équation $f=0$, dans les suivantes :

$$x=-z(p^2-4pq+q^2),x'=2z(p^2+2pq+q^2),x''=-z(p^2-4pq+11q^2).$$

300. Le problème du n° précédent conduit naturellement à la solution de l'équation

$$ax^2+2bxy+cy^2+2dx+2ey+f=0,$$

lorsque l'on ne demande que des nombres rationnels (Nous l'avons résolue plus haut (nos 216 et suiv.) dans le cas où l'on demande des entiers); car toutes les valeurs rationnelles de x et y pourront être représentées par $\frac{t}{v}$, $\frac{u}{v}$, de manière que t, u et v soient des entiers; d'où il suit que la résolution de cette équation en nombres rationnels, revient à celle de l'équation

$$at^2+2btu+cu^2+2dtv+2euv+fv^2=0$$

en nombres entiers; mais cette dernière coïncide avec l'équation traitée au n° précédent. On doit seulement exclure les solutions dans lesquelles $v=0$; mais il ne peut y en avoir de telles quand b^2-ac n'est pas un quarré.

Ainsi, par exemple, toutes les solutions en nombres rationnels de l'équation

$$x^2+8xy+y^2+2x-4y+1=0,$$

que nous avons déjà résolue en nombres entiers (n° 221), se trouvent comprises dans les formules

$$x = \frac{p^2 - 4pq + q^2}{p^2 - 4pq + 11q^2}, \quad y = -\frac{2p^2 + 4pq + 2q^2}{p^2 - 4pq + 11q^2},$$

p et q étant des nombres entiers quelconques.

Au reste, nous n'avons parlé qu'en peu de mots de ces deux problèmes qui sont étroitement liés entre eux, et nous avons supprimé beaucoup d'observations qui y sont relatives, tant pour éviter la prolixité, que parceque nous avons une autre solution du problème du n° précédent, appuyée sur des principes plus généraux, et dont nous devons réserver l'exposition pour une autre occasion, attendu qu'elle exige l'examen le plus approfondi des formes ternaires.

301. Revenons aux formes binaires dont nous avons encore à examiner plusieurs propriétés remarquables; et d'abord, ajoutons quelque chose sur le nombre de genres et de classes de l'ordre proprement primitif (positif quand le déterminant est négatif), auquel nous sommes forcés, pour abréger, de borner nos recherches.

Le *nombre de genres* en lesquels se distribuent toutes les formes proprement primitives positives de déterminant positif ou négatif $\pm D$, est toujours une puissance de 2, dont l'exposant dépend du nombre de facteurs de D, et que l'on peut entièrement déterminer par les recherches précédentes. Or comme dans la suite des nombres naturels, les nombres premiers sont mêlés avec d'autres plus ou moins composés, il arrive que pour plusieurs déterminans successifs $\pm D$, $\pm(D+1)$, $\pm(D+2)$, le nombre des genres tantôt augmente et tantôt diminue, et il semble qu'il n'y ait aucun ordre dans cette suite de nombres. Néanmoins, si l'on ajoute les nombres de genres correspondans à plusieurs déterminans successifs $\pm D$, $\pm(D+1)$, $\pm$... etc. $(D+m)$, et que l'on divise la somme par le nombre des déterminans, il en résulte un *nombre moyen de genres* qui pourra être censé appartenir au déterminant moyen $\pm\left(D+\frac{m}{2}\right)$, et établit une progression très-régulière. Nous supposons, non-seulement que m est un nombre assez grand, mais encore que D est beaucoup plus grand, de manière que le rapport

des

des déterminans extrêmes D et $D+m$, ne diffère pas trop de l'égalité. La régularité de cette progression doit s'entendre ainsi : si D' est un nombre beaucoup plus grand que D, le nombre moyen de genres pour le déterminant $\pm D'$ sera sensiblement plus grand que pour D; mais si D et D' ne diffèrent pas beaucoup, les nombres moyens de genres sont presqu'égaux. Au reste, le nombre moyen de genres pour le déterminant positif $+D$, se trouve presque toujours égal au nombre moyen de genres pour le déterminant négatif, et cela d'autant plus exactement, que D est plus grand; tandis que pour de petits nombres, le premier se trouve un peu plus grand que le second. Ces observations s'éclairciront davantage par les exemples suivans, tirés d'une table de classification de formes binaires, qui contient plus de 4000 déterminans. Parmi les cent déterminans compris de 801 à 900, on en trouve 7 auxquels ne correspond qu'un genre, 32, 52, 8, 1 auxquels correspondent respectivement 2, 4, 8, 16 genres. Il en résulte en tout 359 genres, et partant, pour le nombre moyen 3,59. Les cent déterminans négatifs depuis — 801 jusqu'à —900, produisent 360 genres. Les exemples suivans sont tous pris des déterminans négatifs. Dans la seizième centaine, c'est-à-dire, depuis — 1501 jusqu'à 1600, le nombre moyen de genres est 3,89; dans la vingt-cinquième, il est 4,03; les six cents déterminans compris de — 9401 à — 10000 donnent 4,59. Ces exemples font voir que les nombres moyens de genres croîtraient bien plus lentement que les déterminans; mais il s'agirait maintenant de savoir quelle est la loi de cette progression.

Une recherche fondée sur une théorie assez difficile, et qu'il serait trop long d'exposer ici, nous a fait trouver que le nombre moyen des genres, pour le déterminant $+D$ ou $-D$, était exprimé d'une manière extrêmement approchée par la formule : $\alpha \log D + \beta$, où α et β sont des quantités constantes, et telles qu'on a, π étant la demi-circonférence dont le rayon est 1,

$$\alpha = \frac{4}{\pi^2} = 0{,}4052847346,$$

$$\beta = 2\alpha g + 3\alpha^2 h - \tfrac{1}{2}\alpha \log. 2 = 0{,}8830460462,$$

g étant la somme de la série

$$1 - \log.(1+1) + \tfrac{1}{2} - \log.(1+\tfrac{1}{2}) + \tfrac{1}{3} - \log.(1+\tfrac{1}{3}) + \text{etc.}$$
$$= 0{,}5772156649, \qquad (\textit{Euler, Calc. diff. p. } 444),$$

et h la somme de la série

$$\tfrac{1}{4}\log.2 + \tfrac{1}{9}\log.3 + \tfrac{1}{16}\log.4 + \text{etc.} = 0{,}9375482543.$$

Cette formule fait voir que les nombres moyens des genres croissent en progression arithmétique, si les déterminans croissent en progression géométrique. Elle donne pour les déterminans

$$850\tfrac{1}{2}; \quad 1550\tfrac{1}{2}; \quad 2450\tfrac{1}{2}; \quad 5050\tfrac{1}{2}; \quad 9700\tfrac{1}{2},$$

les valeurs

$$3{,}627; \quad 3{,}860; \quad 4{,}046; \quad 4{,}339; \quad 4{,}601$$

respectivement, qui ne diffèrent presque pas des nombres moyens donnés plus haut. Plus le déterminant moyen sera grand, et plus on prendra de déterminans pour calculer le nombre moyen de genres, moins ce dernier différera de la valeur de la formule. A l'aide de cette formule, on peut trouver avec beaucoup de précision la somme des nombres de genres qui répondent aux déterminans successifs $\pm D$, $\pm(D+1)$, $\pm(D+2)$, etc. $\pm(D+m)$, en ajoutant ensemble les nombres moyens de genres qui correspondent à ces différens déterminans, quelque différence qu'il y ait entre les extrêmes D et $D+m$. Cette somme sera

$$\alpha\{\log.D + \log.(D+1) + \log.(D+2) + \text{etc.} + \log.(D+m)\} + (m+1)\beta;$$

ou assez exactement

$$\alpha\{(D+m)\log.(D+m) - (D-1)\log.(D-1)\} + (m+1)(\beta-\alpha).$$

De cette manière, on trouve que le nombre des genres depuis le déterminant -1, jusqu'au déterminant -100, est $= 234{,}4$, tandis qu'il est en effet 233. De même, depuis -1 jusqu'à -2000, on trouve 7116,6 genres, tandis qu'il y en a en effet 7112; de 9001 à 10000, on trouve 4594,9, et il y en a 4595, approximation plus grande qu'on ne pouvait l'espérer.

302. A l'égard du nombre de classes (proprement primitives positives, comme on doit toujours le sous-entendre), les déterminans positifs et les déterminans négatifs se comportent d'une

manière bien différente ; aussi nous les considérerons séparément: ils s'accordent cependant tous en cela que, pour un déterminant donné, chaque genre contient le même nombre de classes, et que partant, le nombre de toutes les classes est égal au produit du nombre de genres par le nombre de classes contenues dans chaque genre.

Considérons d'abord les déterminans négatifs ; les nombres de classes qui répondent à plusieurs déterminans successifs, $-D$, $-(D+1)$, $-(D+2)\ldots$, etc. forment une progression aussi irrégulière que celle des genres. Mais *les nombres moyens de classes* croissent très-régulièrement, comme on le verra par les exemples suivans. Les cent déterminans depuis —500, jusqu'à—600, donnent 1729 classes; donc le nombre moyen est 17,29. De même, dans la quinzième centaine, le nombre moyen de classes se trouve être 28, 26. De la vingt-quatrième et de la vingt-cinquième centaines on tire 36, 28; des soixante-unième, soixante-deuxième et soixante-troisième, il résulte 58,50; de la quatre-vingt-onzième à la quatre-vingt-quinzième, c'est-à-dire de 9001 à 9500, on trouve 71,56, et de la quatre-vingt-seizième à la centième, 73,54. Ces exemples montrent que si les nombres moyens et classes croissent beaucoup plus lentement que les déterminans, ils croissent beaucoup plus rapidement que les nombres moyens de genres; avec une légère attention, on apperçoit qu'ils croissent à peu-près comme les racines quarrées des déterminans moyens. Et en effet, par une recherche fondée sur la théorie, nous avons trouvé que le nombre moyen de classes pour le déterminant $-D$, était exprimé d'une manière très-approchée par $\gamma\sqrt{D}-\beta$; ou l'on a

$$\gamma = 0{,}7467183115 = \frac{2\pi}{7\theta},\ \text{et}\ \theta = 1+\tfrac{1}{8}+\tfrac{1}{27}+\tfrac{1}{64}+\tfrac{1}{125}+\text{etc.},$$

$$\beta = 0{,}2026423673 = \frac{2}{\pi^2};$$

les nombres moyens calculés d'après cette formule, diffèrent peu de ceux que nous avons extraits plus haut de la table de classification. A l'aide de cette formule, on peut aussi assigner assez exactement la somme de tous les nombres de classes qui répondent à plusieurs déterminans successifs

$$-D, -(D+1), -(D+2), \ldots\ldots -(D+m-1),$$

quelque différence qu'il y ait entre les extrêmes; en ajoutant les nombres moyens qui, d'après la formule, appartiennent à ces déterminans. On trouve pour cette somme

$$\gamma\{\sqrt{D}+\sqrt{(D+1)}+\text{etc.}+\sqrt{(D+m-1)}\}+\delta m.$$

ou..... $\frac{2}{3}\gamma\{(D+m-\frac{1}{2})^{\frac{3}{2}}-(D-\frac{1}{2})^{\frac{3}{2}}\}+\delta m$

à très-peu-près. Ainsi, par exemple, pour les cent déterminans compris de —1 à —100, la formule donne 481,1, tandis que le nombre exact est 477; les mille déterminans —1....—1000. donnent, d'après la table, 15533 classes, et par la formule, 15551,4; le second mille donne, d'après la table, 28603, et par la formule, 28585,7; de même le troisième mille donne effectivement 37092, et par la formule, 37074,3; enfin pour le dixième mille la table donne 72549, et la formule, 72572.

303. La table des déterminans négatifs, disposée d'après la diversité des classifications, fournit plusieurs autres observations remarquables. Pour les déterminans de la forme $-(8n+3)$, le nombre des classes contenues, tant dans chaque genre proprement primitif que dans l'ensemble de tous ces genres, est toujours divisible par 3, le seul déterminant —3 excepté, ainsi qu'on peut le conclure du n° 256, VI. Quant aux déterminans pour lesquels les formes ne composent qu'un seul genre, le nombre de classes est toujours impair; en effet, comme pour un pareil déterminant il n'y a jamais qu'une classe ambiguë, qui est la classe principale, le nombre des autres classes qui seront opposées deux à deux sera nécessairement pair, et partant le nombre de toutes les classes sera impair. — Or la série des déterminans auxquels répond une même classification donnée, c'est-à-dire, un nombre donné de genres et de classes, paraît toujours finie; nous allons faire appercevoir cette observation surprenante, dans quelques exemples. Dans la table suivante, le premier nombre, en chiffres romains, indique le nombre de genres proprement primitifs positifs; le second, le nombre de classes contenues dans chaque genre; toutes les autres forment la série des déterminans auxquels cette classification appartient.

I.....1...1, 2, 3, 4, 7;
I.....3...11, 19, 23, 27, 31, 43, 67, 163;
I.....5...47, 79, 103, 127;
I.....7...71, 151, 223, 343, 463, 487;
II.....1...5, 6, 8, 9, 10, 12, 13, 15, 16, 18, 22, 25, 28, 37, 58;
II.....2...14, 17, 20, 32, 34, 36, 39, 46, 49, 52, 55, 63, 64, 73, 82, 97, 100, 142, 148, 193;
IV.....1...21, 24, 30, 33, 40, 42, 45, 48, 57, 60, 70, 72, 78, 85, 88, 93, 102, 112, 130, 133, 177, 190, 232, 253;
VIII...1...105, 120, 165, 168, 210, 240, 273, 280, 312, 330, 345, 357, 385, 408, 462, 520, 760;
XVI...1...840, 1320, 1365, 1848.

On trouve de même vingt déterminans, dont le plus grand est —1423, auxquels répond la classification I.9; quatre, dont le plus grand est —1303, auxquels répond la classification I.11, etc. Les classifications II.3, II.4, II.5, IV.2, ne répondent pas à plus de 48, 32, 42, 68 déterminans, dont les plus grands sont respectivement —652, —862, —1318, —1012. Comme la table dans laquelle nous avons pris ces exemples a été prolongée bien au-delà des déterminans qui paraissent ici (*), et qu'elle ne fournit aucun autre déterminant qui appartienne à ces classifications, il paraît hors de doute que les séries précédentes sont finies, et l'on peut, par analogie, étendre la même conclusion à toute autre classification. Par exemple, comme dans tout le dixième millier de déterminans, il ne s'en rencontre aucun qui réponde à moins de vingt-quatre classes, il est extrêmement vraisemblable que les classifications

I.23, I.21, etc.; II.11, II.10, etc.;
IV.5, IV.4, IV.3, etc.; VIII.2, etc.

s'étaient arrêtées avant —9000, ou qu'elles n'ont lieu que pour peu de déterminans plus grands que —10000; mais il paraît très-difficile de donner de ces observations des démonstrations rigoureuses.

(*) Pendant que cet ouvrage s'imprime, nous l'avons poussée sans interruption jusqu'à —3000; nous y avons ajouté le dixième millier tout entier, plusieurs centaines éparses et un grand nombre de déterminans isolés choisis avec soin.

Il est encore à remarquer que tous les déterminans dont les formes peuvent se distribuer en trente-deux genres au plus, ont au moins deux classes dans chaque genre, desorte que les classifications XXXII.1, LXIV.1, etc. n'existent point. Le plus petit déterminant de cette espèce est —9240, et la classification qui lui répond est XXXII.2; et il est assez probable que, le nombre des genres augmentant continuellement, le nombre des classifications qui disparaissent augmente aussi. A cet égard, les soixante-cinq déterminans inscrits plus haut, auxquels répondent les classifications: I.1, II.1, IV.1, VIII.1, XVI.1, méritent d'être distingués, et il est facile de voir qu'ils jouissent tous et seuls de deux propriétés remarquables; la première consiste en ce que les classes suivant lesquelles se distribuent leurs formes sont toutes ambiguës; la seconde, en ce que deux formes quelconques contenues dans le même genre sont équivalentes, tant proprement qu'improprement. Au reste, ces mêmes soixante-cinq nombres ont déjà été présentés par *Euler* (*Nouv. Mém. de l'Ac. de Berlin*, 1776, *p.* 338), sous un aspect un peu différent, dont nous parlerons plus bas, et avec une propriété facile à démontrer.

304. Le nombre des classes proprement primitives que fournissent les formes binaires de déterminant *quarré* k^2, peut être assigné *à priori;* il y a autant de ces classes que de nombres premiers avec $2k$ et plus petits que lui. De là, à l'aide de raisonnemens qui n'ont aucune difficulté, mais que nous supprimons, on trouve que le nombre moyen des classes qui appartiennent à des déterminans quarrés voisins de k^2 est exprimé d'une manière très-approchée par $\frac{8k}{\pi^2}$.

Quant aux déterminans positifs non-quarrés, ils présentent à cet égard des propriétés tout-à-fait singulières. Pour les déterminans négatifs ou quarrés, les petits nombres de classes, par exemple les classifications I.1, ou I.3, ou II.1, n'ont lieu que pour de petits déterminans et dont la suite s'arrête bientôt; pour les déterminans positifs non-quarrés au contraire, pourvu qu'ils ne soient pas très-grands, la plus grande partie donne des classifications où il n'y a qu'une seule classe dans chaque genre, desorte que les classifications: I.3, I.5, II.2, II.3, IV.2, etc.

sont très-rares. Ainsi, par exemple, parmi les quatre-vingt-dix déterminans non-quarrés qui sont au-dessous de 100, on en trouve trois 11, 48, 27 auxquels répondent les classifications I.1, II.1, IV.1, respectivement; et il y en a un, 37, auquel répond I.3; deux, 34 et 82, auxquels répond II.2, et un, 79, auquel répond II.3. Cependant, à mesure que les déterminans augmentent, les nombres de classes plus élevés se multiplient peu-à-peu. Par exemple, parmi les quatre-vingt-seize déterminans non-quarrés qui sont compris entre 100 et 200, il y en a deux, 101 et 197, auxquels répond I.3; quatre, 145, 146, 178, 194, auxquels répond II.2; trois, 141, 148, 189, auxquels répond II.3. Parmi les cent quatre-vingt-dix-sept déterminans non-quarrés compris depuis 801 jusqu'à 1000, il y en a

3, 4, 14, 2, 2, 15, 6, 2, 4,

auxquels répondent respectivement les classifications

I.3, II.2, II.3, II.5, II.6, IV.2, IV.3, IV.4, VIII.2.

Pour les cent quarante-cinq autres, il n'y a qu'une classe dans chaque genre.

Ce serait une question curieuse, et qui ne serait pas indigne de la prétention des géomètres, que de chercher suivant quelle loi les déterminans qui ne donnent qu'une classe par genre deviennent de plus en plus rares. Jusqu'à présent nous ne pouvons décider par la théorie, ni tirer de l'observation des conjectures assez certaines pour affirmer si la série s'arrête toujours, ce qui paraît au reste peu probable, ou du moins si ces déterminans deviennent infiniment rares, ou si le nombre tend toujours et de plus en plus vers une certaine limite fixe. Les nombres moyens de classes croissent dans un rapport qui n'est guère plus grand que celui des nombres moyens de genres, et bien plus lentement que les racines quarrées des déterminans: entre 800 et 1000, on trouve 5,01. Qu'il nous soit permis d'ajouter une autre observation, qui rétablit en quelque sorte l'analogie entre les déterminans positifs et négatifs. Nous avons trouvé que si le nombre des classes pour un déterminant positif D n'était pas analogue au nombre des classes pour le déterminant négatif, la chose a lieu du moins pour le produit de ce nombre par le logarithme de $t+u\sqrt{D}$;

t et u désignant les plus petits nombres, excepté 1 et 0, qui satisfont à l'équation $t^2 - Du^2 = 1$, nous ne pouvons donner plus de détails sur la raison de cette analogie. La valeur moyenne de ce produit s'exprime assez exactement par la formule $m\sqrt{D} - n$; mais nous n'avons pas encore pu déterminer par la théorie les constantes m et n. S'il est permis de tirer une conclusion de la comparaison de quelques centaines de déterminans, m paraît peu différent de $2\frac{1}{3}$.

Au reste, nous nous réservons de revenir dans une autre occasion sur les valeurs moyennes des quantités qui ne suivent pas une loi analytique, mais qui approchent continuellement et de plus en plus de la suivre. Nous passons maintenant à une autre recherche, par laquelle nous comparerons entre elles les différentes classes proprement primitives de même déterminant, et qui terminera cette longue Section.

305. THÉORÈME. K *désignant la classe principale des formes de déterminant donné* D, C *une autre classe quelconque prise dans le genre principal de même déterminant*, C^2, C^3, C^4, C^5, *etc. les classes qui naissent de la duplication, de la triplication, etc. de la classe* C (Voyez n° 249); *en continuant assez loin la progression* C, C^2, C^3, *etc., on parviendra enfin à une classe identique avec* K; *et si l'on suppose que* C^m *soit la première classe identique avec* K, *et que le nombre de toutes les classes du genre principal soit* n, *on aura* m=n, *ou bien* m *sera une partie aliquote de* m.

I. Comme toutes les classes K, C, C^2, C^3, etc. appartiennent nécessairement au genre principal, les $n+1$ premières classes de cette série K, C, C^2, ... C^n ne peuvent pas être différentes; ainsi K sera donc identique avec une des classes C, C^2, C^3.... C^n, ou deux d'entre elles seront identiques. Soit donc $C^r = C^s$ et $r > s$, on aura aussi $C^{r-1} = C^{s-1}$, $C^{r-2} = C^{s-2}$, etc., et $C^{r+1-s} = C$, d'où $C^{r-s} = K$.

II. Il suit de là sur-le-champ que l'on a $m = n$, ou $m < n$; ainsi il ne reste plus qu'à faire voir que, dans le second cas, m est une partie aliquote de n. Comme les classes K, C, C^2... C^{m-1}, dont nous désignerons l'ensemble par (Γ), n'épuisent pas le genre principal,

principal, soit C' une classe de ce genre qui ne soit pas contenue dans (Γ), et désignons par (Γ') l'ensemble de toutes les classes qui résultent de la composition de C' avec chacune des classes de (Γ). On voit facilement que toutes les classes de (Γ') sont différentes tant entre elles que des classes contenues dans (Γ), et qu'elles sont du genre principal; desorte que si (Γ) et (Γ') épuisent ce genre, on aura $n = 2m$, sinon on aura $2m < n$. Soit donc, dans le second cas, C'' une classe du genre principal qui ne soit contenue ni dans (Γ), ni dans (Γ'), et désignons par (Γ'') l'ensemble de toutes les classes qui résultent de la décomposition de C'' avec toutes les classes de (Γ); il est évident qu'elles diffèrent toutes entre elles et des classes contenues dans (Γ) et (Γ'), et qu'elles sont du genre principal; donc si (Γ), (Γ'), (Γ'') épuisent ce genre, on aura $n = 3m$, sinon $n > 3m$. Dans ce dernier cas, en traitant de la même manière une classe C''' qui ne soit contenue ni dans (Γ), ni dans (Γ'), ni dans (Γ''), il en résultera que l'on a $n = 4m$, ou $m > 4m$, et ainsi de suite. Or comme n et m sont des nombres finis, le genre principal s'épuisera enfin, et n sera un multiple de m, ou m une partie aliquote de n.

Soit, par exemple, $D = -356$, $C = (5, 2, 72)$ (*); on trouve $C^2 = (20, 8, 21)$, $C^3 = (4, 1, 89)$, $C^4 = (20, -8, 21)$, $C^5 = (5, -2, 72)$, $C^6 = (1, 0, 356)$. On a donc ici $m = 6$, et pour ce déterminant $n = 12$. En prenant $C' = (8, 2, 45)$, les cinq autres classes de (Γ') sont : $(9, -2, 40)$, $(9, 2, 40)$, $(8, -2, 45)$, $(17, 1, 21)$, $(17, -1, 21)$.

306. On remarquera sur-le-champ l'analogie de la démonstration du théorème précédent, avec les démonstrations des n°s 45, 49; et effectivement, la théorie de la multiplication des classes a une grande affinité avec le sujet traité dans la Section III. Mais les limites de cet ouvrage ne nous permettent pas de poursuivre cette théorie qui est digne de grands développemens; aussi nous n'ajouterons que quelques observations, et nous supprimerons les démonstrations qui exigeraient trop de détails, nous réservant encore de revenir sur ce sujet et de l'approfondir.

(*) Nous exprimons toujours les classes par les formes les plus simples qu'elles renferment.

1°. Si la série $K, C, C^2, C^3 \ldots C^{m-1}$ est prolongée au-delà de C^{m-1}, les mêmes classes reparaissent de nouveau, desorte qu'on a $C^m = K$, $C^{m+1} = C$, $C^{m+2} = C^2$, etc.; et généralement, si l'on regarde K comme C^0, les classes C^g et $C^{g'}$ seront identiques ou différentes, suivant que g et g' seront congrus ou incongrus suivant le module m. Ainsi la classe C^n est toujours identique avec la classe principale K.

2°. Nous appellerons *périodes de la classe* C l'ensemble K, C, C^2, $C^3 \ldots C^{m-1}$, que nous avons désigné par (Γ); mais cette expression ne doit pas être confondue avec les *périodes* de formes réduites de déterminant positif non-quarré, dont nous avons parlé n° 186 et suivans. Ainsi il est clair que de la composition de tant de classes qu'on voudra d'une même période, il résulte une classe contenue dans la période C^g, $C^{g'}$, $C^{g''}$, etc. $= C^{g+g'+g''+\text{etc.}}$

3°. Comme $C.C^{m-1} = K$, les classes C et C^{m-1} seront opposées, et partant C^2 et C^{m-2}, C^3 et C^{m-3}, etc. Ainsi, lorsque m est pair, la classe $C^{\frac{m}{2}}$ sera elle-même son opposée, et sera par-conséquent ambiguë; réciproquement, si, indépendamment de K, il se trouve dans (Γ) une autre classe ambiguë C^g, on aura $C^g = C^{m-g}$, et partant $g = m - g = \frac{1}{2}m$. Il suit de là que si m est pair, il n'y a pas d'autre classe ambiguë que K et C^g, et que si m est impair, il n'y en a pas d'autre que K.

4°. Si la période d'une classe C^h contenue dans (Γ) est K, C^h, C^{2h}, $C^{3h} \ldots C^{(m'-1)h}$, il est évident que $m'h$ est le plus petit multiple de h qui soit divisible par m. Si donc m et h sont premiers entre eux, on aura $m = m'$, et les deux périodes contiendront les mêmes classes, mais dans un ordre différent; mais généralement, μ étant le plus grand commun diviseur des nombres m, h, on aura $m' = \frac{m}{\mu}$; d'où il suit que le nombre de classes contenues dans la période d'une classe quelconque prise dans (Γ) est m ou une partie aliquote de m, et qu'il y a autant de classes de (Γ) dont les périodes soient composées de m termes, qu'il y a de nombres premiers avec m dans la suite 0, 1, 2, $\ldots m-1$, c'est-à-dire, qu'il y en a φm, en employant le signe du n° 39. Généralement, il y aura autant de classes dans (Γ) dont les périodes

soient composées de $\frac{m}{\mu}$ termes, qu'il y a dans la suite 0, 1, 2...m—1 de nombres qui aient μ pour plus grand commun diviseur avec m. On voit facilement que le nombre en est $\varphi\frac{m}{\mu}$. Si donc $m=n$, c'est-à-dire, si (Γ) renferme tout le genre principal, il y a dans ce genre φn classes dont les périodes renferment le genre entier, et φe classes dont les périodes renferment un nombre e de termes, e désignant un diviseur quelconque de n. Cette conclusion a généralement lieu, quand il existe une classe du genre principal dont la période ait n termes.

5°. Dans la même supposition, le système des classes du genre principal ne peut être disposé plus convenablement, qu'en prenant, comme pour base, une classe dont la période ait n termes, et plaçant les classes du genre principal dans l'ordre qu'elles occupent dans cette période. Desorte que si l'on affecte la classe principale de l'indice 0, la classe prise pour base aura l'indice 1, et ainsi de suite. La seule addition des indices suffit pour trouver quelle classe naît de la composition de classes quelconques du genre principal.

Voici un exemple pour le déterminant —356, où la classe (9, 2, 40) a été prise pour base :

0...(1, 0, 356)	3...(8, —2, 45)	6...(4, 0, 89)	9...(8, 2, 45)
1...(9, 2, 40)	4...(20, 8, 21)	7...(17, —1, 21)	10...(5, —2, 72)
2...(5, 2, 72)	5...(17, 1, 21)	8...(20, —8, 21)	11...(9, —2, 40).

6°. Quoique l'analogie avec la Section III, et l'induction qu'on peut tirer de plus de deux cents déterminans négatifs, et d'un bien plus grand nombre de déterminans positifs non-quarrés, semblent porter au plus haut degré de probabilité la vérité de cette supposition pour tous les déterminans, une pareille conclusion n'en serait pas moins fausse et démentie par la continuation de la table de classification. Nous nommerons, pour abréger, déterminans *réguliers* ceux pour lesquels une seule période peut renfermer tout le genre principal, et déterminans *irréguliers* ceux qui ne jouissent pas de cette propriété (*). Un petit nombre d'ob-

(*) Voyez les Additions de l'auteur.

servations nous suffiront pour éclaircir ce sujet, qui semble cependant dépendre des plus profonds mystères de l'Arithmétique transcendante, et donner lieu aux recherches les plus difficiles; nous commencerons par la suivante, qui est générale.

7°. Si dans le genre principal se trouvent deux classes C, C', dont les périodes sont composées de m, m' termes, et que M soit le plus petit nombre divisible par m et par m'; il y aura aussi dans le même genre une classe dont la période contiendra M termes: si l'on décompose M en deux facteurs r et r' premiers entre eux dont l'un, r, divise m, et dont l'autre, r', divise m' (n° 73), la classe $C^{\frac{m}{r}}.C'^{\frac{m'}{r'}}=C''$ jouira de la propriété précitée. En effet, supposons que la période de la classe C'' soit composée de g termes, on aura

$$K=C''^{gr}=C^{gm}.C'^{\frac{grm'}{r'}}=K.C'^{\frac{grm'}{r'}}=C'^{\frac{grm'}{r'}};$$

donc $\frac{grm'}{r'}$ est divisible par m', et partant gr par r' ou g par r'. On prouve absolument de la même manière que g est divisible par r, donc il l'est par $rr'=M$; mais comme on a évidemment $C''^{M}=K$, M est donc aussi divisible par g, et partant $M=g$. Il suit de là que le plus grand nombre de classes qui puissent être contenues dans une période pour un déterminant donné, est divisible par le nombre de classes de toute autre période d'une classe du même genre principal. On peut en même temps en déduire une méthode pour trouver la classe dont la période est la plus grande, c'est-à-dire, pour les déterminans réguliers, la classe dont la période renferme tout le genre principal; cette méthode est absolument semblable à celle des n°s 73 et 74; mais dans la pratique on peut l'abréger par plusieurs artifices. Le quotient de la division du nombre n par le nombre de termes de la plus grande période, quotient qui est 1 pour les déterminans réguliers, et plus grand que 1 pour les déterminans irréguliers, est d'après cela très-commode pour exprimer les différentes espèces d'irrégularités, et par cette raison pourra être nommé *exposant d'irrégularité*.

8°. Jusqu'à présent il n'y a pas de règle générale qui puisse faire distinguer *à priori* les déterminans réguliers des irréguliers,

d'autant plus que parmi les derniers se trouvent en même temps des nombres premiers et des nombres composés; ainsi il suffira d'ajouter ici quelques observations particulières. Quand il y a plus de deux classes ambiguës dans le genre principal, le déterminant est surement irrégulier, et l'exposant d'irrégularité est pair. Mais quand il n'y a qu'une ou deux classes ambiguës, le déterminant est régulier, ou du moins l'exposant d'irrégularité est impair. Tous les déterminans négatifs de la forme $-(216k+27)$, le nombre -27 excepté, sont irréguliers, et l'exposant d'irrégularité est divisible par 3. La même chose a lieu pour les déterminans négatifs de la forme $-(1000k+75)$ et $-(1000k+675)$, en exceptant le seul nombre -75, et pour une infinité d'autres.

Si l'exposant d'irrégularité est un nombre premier p, n est divisible par p^2; desorte que si n n'est divisible par aucun nombre quarré, le déterminant sera nécessairement régulier.

Il n'y a que pour les déterminans positifs quarrés e^2 que l'on puisse distinguer *à priori*, s'ils sont réguliers ou irréguliers. Le premier cas arrive quand e est 1 ou 2, ou un nombre premier impair, ou une puissance d'un nombre premier impair; le second pour toute autre valeur de e.

Pour les déterminans négatifs, les irréguliers deviennent d'autant plus fréquens, que les déterminans seront plus grands. Par exemple, dans le premier millier, on trouve 13 irréguliers qui sont, en omettant le signe,

576, 380, 820, 884, 900, dont l'exposant d'irrégularité est 2.
243, 307, 339, 459, 675, 755, 891, 974, dont l'exposant est 3.

Dans le second millier, on en trouve 13 dont l'exposant est 2, et 15 dont l'exposant est 3. Dans le dixième millier, 31 dont l'exposant est 2, et 32 dont l'exposant est 3. Nous ne pouvons encore décider s'il existe au-dessous de -10000 des déterminans dont l'exposant d'irrégularité soit plus grand que 3. Au-delà de cette limite, on peut trouver des déterminans qui aient un exposant donné quelconque. Il est probable que les déterminans croissant toujours, le nombre de ceux qui sont irréguliers tend à être dans un rapport constant avec le nombre des déterminans réguliers. La détermination de ce rapport serait digne de la sagacité des géomètres.

Parmi les déterminans positifs non quarrés, les irréguliers sont plus rares; il y en a une infinité pour lesquels l'exposant est 2, par exemple 3026 a 2 pour exposant d'irrégularité. Il semble aussi hors de doute qu'il existe des déterminans dont l'exposant d'irrégularité soit impair, quoique nous soyons forcés d'avouer qu'il ne s'en est pas offert à nous jusqu'à présent.

9°. Nous ne pouvons, sans donner trop d'étendue à cet ouvrage, parler ici de la disposition la plus commode du système des classes contenues dans le genre principal pour un déterminant irrégulier; nous observerons seulement que comme dans ce cas une base ne peut suffire, il faut en prendre deux ou un plus grand nombre qui, par la multiplication et la composition, puissent produire toutes les classes. De là naîtront des indices *doubles ou multiples* qui auront presque le même usage que les indices simples pour les déterminans réguliers.

10°. Observons enfin que toutes les propriétés considérées dans ce n° et dans le précédent, dépendant principalement du nombre n, qui a quelque analogie avec le nombre $p-1$ de la section III, ce nombre mérite une grande attention; il serait donc à desirer que l'on pût découvrir une relation générale entre n et le déterminant. Nous pensons que l'on doit d'autant moins désespérer d'y parvenir, que nous avons déjà réussi à soumettre à une formule analytique, du moins pour les déterminans négatifs (n° 302), la valeur moyenne du produit de n par le nombre de genres qui peut être assignée *à priori*. (*).

307. Les recherches précédentes n'embrassent que les classes du genre principal, et suffisent parconséquent, tant pour les déterminans positifs qui ne donnent qu'un seul genre, que pour les déterminans qui ne donnent qu'un genre positif, si nous ne considérons pas le genre négatif. Il nous reste à ajouter quelque chose sur les autres genres proprement primitifs.

1°. Lorsque le genre G' différant du genre principal G de même déterminant, renferme quelque classe ambiguë, il y en aura autant dans l'un et l'autre genre. Soient L, M, N, etc. les classes

(*) Voyez les Additions de l'auteur.

ambiguës de G, parmi lesquelles se trouve la classe principale K, et L', M', N', etc. les classes ambiguës contenues dans G'; et désignons l'ensemble des premières par A, l'ensemble des dernières par A'. Comme toutes les classes $L.L'$, $M.L'$, $N'.L'$, etc. sont évidemment ambiguës, et du genre G', elles feront nécessairement partie de A'; et partant, le nombre de classes contenues dans A' n'est surement pas plus petit que celui des classes contenues dans A : d'ailleurs les classes $L'.L'$, $M'.L'$, $N'.L'$, etc. étant ambiguës et du genre G, elles feront nécessairement partie de A; donc le nombre de classes contenues dans A n'est pas plus petit que le nombre de classes contenues dans A'. Donc les nombres de classes de A et de A' sont nécessairement égaux.

2°. Comme le nombre de toutes les classes ambiguës est égal au nombre des genres (n°s 261 et 287, 3°.), il est évident que si G ne contient qu'une classe ambiguë, chaque genre en contiendra nécessairement une et une seule; si G contient deux classes ambiguës, la moitié de tous les genres en contiendra deux, et les autres n'en contiendront aucune; enfin, s'il y a dans G un nombre a de classes ambiguës (*), et que N soit le nombre total des genres, il y aura $\frac{N}{a}$ genres qui contiendront a classes ambiguës, et les autres n'en contiendront pas.

3°. Soient, pour le cas où G renferme deux classes ambiguës, G, G', G'', etc. les genres qui en contiennent deux; H, H', H'', etc. ceux qui n'en contiennent point; et désignons par g l'ensemble des premiers, et par h l'ensemble des derniers. Comme la composition de deux classes ambiguës donne toujours pour résultante une classe ambiguë (n° 249), on verra sans peine que la composition de deux genres compris dans g donne un genre compris dans g. Il suit de là que de la composition d'un genre de g avec un genre de h, il résulte un genre de h. En effet, si par exemple $G'.H$ appartenait à g, $G'.H.G'$ serait aussi compris dans g; mais $G'.G' = G$, et il s'ensuivrait que H serait compris dans g, contre l'hypothèse. Enfin on reconnaît facilement que les genres

$$G.H,\ G'.H,\ G''.H,\ \text{etc.}\quad H.H,\ H'.H,\ H''.H,\ \text{etc.}$$

(*) Cela ne peut arriver que pour les déterminans irréguliers, et a sera toujours une puissance de 2.

sont tous différens entre eux, et que, pris ensemble, ils équivalent à g et à h. Mais par ce qui vient d'être démontré, les genres $G.H$, $G'.H$, $G''.H$, etc. appartiennent tous à h, et partant, l'épuisent entièrement; donc les genres $H.H$, $H'.H$, $H''.H$, etc. appartiennent nécessairement à g, et partant, la composition de deux genres de h donne toujours un genre de g.

4°. Si E est une classe du genre V différent du genre principal G, il est clair que E^2, E^4, E^6, etc. appartiennent toutes à G, tandis que E^3, E^5, E^7, etc. appartiennent à V. Si donc la période de la classe E^2 est composée de m termes, il est évident que dans la suite E, E^2, E^3, etc., la classe E^{2m} sera indentique avec K, et qu'aucune ne pourra l'être avant elle, c'est-à-dire, que la période de la classe E sera composée de $2m$ termes; donc le nombre de termes de la période d'une classe quelconque, d'un autre genre que le genre principal, sera $2n$ ou une partie aliquote de $2n$, n désignant le nombre de classes commun à tous les genres.

5°. Soit C une classe donnée du genre principal G, E une classe du genre V qui donne C par sa duplication (n° 286), et K, K', K'', etc., toutes les classes ambiguës proprement primitives de même déterminant; toutes les classes dont la duplication donne C seront: $E(=E.K)$, $E.K'$, $E.K''$, etc., dont nous exprimerons l'ensemble par ω, et dont le nombre sera évidemment égal au nombre des classes ambiguës, ou au nombre des genres. Il est manifeste que parmi les classes ω, il y en a autant qui appartiennent au genre V, qu'il y a de classes ambiguës dans le genre G; ainsi, désignant par a le nombre de ces dernières, il y a dans chaque genre a classes comprises dans ω; ou il n'y en a aucune. On déduit facilement de là, que si $a=1$, chaque genre contient une des classes ω; si $a=2$, la moitié des genres contiennent deux des classes ω, tandis que les autres n'en contiennent aucune, et même la première moitié coïncide avec g (v. 3°.), et la seconde avec h, et réciproquement. Quand a est plus grand il y a toujours, en désignant par N le nombre de tous les genres, $\frac{N}{a}$ genres qui contiennent des classes ω, et chacune en contient a.

6°. Supposons maintenant que C soit une classe dont la période soit composée de n termes; on voit facilement que dans le cas où

$a=2$,

$a = 2$, et où partant, n est pair, aucune classe de ω ne peut appartenir à G; car alors cette classe serait contenue dans la période de C; et si on la représente par C^r, il s'ensuivrait $C^{2r} = C$, et partant, $2r \equiv 1 \pmod{n}$, ce qui est absurde. Ainsi, comme G appartient à g, toutes les classes ω seront nécessairement distribuées entre les genres h. Puisque pour un déterminant régulier, G contient φn classes dont les périodes sont de n termes, il suit de ce qui précède que pour le cas où $a = 2$, il y a dans chaque genre h, $2\varphi n$ classes dont la période contient $2n$ termes, et renferme parconséquent à-la-fois le genre de la classe et le genre principal. Mais quand $a = 1$, il y aura φn classes de cette espèce dans chaque genre différent du genre principal.

7°. Nous établissons sur ces observations la méthode suivante, pour former le système de toutes les classes proprement primitives de déterminant régulier donné, car nous laissons absolument de côté les déterminans irréguliers. On prendra à volonté une classe E, dont la période contienne $2n$ termes, et parconséquent le genre de cette forme que nous nommerons V, et le genre principal G, et l'on distribuera les classes de ces deux genres comme elles se présentent dans cette période. L'opération serait finie, quand il n'existera que ces deux genres, ou que l'on n'aura pas besoin de s'occuper des autres (par exemple, pour un déterminant négatif qui ne donne que deux genres positifs). Mais quand il y a quatre, ou un plus grand nombre de genres, on traitera les autres de la manière suivante. Soit V' un des deux autres, et $V \times V' = V''$. Il y aura dans V' et V'' deux classes ambiguës, une dans chacun, ou deux dans l'une et aucune dans l'autre. On en prendra une A à volonté, et l'on voit facilement que si l'on compose A avec chacune des classes de G et de V, il en résultera $2n$ classes différentes qui appartiendront à V' et V'', et épuiseront parconséquent ces deux genres, que l'on pourra disposer aussi de cette manière.

S'il y a plus de quatre genres, soit V''' un des autres, et V^{IV}, V^{V}, V^{VI} les genres qui résultent de la composition du genre V''' avec les genres V, V', V''; les quatre genres V'''..... V^{VI}, contiendront quatre classes ambiguës, et il est clair que si l'on prend

une d'elles, et qu'on la compose avec chaque classe des genres G, V, V', V'', on obtiendra toutes les classes des genres $V'''\ldots V^{VI}$.

S'il y a d'autres genres, on continuera de la même manière, jusqu'à ce qu'ils soient tous épuisés. On voit, que si le nombre de tous les genres est 2μ, on aura besoin en tout de $\mu - 1$ classes ambiguës, et que toute classe de ces genres peut être produite ou par la multiplication de la classe E, ou par la composition d'une classe résultante de cette première opération avec une ou plusieurs classes ambiguës.

Nous ajoutons deux exemples qui serviront d'éclaircissement à ce procédé, mais nous ne pouvons rien dire de plus sur l'usage de cette construction, ni sur les artifices au moyen desquels on peut diminuer le travail.

I. Déterminant — 161.

Quatre genres positifs; dans chacun d'eux quatre classes.

G.	V.
$1, 4; R7; R23.$	$3, 4; N7; R23.$
$(1, 0, 161) = K$	$(3, 1, 54) = E$
$(9, 1, 18) = E^2$	$(6, -1, 27) = E^3$
$(2, 1, 81) = E^4$	$(6, 1, 27) = E^5$
$(9, -1, 18) = E^6$	$(3, -1, 54) = E^7.$

V'.	V''.
$3, 4; R^7; N23.$	$1, 4; N.7; N23.$
$(7, 0, 23) = A$	$(10, 3, 17) = A.E$
$(11, -2, 15) = A.E^2$	$(5, 2, 33) = A.E^3$
$(14, -7, 15) = A.E^4$	$(5, -2, 33) = A.E^5$
$(11, 2, 15) = A.E^6$	$(10, -3, 17) = A.E^7.$

II. Déterminant — 546.

Huit genres positifs; dans chacun d'eux trois classes.

G.	V.
1 et $3, 8; R3; R7; R13.$	5 et $7, 8; N3; N7; N13.$
$(1, 0, 546) = K$	$(5, 2, 110) = E$
$(22, -2, 35) = E^2$	$(21, 0, 26) = E^3$
$(22, 2, 25) = E^4$	$(5, -2, 110) = E^5.$

V'

1 et 3, 8; $N3$; $R7$; $N13$.

$(2, 0, 273) = A$
$(11, -2, 50) = A.E^2$
$(11, 2, 50) = A.E^4$

V''

5 et 7,8; $R3$; $N7$; $R13$.

$(10, 2, 55) = A.E$
$(13, 0, 42) = A.E^3$
$(10, -2, 55) = A.E^5$.

V''.

1 et 3, 8; $N3$; $N7$; $R13$.

$(3, 0, 182) = A'$
$(17, 7, 35) = A'.E^2$
$(17, -7, 35) = A'.E^4$

V^{IV}.

5 et 7, 8; $R3$; $R7$; $N13$.

$(15, -3, 37) = A'.E$
$(7, 0, 78) = A'.E^3$
$(15, 3, 37) = A'.E^5$.

V^{V}.

1 et 3, 8; $R3$, $N7$; $N13$.

$(6, 0, 91) = A.A'$
$(19, 9, 33) = A.A'.E^2$
$(19, -9, 33) = A.A'.E^3$.

V^{VI}.

5 et 7, 8; $N.3$; $R7$; $R13$.

$(23, 11, 29) = A.A'.E$
$(14, 0, 26) = A.A'.E^3$
$(23, -11, 29) = A.A'.E^5$.

SECTION SIXIÈME.

Applications des différentes Recherches précédentes.

308. Nous avons déjà indiqué en différens endroits combien l'arithmétique transcendante peut être utile dans les autres parties des mathématiques. Mais nous ne croyons pas inutile de traiter à part quelques applications qui méritent d'être exposées avec plus de détail, non dans la vue d'épuiser ce sujet, qui suffirait pour remplir plusieurs volumes, mais pour l'éclaircir par quelques exemples.

Dans cette Section, nous parlerons d'abord de la décomposition des fractions en fractions plus simples; ensuite, de la conversion des fractions ordinaires en fractions décimales; nous exposerons une nouvelle méthode d'exclusion, qui sert à la résolution des équations indéterminées du second degré; enfin, nous donnerons de nouvelles méthodes abrégées, pour distinguer les nombres premiers des nombres composés, et trouver les facteurs de ces derniers.

Dans la Section suivante, nous établirons la théorie générale d'une espèce particulière de fonctions, qui s'étend très-loin dans toute l'analyse, et qui est intimement liée à l'arithmétique transcendante; nous nous attacherons surtout à agrandir la théorie des sections du cercle, dont jusqu'à présent on n'a connu que les premiers élémens.

309. Problème. *Décomposer la fraction* $\frac{m}{n}$, *dont le dénominateur* n *est le produit de deux nombres* a *et* b *premiers entre eux, en deux autres dont les dénominateurs soient* a *et* b.

Soient $\frac{x}{a}$, $\frac{y}{b}$ les fractions cherchées; on doit avoir $bx+ay=m$; donc x sera racine de la congruence $bx \equiv m \pmod{a}$, et par-

conséquent peut se trouver par la Section II : on aura d'ailleurs $y = \frac{m-bx}{a}$.

Au reste, on sait que la congruence $bx \equiv m$ a une infinité de racines, mais toutes congrues suivant a, et il peut arriver que y acquière une valeur négative. Il est à peine nécessaire de dire que l'on peut aussi trouver y par la congruence $ay \equiv m \pmod{b}$, et x par l'équation $x = \frac{m-ay}{b}$.

Par exemple, étant proposée la fraction $\frac{58}{77}$, 4 sera valeur de l'expression $\frac{58}{11} \pmod{7}$; donc $\frac{58}{77}$ se décompose en $\frac{4}{7} + \frac{1}{11}$.

310. Si l'on propose une fraction $\frac{m}{n}$ dont le dénominateur n soit le produit de tant de facteurs a, b, c, d, etc. qu'on voudra, qui soient premiers entre eux, on pourra, par le n° précédent, la décomposer d'abord en deux fractions dont les dénominateurs soient a et bcd, etc., ensuite la dernière en deux dont les dénominateurs soient b et cd, etc., et ainsi de suite, desorte que la fraction proposée sera mise sous la forme

$$\frac{m}{n} = \frac{\alpha}{a} + \frac{\beta}{b} + \frac{\gamma}{c} + \frac{\delta}{d} + \text{etc.}$$

Il est évident que l'on pourra toujours prendre les numérateurs α, β, γ, δ, etc. positifs et plus petits que leurs dénominateurs respectifs, excepté le dernier, qui n'est plus arbitraire, lorsque les autres sont déterminés, et peut être négatif et plus grand que son dénominateur (si du moins nous ne supposons pas $m < n$). Alors, le plus souvent, il sera avantageux de mettre la dernière fraction sous la forme $\frac{\varepsilon}{e} + k$, de manière que ε soit positif et moindre que e, et que k soit un entier.

Exemple. La fraction $\frac{391}{924}$, dont le dénominateur $= 4.3.7.11$, se décompose de cette manière en $\frac{1}{4} + \frac{40}{231}$; $\frac{40}{231}$ en $\frac{2}{3} - \frac{38}{77}$; $-\frac{38}{77}$ en $\frac{1}{7} - \frac{7}{11}$; donc mettant $\frac{4}{11} - 1$ pour $-\frac{7}{11}$, il vient enfin

$$\frac{391}{924} = \frac{1}{4} + \frac{2}{3} + \frac{1}{7} + \frac{4}{11} - 1.$$

311. La fraction $\frac{m}{n}$ ne peut se mettre *que d'une seule manière*

sous la forme $\frac{\alpha}{a}+\frac{\beta}{b}+$ etc. $\mp k$, de manière que α, β, etc. soient positifs et moindres que a, b, etc., c'est-à-dire que si l'on supposait

$$\frac{m}{n}=\frac{\alpha}{a}+\frac{\beta}{b}+\frac{\gamma}{c}+\text{etc.}\mp k=\frac{\alpha'}{a}+\frac{\beta'}{b}+\frac{\gamma'}{c}+\text{etc.}\mp k',$$

on aurait nécessairement $\alpha=\alpha'$, $\beta=\beta'$, etc. $k=k'$, tant que α', β', γ', etc. seront positifs et plus petits que a, b, c, etc. En effet, en multipliant par $n=abcd$, etc., on a $m\equiv\alpha bcd$, etc., $\equiv\alpha' bcd$, etc. (mod. a), et comme bcd, etc. est premier avec a, il s'ensuit nécessairement $\alpha\equiv\alpha'$, et partant $\alpha=\alpha'$; de même $\beta=\beta'$, etc., et parconséquent $k=k'$. Or comme il est absolument arbitraire par quel dénominateur commence le calcul, il est évident que tous les numérateurs peuvent être cherchés comme α dans le n° précédent, par exemple, β par la congruence βacd, etc. $\equiv m$ (mod. b), γ par la congruence γabd, etc. $\equiv m$ (mod. c), etc. La somme de toutes les fractions ainsi calculées, sera égale à la proposée, ou la différence sera un nombre entier $=k$, ce qui nous donne un moyen de confirmer le calcul.

Ainsi dans l'exemple du n° précédent, les valeurs des expressions

$$\tfrac{391}{231}\text{ (mod. 4)},\ \tfrac{391}{308}\text{ (mod. 3)},\ \tfrac{391}{132}\text{ (mod. 7)},\ \tfrac{391}{84}\text{ (mod. 11)},$$

donnent les numérateurs 1, 2, 1, 4, qui répondent aux dénominateurs 4, 3, 7, 11, et l'on trouve que la somme de ces fractions surpasse d'une unité la fraction proposée.

312. *Définition.* Si l'on convertit une fraction ordinaire en fraction décimale, la suite de figures décimales (*) (en excluant la partie entière, s'il y en a), soit finie, soit infinie, s'appellera *mantisse* de la fraction, en prenant ici dans une acception plus générale une expression qui n'était jusqu'à présent usitée que pour les logarithmes. Ainsi, par exemple, la mantisse de la fraction $\frac{1}{8}$ est 125, la mantisse de la fraction $\frac{35}{16}$ est 1875, celle de la fraction $\frac{2}{37}$ est 054054..... à l'infini.

Il suit de là sur-le-champ, que deux fractions $\frac{l}{n}$, $\frac{m}{n}$ de même

(*) Pour abréger, nous ne nous arrêtons qu'au système décimal vulgaire, quoique nos recherches pussent s'étendre à un système quelconque.

dénominateur ont des mantisses égales ou différentes, suivant que les numérateurs l, m sont congrus ou incongrus suivant n. Une mantisse finie ne change pas lorsqu'on ajoute plusieurs zéros à sa droite. La mantisse de la fraction $\frac{10m}{n}$ s'obtient en retranchant la première figure de la mantisse de la fraction $\frac{m}{n}$, et généralement, la mantisse de la fraction $\frac{10^{\nu}m}{n}$ se trouve en retranchant les ν premières figures de la mantisse de la fraction $\frac{m}{n}$. La mantisse de la fraction $\frac{1}{n}$ commence par un chiffre significatif, si $n < 10$ ou $= 10$; mais si $n > 10$, et que le nombre de ses chiffres soit k, les $k-1$ premières figures de la mantisse seront des zéros, et la $k^{ième}$ un chiffre significatif. Il suit de là que si $\frac{l}{n}$ et $\frac{m}{n}$ ont des mantisses différentes, c'est-à-dire, si l et m sont incongrus suivant n, ces mantisses ne peuvent avoir les k premiers chiffres égaux, et qu'elles diffèrent au moins dans le $k^{ième}$.

313. Problème. *Etant donné le dénominateur d'une fraction* $\frac{\mathrm{m}}{\mathrm{n}}$, *et les* k *premières figures de sa mantisse, trouver le numérateur* m, *que nous supposons plus petit que* n.

Considérons ces k figures comme un nombre entier; multiplions-le par n et divisons le produit par 10^k, en en retranchant les k premières figures; si le quotient est entier, c'est-à-dire, si les chiffres retranchés sont des zéros, ce sera évidemment le numérateur cherché, et la mantisse donnée sera complète, sinon le numérateur cherché sera l'entier immédiatement plus grand, ou ce quotient augmenté de l'unité, lorsqu'on en aura retranché la partie décimale. La raison de cette règle se tire si facilement des observations que nous avons faites à la fin du n° précédent, qu'il n'y a pas besoin de plus grands développemens.

Exemple. Si l'on sait que 69 sont les deux premières figures de la mantisse de la fraction dont le dénominateur est 23, on a le produit $23.69 = 1587$; retranchant les deux derniers chiffres, et ajoutant l'unité, on trouve 16 pour le numérateur cherché.

314. Considérons d'abord les fractions dont les dénominateurs sont des nombres premiers ou des puissances de nombres premiers;

nous ferons voir ensuite comment on peut y ramener les autres. Nous commencerons par observer que la mantisse d'une telle fraction $\frac{a}{p^\mu}$, dans laquelle nous supposons que le numérateur a ne soit pas divisible par le nombre premier p, est toujours finie lorsque $p=2$, ou $=5$, et qu'elle est composée de μ chiffres. Dans le premier cas, cette mantisse, considérée comme un nombre entier, sera $5^\mu a$; dans le second, $2^\mu a$. Ces vérités sont si évidentes, qu'il est inutile de s'y arrêter.

Mais si p est un autre nombre premier, $10^r a$ ne sera jamais divisible par p^μ, quel que grand que l'on prenne r; d'où il suit que la mantisse de la fraction $F=\frac{a}{p^\mu}$ est nécessairement infinie. Supposons que 10e soit la plus petite puissance de 10 qui soit congrue à l'unité, suivant le module p^μ (V. Section III, où nous avons fait voir que e est égal à $(p-1)p^{\mu-1}$, ou à une partie aliquote de ce nombre), on voit facilement que $10^e a$ est le premier nombre de la suite $10a$, $100a$, $1000a$, etc. qui soit congru avec a, suivant le même module. Or comme, par le n° 312, les mantisses des fractions $\frac{10a}{p^\mu}$, $\frac{100a}{p^\mu}$, $\frac{1000a}{p^\mu}$, etc. $\frac{10^e.a}{p^\mu}$ résultent de celle de la fraction F en supprimant le premier chiffre, les deux, trois, etc. e premiers chiffres, il est évident que dans cette mantisse, après les e premiers chiffres, et non auparavant, les mêmes chiffres reparaîtront dans le même ordre. Ces e premiers chiffres qui, répétés à l'infini, forment la mantisse, peuvent être nommés *période* de cette mantisse ou de la fraction, et il est clair que la grandeur de la période, c'est-à-dire le nombre des chiffres qui la composent, qui est $=e$, est tout-à-fait indépendant du numérateur a, et que le dénominateur seul le détermine. Ainsi, par exemple, la période de la fraction $\frac{1}{11}$ est 09, celle de la fraction $\frac{3}{7}$ est 428571 (*).

(*) *Robertson* marque le commencement et la fin de la période, en plaçant un point sur le premier et le dernier chiffre (*Theory of circulating fractions*, *Philos. trans.*, 1764), mais nous ne l'avons pas jugé nécessaire.

315. Ainsi, dès que l'on connaît la période d'une fraction, on peut obtenir la mantisse avec autant de figures qu'on voudra; d'ailleurs il est clair que si l'on a $b \equiv 10^{\lambda} a \pmod{p^{\mu}}$, on obtient la période de la fraction $\frac{b}{p^{\mu}}$, si (en supposant, comme il est toujours permis, que $\lambda < e$) on écrit les λ premiers chiffres de la période de la fraction F après les $e-\lambda$ qui restent, et parconséquent lorsqu'on a la période de la fraction F, on a en même temps celles de toutes les fractions dont les numérateurs sont congrus aux nombres $10a$, $100a$, $1000a$, etc., suivant le module p^{μ}. Ainsi, par exemple, comme $6 \equiv 3.10^{2} \pmod{7}$, la période de la fraction $\frac{6}{7}$ se trouve au moyen de la période de la fraction $\frac{3}{7}$; elle est 857142.

Donc toutes les fois que, pour le module p^{μ}, le nombre 10 est une racine primitive (nos 57 et 89), on peut, de la période de la fraction $\frac{1}{p^{\mu}}$, déduire sur-le-champ la période de toute autre fraction $\frac{m}{p^{\mu}}$, m n'étant pas divisible par p, en retranchant à gauche pour écrire à droite, autant de chiffres qu'il y a d'unités dans l'indice du nombre m, 10 étant pris pour base. On voit par là pourquoi, dans la Table I, nous avons toujours pris 10 pour base, quand la chose était possible.

Mais quand 10 n'est pas racine primitive, on ne peut tirer de la période de la fraction $\frac{1}{p^{\mu}}$ que celles des fractions dont les dénominateurs sont congrus, suivant p^{μ}, à quelque puissance de 10. Soit 10e la plus petite puissance de 10 congrue à l'unité, suivant le module p^{μ}, faisons $(p-1)p^{\mu-1} = ef$, et prenons (n° 71) pour base une racine primitive r telle que f soit l'indice du nombre 10. Dans ce système, les numérateurs des fractions dont les périodes peuvent se tirer de la période de la fraction $\frac{1}{p^{\mu}}$, auront pour indices

$$f,\ 2f,\ 3f \ldots \text{etc.},\ (e-1)f.$$

De la même manière, on peut déduire de la période de la fraction $\frac{r}{p^\mu}$, celles des fractions dont les numérateurs répondent aux indices

$$f+1,\ 2f+1,\ 3f+1,\ \text{etc.}$$

De la période de la fraction dont le numérateur est r^2 (l'indice en est 2), on déduira celles des fractions dont les numérateurs ont pour indices

$$f+2,\ 2f+2,\ 3f+2,\ \text{etc.}$$

Et généralement, de la période de la fraction dont le numérateur est r^i, on déduira celles des fractions dont les numérateurs ont pour indices

$$f+i,\ 2f+i,\ 3f+i,\ \text{etc.}$$

On conclura facilement de là que si l'on connaît seulement les périodes des fractions qui ont pour numérateurs

$$1,\ r,\ r^2,\ r^3,\ldots.r^{f-1},$$

on peut tirer toutes les autres par la seule transposition, à l'aide de la règle suivante : Soit i l'indice du numérateur m de la fraction proposée $\frac{m}{p^\mu}$, dans le système où r est pris pour base, nous supposons $i<(p-1)p^{\mu-1}$; on fera, en divisant par f, $i=\alpha f+\beta$, de manière que α, β soient des entiers positifs, ou même $=0$, et qu'on ait $\beta<f$. Cela posé, la période de la fraction $\frac{m}{p^\mu}$ naîtra de celle de la fraction dont le numérateur est r^β (et partant 1, quand $\beta=0$) en plaçant les α premiers chiffres après les autres (et conservant parconséquent cette période elle-même, quand $\alpha=0$). Ce qui précède suffit pour faire voir pourquoi, en formant la Table I, nous avons suivi la règle exposée n° 72.

316. Nous avons construit, d'après ces principes, pour tous les dénominateurs de la forme p^μ, au-dessous de 1000, une Table des périodes nécessaires, que nous donnerons en entier, et même continuée plus loin à la première occasion qui se présentera. Nous

plaçons ici la Table III, pour en donner une idée; elle ne va que jusqu'à 100, et elle a à peine besoin d'explication.

Pour les dénominateurs à l'égard desquels 10 est racine primitive, elle donne les périodes des fractions dont le numérateur est 1, par exemple pour les nombres :

7, 17, 19, 23, 29, 47, 59, 61, 97;

pour les autres, les f périodes qui répondent aux numérateurs $1, r, r^2, \ldots r^{f-1}$, périodes qui sont distinguées par les nombres (0), (1), (2), etc.; on a toujours pris la même base que dans la Table I. A l'aide de cette Table et de ce qui a été enseigné dan le n° précédent, on peut trouver la période d'une fraction quelconque, pourvu que son dénominateur soit contenu dans cette Table, et que l'on ait calculé l'indice du numérateur au moyen de la Table I. Au reste, pour des dénominateurs aussi petits, on peut se passer de la Table I, en calculant par la division arithmétique autant de chiffres de la mantisse cherchée, qu'il est nécessaire, d'après le n° 313, pour la distinguer de toute autre du même dénominateur (pour la Table III, il n'en faut jamais plus de deux), et en parcourant les différentes périodes qui répondent au dénominateur donné, jusqu'à ce que nous soyons parvenus à ces chiffres initiaux, qui indiqueront surement le commencement de la période. Il faut cependant avertir que ces chiffres peuvent être séparés de manière que le premier, ou plusieurs, forment la fin de la période, et l'autre ou les autres la commencent.

Exemple. On demande la période de la fraction $\frac{12}{19}$. La Table I donne, pour la base 19, ind. $12 = 2$ ind. $2 +$ ind. $3 = 39 \equiv 3$ (mod. 18) (n° 57). Donc, comme dans ce cas il n'y a qu'une seule période qui répond au numérateur, il faut transporter à la fin les trois premiers chiffres, ce qui donne 631578947368421052. Les deux premiers chiffres 63 auraient fait trouver aussi facilement le commencement de la période.

Si l'on demande la période de la fraction $\frac{45}{53}$, on trouve pour le module 53, ind. $45 = 2$ ind. $3 +$ ind. $5 = 49$; le nombre des périodes est ici, $4 = f$, et l'on a $49 = 12f + 1$; donc il faut à la période désignée par (1) transposer les douze premiers chiffres,

et l'on trouve 849056603773 5 pour la période cherchée. Les chiffres initiaux 84 sont dans ce cas séparés dans la Table.

Nous observerons encore, qu'à l'aide de la Table III on peut trouver un nombre qui, pour un module donné, contenu dans cette Table, dans la colonne des dénominateurs, réponde à un indice donné, ainsi que nous l'avons promis n° 59: il suit en effet de ce que nous avons dit plus haut, que l'on peut trouver la période d'une fraction au numérateur de laquelle réponde un indice donné, quoique ce numérateur soit inconnu; il suffit de prendre de cette période autant de chiffres initiaux qu'il y a de chiffres au dénominateur, et par le n° 313, on trouvera, à l'aide de ces chiffres, le numérateur, ou le nombre cherché qui répond à l'indice donné.

317. On peut par ce qui précède trouver sans calcul la mantisse d'une fraction quelconque, dont le dénominateur est un nombre premier, ou une puissance d'un nombre premier compris entre les limites de la Table. Mais, à l'aide des recherches que nous avons faites au commencement de cette Section, l'usage de cette Table devient bien plus étendu, et elle renferme même les fractions dont les dénominateurs sont des produits de nombres premiers ou de puissances de nombres premiers. En effet, une pareille fraction peut se décomposer en d'autres dont les dénominateurs soient ces facteurs, et ces dernières peuvent être converties en fractions décimales, avec tel degré d'approximation qu'on voudra; ainsi il ne reste qu'à les réunir par l'addition. Il est à peine nécessaire d'observer que le dernier chiffre de la somme pourra se trouver un peu plus petit qu'il ne devrait être; mais il est évident que l'erreur ne peut monter à autant d'unités qu'il y a de fractions à ajouter; ainsi il conviendra de calculer ces dernières avec quelques figures de plus qu'on n'en veut avoir à la fraction proposée.

Considérons, comme exemple, la fraction

$$F = \frac{6099380351}{12718087120}\ (*),$$

(*) Cette fraction est une de celles qui approchent le plus de la racine quarrée de 23, et l'excès est moindre que sept unités du vingtième ordre décimal.

dont le dénominateur est le produit des nombres 16, 9, 5, 49, 13, 47, 59. On trouve par ce qui précède

$$F = 1 + \frac{11}{16} + \frac{4}{9} + \frac{4}{5} + \frac{22}{49} + \frac{5}{13} + \frac{7}{47} + \frac{52}{59};$$

ces fractions particulières réduites en décimales, donnent

1	$= 1$		
$\frac{11}{16}$	$= 0,6875$		
$\frac{4}{5}$	$= 0,8$		
$\frac{4}{9}$	$= 0,4444444444$	4444444444	44
$\frac{22}{49}$	$= 0,4489795918$	3673469387	75
$\frac{5}{13}$	$= 0,3846153846$	1538461538	46
$\frac{7}{47}$	$= 0,1489361702$	1276595744	68
$\frac{52}{59}$	$= 0,8813559322$	0338983050	84
F	$= 4,7958315233$	1271954166	17.

L'erreur en moins de cette somme, comparée, à la valeur exacte, est moindre que cinq unités du vingt-deuxième ordre, donc les vingt premiers chiffres sont exacts. En poussant le calcul à un plus grand nombre de décimales, au lieu des deux derniers chiffres 17, on trouve 1893936. Au reste, chacun sentira bien, même sans que nous en avertissions, que cette méthode de réduire les fractions ordinaires en fractions décimales, est principalement applicable au cas où l'on veut avoir un grand nombre de chiffres; car, s'il suffit d'un petit nombre, la division ou les logarithmes peuvent être souvent employés avec autant d'avantage.

318. Comme nous avons ramené les fractions dont le dénominateur est composé de plusieurs nombres premiers différens, au cas où le dénominateur est un nombre premier, ou une puissance d'un nombre premier, il ne nous reste qu'à ajouter quelque chose sur la mantisse de ces fractions. Si le dénominateur ne renferme ni le facteur 2 ni le facteur 5, la mantisse sera encore composée de périodes, parceque, pour ce cas, on parviendra aussi à un terme de la suite 10, 100, 1000, etc. qui soit congru à l'unité, suivant le dénominateur, et l'exposant de ce terme, que l'on peut déterminer par le n° 92, indiquera la grandeur de la période, qui est indépendante du numérateur, tant que la fraction est irréductible.

Mais si le dénominateur est de la forme $2^\alpha 5^\beta N$, N étant un nombre premier avec 10, α et β des nombres qui ne peuvent être zéro à-la-fois, la mantisse deviendra périodique après les α ou β premiers chiffres, suivant que α ou β est le plus grand; ces périodes seront composées d'autant de chiffres que celles des fractions dont le dénominateur est N. Ceci se déduit facilement de ce que la fraction proposée peut se décomposer en deux autres dont les dénominateurs soient $2^\alpha 5^\beta$ et N, et dont la première sera interrompue après les α ou β premiers chiffres.

Au reste, nous pourrions ajouter encore beaucoup d'autres observations sur ce sujet, surtout à l'égard des artifices au moyen desquels on peut construire avec une grande facilité la Table III; mais, forcés d'abréger, nous les omettons d'autant plus volontiers qu'une grande partie a été publiée tant par *Robertson* que par *Bernoulli* (*Nouv. Mém. de l'Acad. de Berlin*, 1771).

319. Nous avons traité (n° 146) de la possibilité de la congruence $x^2 \equiv A \pmod{m}$, qui revient à l'équation indéterminée $x^2 = A + my$, de manière à ce qu'il semble qu'on ait rien à desirer; mais pour la recherche de l'inconnue elle-même, nous avons déjà observé (n° 151) que les méthodes indirectes étaient de beaucoup préférables aux méthodes directes. Si m est un nombre premier, cas auquel les autres se ramènent facilement, la Table des indices I, combinée avec la Table III, suivant l'observation du n° 316, peut être employée à cette fin, comme nous l'avons fait voir plus généralement (n° 60); mais cette méthode ne s'étendrait qu'aux nombres compris dans les Tables; c'est pourquoi nous espérons que la méthode suivante, par sa généralité et sa briéveté, ne déplaira pas aux amateurs de l'Arithmétique.

Observons avant tout qu'il suffit de connaître les valeurs de x qui sont positives et non plus grandes que $\frac{m}{2}$, puisque toute autre valeur sera congrue à l'une de celles-là, prise positivement ou négativement. Or, pour une telle valeur de x, celle de y est nécessairement contenue entre les limites $-\frac{A}{m}$ et $\frac{1}{4}m - \frac{A}{m}$. Ainsi une méthode qui s'offre d'elle-même, consisterait à calculer la va-

leur de $A+my \ldots V$, pour toutes les valeurs de y comprises entre ces limites, et dont nous désignerons l'ensemble par ω, en ne retenant que celles qui rendraient V un quarré. Quand m est petit, le nombre des essais est si peu considérable qu'il n'est presque pas nécessaire de chercher à l'abréger; mais quand m est grand, on peut diminuer le travail autant qu'on voudra, par la *méthode d'exclusion* suivante.

320. Soit E un nombre entier arbitraire et plus grand que 2; soient aussi a, b, c, etc. tous ses résidus quadratiques différens, c'est-à-dire, incongrus suivant E; enfin α, β, γ, etc. les racines des congruences

$$A+my \equiv a,\ A+my \equiv b,\ A+my \equiv c,\ \text{etc. (mod. } E),$$

que l'on peut prendre toutes positives et plus petites que E; si l'on donne à y une valeur congrue, suivant le module E, à l'un des nombres α, β, γ, etc., la valeur de $N = A+my$ qui en résultera sera congrue à l'un des nombres a, b, c, etc., et sera parconséquent non-résidu de E; partant elle ne pourra être un quarré. Par là, on peut donc rejeter sur-le-champ, de ω, tous les nombres inutiles qui sont contenus sous les formes

$$Et+\alpha,\quad Et+\beta,\quad Et+\gamma,\ \text{etc.},$$

et il suffira d'essayer les autres, dont nous représenterons l'ensemble par ω'. Dans cette opération, nous pouvons donner au nombre E le nom d'*excluant*.

En prenant pour excluant un autre nombre convenable E', on trouvera de la même manière autant de nombres α', β', γ', etc. qu'il y a de non-résidus différens, et auxquels y ne peut être congru suivant le module E'. On peut donc encore rejeter de ω' tous les nombres compris sous les formes

$$E't+\alpha',\quad E't+\beta',\quad E't+\gamma',\ \text{etc.}$$

On peut continuer de cette manière les exclusions, jusqu'à ce que le nombre des valeurs ω soit tellement diminué, qu'il ne paraisse pas plus difficile d'essayer directement celles qui restent, que d'entreprendre de nouvelles exclusions.

Exemple. Soit proposée l'équation $x^2 = 22+97y$; les limites des valeurs de y sont $-\frac{22}{97}$ et $24+\frac{1}{4}-\frac{22}{97}$; donc, comme la valeur

zéro est évidemment inutile, ω comprendra les nombres 1, 2, 3...24. Pour $E=3$, il n'y a qu'un non-résidu $a=2$, qui donne $\alpha=1$; il faut donc exclure de ω les nombres de la forme $3t+1$, et il en reste 16; de même pour $E=4$, on a $a=2$, $b=3$, d'où $\alpha=0$, $\beta=1$; on doit donc rejeter les nombres de la forme $4t$ et $4t+1$, ceux qui restent sont au nombre de huit: 2, 3, 6, 11, 14, 15, 18, 23. Ensuite pour $E=5$, on doit rejeter tous les nombres $5t$ et $5t+3$, et il reste 2, 6, 11, 14. L'excluant 6 ferait rejeter les nombres de la forme $6t+1$, $6t+4$, qui ont déjà disparu, comme étant de la forme $3t+1$. L'excluant 7 fait rejeter les nombres des formes $7t+2$, $7t+3$, $7t+5$, et laisse 6, 11, 14. En les substituant pour y, ces nombres donnent $V=604$, 1089, 1380, valeurs dont la seconde seule est un quarré. Ainsi $x=\pm 33$.

321. Puisque l'opération entreprise avec l'excluant E rejette des valeurs de V correspondantes aux valeurs de y comprises dans ω, toutes celles qui sont non-résidus quadratiques de E, tandis qu'elle n'atteint pas les résidus, on voit facilement que l'usage des excluans E et $2E$ ne présente aucune différence, lorsque E est un nombre impair, car dans ce cas E et $2E$ ont les mêmes résidus et les mêmes non-résidus. Il suit de là que si l'on emploie successivement les nombres 3, 4, 5, etc., les nombres impairement pairs, tels que 6, 10, 14, etc. doivent être négligés comme superflus. Il est encore évident que la double opération entreprise avec les excluans E et E' rejette les valeurs de N qui sont non-résidus des deux excluans ou de l'un d'eux seulement, desorte que celles qui sont résidus de l'un et de l'autre restent seules. Or comme dans le cas où E et E' sont premiers entre eux, tous les nombres rejetés sont non-résidus de EE', et tous les nombres conservés en sont résidus; il est clair que l'usage de l'excluant EE' est le même que celui des deux excluans E et E', et que parconséquent il est superflu. On peut donc passer tous les excluans qui peuvent se décomposer en deux facteurs premiers entre eux, et parconséquent n'employer que ceux qui sont des nombres premiers, non-diviseurs de m, ou des puissances de nombres premiers. Enfin, après avoir employé l'excluant p^{μ}, p étant un nombre premier, l'emploi de l'excluant p ou p^{ν}, ν étant $<\mu$, devien

vient superflu; car p^{μ} ne conservant des valeurs de V que celles qui sont ses propres résidus, on est sûr, à plus forte raison, qu'il ne restera plus de non-résidus de p, ni d'aucune autre puissance moindre que p^{ν}. Mais si p ou p^{ν} a été employé avant p^{μ}, ce dernier ne peut rejeter que les valeurs de V qui seraient résidus de p^{ν} et non-résidus de p^{α}; donc il suffirait de prendre pour a, b, c, etc. ces non-résidus de p^{μ}.

322. Le calcul des nombres α, β, γ, etc. qui répondent à un excluant quelconque donné E, s'abrège beaucoup par les observations suivantes. Soient M, N, P, etc. les racines des congruences $my \equiv a$, $my \equiv b$, $my \equiv c$, etc. (mod. E), et k la racine de la congruence $my \equiv -A$, on aura $\alpha = M+k$, $\beta = N+k$, $\gamma = P+k$, etc. S'il fallait effectivement trouver M, N, P, etc. par la résolution de ces congruences, ce procédé ne serait pas plus abrégé que celui que nous avons indiqué plus haut; mais cela n'est point nécessaire. En effet, si d'abord E est un nombre premier, et que m soit résidu quadratique de E, il est clair, par le n° 98, que M, N, P, etc., qui sont les valeurs des expressions $\frac{a}{m}, \frac{b}{m}, \frac{c}{m}$, etc. (mod. E), sont les non-résidus différens de E, et parconséquent coïncident avec α, β, γ, etc., abstraction faite de l'ordre, qui n'est ici d'aucune importance; mais si, dans la même hypothèse, m est non-résidu de E, les nombres M, N, P, etc. coïncideront avec les résidus quadratiques de E, zéro excepté.

Si E est le quarré d'un nombre premier impair $= p^2$, et que p ait déjà été employé comme excluant, il suffit, par le n° précédent, de prendre pour a, b, c, etc. les non-résidus de p^2 qui sont résidus de p, c'est-à-dire, les nombres $p, 2p, 3p, \ldots\ldots (p-1)p$, (ou tous les nombres au-dessous de p^2 qui sont divisibles par p, zéro excepté); on voit par-là qu'on doit trouver pour M, N, P, etc. absolument les mêmes nombres, disposés seulement d'une autre manière. De même, si après l'emploi des excluans p et p^2, on fait $E = p^3$, il suffira de prendre pour a, b, c, etc. les produits de chaque non-résidu de p par p^2, et de là on tirera pour M, N, P, etc., ou les mêmes nombres, ou les produits de p^2

par chacun des résidus de p, zéro excepté, suivant que m est résidu ou non-résidu de p. Généralement, si l'on prend $E=p^{\mu}$, toutes les puissances inférieures de p ayant été employées, on trouvera pour M, N, P, etc. les produits de $p^{\mu-1}$, par tous les nombres moindres que p, zéro toujours excepté, quand μ est pair, ou par tous les non-résidus de p moindres que p, quand μ est impair et mRp, ou par tous les résidus, quand mNp.

Si $E=4$ et partant $a=2$, $b=3$, on a pour M et N, 2 et 3 ou 2 et 1, suivant que $m\equiv 1$ ou $\equiv 3$ (mod. 4). Si après avoir employé 4, on fait $E=8$, on a $a=5$; donc M est 5,7, 1,3, suivant que $m\equiv 1$, 3, 5, 7 (mod. 8). Généralement, si $E=2^{\mu}$, les puissances inférieures étant déjà employées, on doit poser $a=2^{\mu-1}$, $b=3.2^{\mu-2}$, quand μ est pair, d'où il résulte $M=2^{\mu-1}$, $N=3.2^{\mu-2}$ ou $=2^{\mu-2}$, suivant que $m\equiv 1$ ou $\equiv 3$; mais quand μ est impair, on doit poser $a=5.2^{\mu-3}$, d'où il vient M égal au produit de $2^{\mu-3}$ par 5, 7, 1 ou 3, suivant que $m\equiv 1$, 3, 5 ou 7 (mod. 8).

Au reste, les gens instruits trouveront facilement la manière de rejeter *méeaniquement* les valeurs inutiles de y, après qu'on aura calculé les valeurs de α, β, γ, etc. pour tant d'excluans qu'il paraîtra nécessaire; mais nous ne pouvons nous y arrêter, ni aux autres artifices par lesquels on peut abréger le travail.

323. Toutes les représentations d'un nombre donné A par la forme binaire mx^2+ny^2, où les solutions de l'équation indéterminée $mx^2+ny^2=A$, peuvent être trouvées par la méthode exposée Section V, qui semble ne rien laisser à desirer du côté de la briéveté, si l'on a les différentes valeurs de l'expression $\sqrt{-mn}$, suivant le module A et suivant A divisé par ses différens facteurs quarrés. Mais nous allons donner ici, pour le cas où mn est positif, une solution beaucoup plus abrégée que la solution directe, lorsqu'il faut pour cette dernière calculer les valeurs dont nous venons de parler. Nous supposerons que les nombres m, n, A soient positifs et premiers entre eux, parceque

les autres cas se ramènent facilement à celui-là. Il suffit encore évidemment de trouver les valeurs positives de x, y, puisque les autres s'en déduisent par un simple changement de signe.

Il est clair que x doit être tel que $\frac{A-mx^2}{n}$, que nous désignerons par V, soit positif, entier et quarré. La première condition exige que x ne soit pas plus grand que $\sqrt{\frac{A}{m}}$; la seconde a lieu par elle-même quand $n=1$, autrement elle exige que la valeur de l'expression $\frac{A}{m}$ (mod. n) soit résidu quadratique de n, et qu'en désignant les diverses valeurs de l'expression $\sqrt{\frac{A}{m}}$ (mod. n) par $\pm r$, $\pm r'$, etc., x soit compris sous une des formes:

$$nt+r,\ nt-r,\ nt+r',\ nt-r',\ \text{etc.}$$

Ainsi, il serait très-simple de substituer à la place de x tous les nombres de ces formes et moindres que $\sqrt{\frac{A}{m}}$, nombres dont nous représenterons l'ensemble par ω, et de ne retenir que ceux qui rendraient V un quarré. Nous allons donner dans le n° suivant le moyen d'abréger le nombre de ces essais autant que l'on voudra.

324. La méthode d'exclusion à l'aide de laquelle nous y parviendrons, consiste, comme la précédente, à prendre à volonté plusieurs nombres, que nous appellerons encore *excluans*, à chercher quelles sont les valeurs de x pour lesquelles V devient non-résidu quadratique de ces excluans, et à rejeter de ω ces valeurs de x. On verra absolument de la même manière qu'au n° 321, que l'on ne doit employer pour excluans que des nombres premiers ou des puissances de nombres premiers, et que, pour un excluant du dernier genre, il n'y a plus à rejeter des valeurs de V que les non-résidus qui sont résidus de toutes les puissances inférieures du même nombre premier, si toutefois on a déjà employé ces différentes puissances.

Soit donc l'excluant $E=p^{\mu}$ (μ pouvant être $=1$), où p est un nombre premier qui ne divise pas m, et supposons que p^{ν} soit

la plus haute puissance de p qui puisse diviser n (*). Soient a, b, c, etc. les non-résidus quadratiques de E (tous, quand $\mu = 1$, mais ceux seulement qui sont résidus des puissances inférieures, quand $\mu > 1$). On cherchera les racines des congruences

$$mz \equiv A - na,\ mz \equiv A - nb,\ mz \equiv A - nc, \text{ etc. } (\text{mod. } Ep^\nu = p^{\mu+\nu}),$$

que nous désignerons par α, β, γ, etc.; et l'on voit facilement que si, pour une valeur de x on a $x^2 \equiv \alpha$ (mod. Ep^ν), la valeur correspondante de V sera $\equiv a$ (mod. E), c'est-à-dire, non-résidu de E, et de même pour β, γ, etc. On voit aussi facilement, que si une valeur de x rend $V \equiv a$ (mod. E), la même valeur rendra $x^2 \equiv \alpha$ (mod. Ep^ν), et que parconséquent toutes les valeurs de x pour lesquelles x^2 n'est congru à aucun des nombres α, β, γ, etc., suivant le module Ep^ν, produisent des valeurs de V qui ne sont congrues à aucun des nombres a, b, c, etc., suivant le module E. Cela posé, on choisira parmi les nombres α, β, γ, etc. tous ceux qui sont résidus quadratiques de Ep^ν, et les nommant g, g', g'', etc. on calculera les valeurs des expressions $\sqrt{g}$, $\sqrt{g'}$, $\sqrt{g''}$, etc. (mod. Ep^ν), que nous désignerons par h, h', h'', etc. Il est évident que l'on peut rejeter de ω toutes les formes

$$Ep^\nu t \pm h, \quad Ep^\nu t \pm h', \quad Ep^\nu t \pm h'', \text{ etc.},$$

et qu'aucune des valeurs de x qui resteront ne peuvent répondre à une valeur de V qui soit de la forme

$$Eu + a, \quad Eu + b, \quad Eu + c, \text{ etc.}$$

Au reste il est manifeste qu'aucune valeur de x ne peut donner de telles valeurs de V, quand aucun des nombres α, β, γ, etc. n'est résidu quadratique de Ep^ν, et que, dans ce cas, le nombre E ne peut pas être employé comme excluant.

On peut employer ainsi autant d'excluans qu'on voudra, et parconséquent diminuer à volonté le nombre des valeurs de x à essayer.

(*) Pour abréger, nous traitons à-la-fois le cas où n est divisible par p, et celui où il ne l'est pas; dans le second, on doit faire $\nu = 0$.

Examinons maintenant si l'on ne pourrait pas employer comme excluans des nombres premiers diviseurs de m, et des puissances de ces nombres. Soit B la valeur de l'expression $\frac{A}{n}$ (mod. m), il est clair que l'on a toujours $V \equiv B$ (mod. m), quelque valeur que l'on prenne pour x, et que parconséquent pour que l'équation proposée soit possible, il est nécessaire que B soit résidu quadratique de m. Ainsi, p désignant un diviseur quelconque premier impair de m, qui, par hypothèse, ne doit diviser ni n, ni A, ni parconséquent B; V sera résidu de p pour une valeur quelconque de x, et partant, p ni ses puissances ne peuvent être pris pour excluans.

Par une raison semblable, quand m est divisible par 8, il est nécessaire que l'on ait $B \equiv 1$ (mod. 8), pour que l'équation proposée soit possible; donc pour une valeur quelconque de x, on aura $V \equiv 1$ (mod. 8), et partant, les puissances de 2 ne peuvent servir d'excluans.

Quand m est divisible par 4 et non par 8, on doit par la même raison avoir $B \equiv 1$ (mod. 4), et parconséquent la valeur de l'expression $\frac{A}{n}$ (mod. 8) est 1 ou 5; désignons-la par C. Il est facile de voir que, pour une valeur paire de x on a $V \equiv C$, et $V \equiv C+4$ (mod. 8) pour une valeur impaire; d'où il suit que l'on doit rejeter les valeurs paires quand $C = 5$, et les valeurs impaires quand $C = 1$.

Enfin, quand m est divisible par 2 et non par 4, soit encore C la valeur de l'expression $\frac{A}{n}$ (mod. 8), qui sera 1, 3, 5 ou 7, et D la valeur de l'expression $\frac{\frac{1}{2}m}{n}$ (mod. 4), qui sera 1 ou 3. Comme la valeur de V est toujours $\equiv C - 2Dx^2$ (mod. 8), et partant $\equiv C$, si x est pair, et $\equiv C - 2D$, si x est impair; il est clair qu'on doit rejeter toutes les valeurs impaires de x, lorsque $C = 1$; toutes les valeurs paires, quand $C = 3$ et $D = 1$, et quand $C = 7$ et $D = 3$, et que les valeurs conservées donnent toutes $V \equiv 1$ (mod. 8), c'est-à-dire, V résidu de toute puissance de 2. Quant aux autres cas, savoir, lorsque $C = 5$ ou 3 et $D = 3$, lorsque

$C=7$ et $D=1$, on trouve $V\equiv 3$, 5 ou 7 (mod. 8), soit que x soit pair, soit qu'il soit impair, d'où il résulte évidemment que, dans ces cas, l'équation proposée n'admet aucune solution.

Au reste, comme après les changemens convenables, on peut chercher la valeur de y de la même manière que nous avons cherché celle de x, on peut appliquer de deux manières la méthode d'exclusion au problème proposé (excepté dans le cas où $m=n=1$); on doit préférer celle pour laquelle ω contient un moindre nombre de termes, circonstance dont on peut facilement juger *à priori*.

Enfin, il est à peine nécessaire d'observer, que si après quelques exclusions, tous les nombres de ω disparaissent, on en doit conclure que l'équation proposée est impossible.

325. *Exemple.* Soit l'équation

$$3x^2+455y^2=10857362,$$

que nous résoudrons de deux manières, en cherchant d'abord les valeurs de x, et ensuite celles de y.

1°. La limite des valeurs de x est, dans ce cas, $\sqrt{(3619120+\frac{1}{3})}$, qui tombe entre 1902 et 1903 : la valeur de l'expression $\frac{A}{3}$ (mod. 455) est 354, et les valeurs de l'expression $\sqrt{354}$ (mod. 455) sont

$$\pm 82,\quad \pm 152,\quad \pm 173,\quad \pm 212;$$

d'où il résulte que ω contient les trente-trois nombres suivans :

82, 152, 173, 212, 243, 282, 303, 373, 537, 607, 628, 667, 698, 737, 758, 828, 992, 1062, 1083, 1122, 1153, 1192, 1213, 1283, 1447, 1517, 1538, 1577, 1608, 1647, 1668, 1738, 1902.

Le nombre 3 ne peut être employé ici comme excluant, parcequ'il divise m.

Pour l'excluant 4, on a $a=2$, $b=3$, d'où $\alpha=0$, $\beta=3$, $g=0$; les valeurs de $\sqrt{g}$ (mod. 4) sont 0 et 2; il suit de là que tous les nombres des formes $4t$ et $4t+2$, c'est-à-dire, tous les nombres pairs, doivent être rejetés. Désignons par ω' les seize qui restent.

Pour $E=5$, les racines des congruences $mz\equiv A-2n$,

$mz \equiv A - 3n$ (mod. 25) sont 9 et 24, qui sont toutes deux résidus de 25; les valeurs des expressions $\sqrt{g}$ et $\sqrt{24}$ (mod. 25) sont ± 3 et ± 7; ainsi rejetant les nombres des formes $25t \pm 3$, $25t \pm 7$, ceux qui restent sont au nombre de dix:

$$173, 373, 537, 667, 737, 1083, 1213, 1283, 1517, 1577 \ldots\ldots (\omega'').$$

Pour $E = 7$, les racines des congruences

$$mz \equiv A - 3n, \quad mz \equiv A - 5n, \quad mz \equiv A - 6n \text{ (mod. } 49)$$

sont 32, 39, 18, qui sont toutes résidus de 49; les valeurs des expressions $\sqrt{32}$, $\sqrt{39}$, $\sqrt{18}$ (mod. 49) sont ± 9, ± 23, ± 19; en rejetant de ω'' les nombres de la forme

$$49t \pm 9, \quad 49t \pm 19, \quad 49t \pm 23,$$

il reste les cinq suivans:

$$537, 737, 1083, 1213, 1517 \ldots\ldots\ldots\ldots\ldots (\omega'').$$

Pour $E = 8$, on a $a = 5$, d'où $\alpha = 5$ qui est non-résidu de 8; ainsi l'excluant 8 ne peut être employé. Le nombre 9 doit être passé, par la même raison que le nombre 3.

Pour $E = 11$, les nombres a, b, etc. sont 2, 6, 7, 8, 10, et $\nu = 0$; donc les nombres α, β, etc. sont 8, 10, 5, 0, 1, parmi lesquels 0, 1 et 5 sont seuls résidus de 11; de là on conclut que l'on doit rejeter de ω'' les nombres de la forme

$$11t, \quad 11t \pm 1, \quad 11t \pm 4.$$

Il reste 537, 1083, 1213; en essayant ces nombres, ils donnent pour V les valeurs

$$21961, \quad 16129, \quad 14161,$$

dont le second et le troisième seuls sont des quarrés. Donc l'équation proposée admet deux solutions par des valeurs positives de x, y.

$$x = 1083, \quad y = 127; \quad x = 1213, \quad y = 119.$$

2°. Si l'on veut chercher par exclusion l'autre inconnue de cette équation, on la mettra sous la forme

$$455x^2 + 3y^2 = 10857362,$$

en échangeant x et y, afin de conserver la notation des n°s 323, 324.

La limite des valeurs de x tombe ici entre 154 et 155; la valeur de l'expression $\frac{A}{m}$ (mod. n) est 1, et les valeurs de $\sqrt{1}$ (mod. 3) sont 1 et -1; donc ω contient tous les nombres des formes $3t+1$ et $3t-1$, c'est-à-dire tous les nombres non-divisibles par 3, jusqu'à 154 exclusivement; il y en a cent trois. En appliquant les règles données précédemment, on trouve que

pour les excluans	on doit rejeter les nombres de la forme
3	$9t \pm 4$
4	$4t$, $4t+2$, c'est-à-dire les nombres pairs,
9	$27t \pm 1$, $27t \pm 10$
11	$11t$, $11t \pm 1$, $11t \pm 3$
17	$17t \pm 3$, $17t \pm 4$, $17t \pm 5$, $17t \pm 7$
19	$19t \pm 2$, $19t \pm 3$, $19t \pm 8$, $19t \pm 9$
23	$23t$, $23t \pm 5$, $23t \pm 7$, $23t \pm 9$, $23t \pm 10$.

Après avoir effacé ces différens nombres, il reste 119, 127, 137, dont les deux premiers seuls rendent V un quarré, et donnent les mêmes solutions que la première méthode.

326. La méthode précédente est déjà si expéditive en elle-même, qu'elle laisse à peine quelque chose à desirer; cependant elle peut encore être beaucoup abrégée par un grand nombre d'artifices, sur lesquels nous ne pouvons nous arrêter que légérement. Ainsi nous réduirons nos recherches au cas où l'excluant est un nombre premier impair qui ne divise pas A, ou une puissance d'un tel nombre, d'autant plus que les autres cas peuvent se ramener à celui-ci, ou être traités d'une manière analogue.

Supposons d'abord que l'excluant $E=p$ soit un nombre premier qui ne divise ni m, ni n, et représentons par k, M, N, P, etc. les valeurs des expressions

$$\frac{A}{m}, \quad -\frac{na}{m}, \quad -\frac{nb}{m}, \quad -\frac{nc}{m}, \text{ etc. (mod. } p);$$

respectivement: les nombres α, β, γ, etc. se trouveront par les congruences

$$\alpha \equiv k+M, \quad \beta \equiv k+N, \quad \gamma \equiv k+P, \text{ (mod. } p).$$

Or

Or les nombres M, N, P, etc. peuvent être déterminés par un artifice absolument semblable à celui dont nous nous sommes servis au n° 322, sans résoudre les congruences, et ils coïncideront, soit avec tous les non-résidus, soit avec les résidus de p (zéro excepté), suivant que la valeur de l'expression $-\frac{m}{n}$(mod.p), ou, ce qui revient au même, suivant que le nombre $-mn$ est résidu ou non-résidu de p. Ainsi, dans l'exemple 2 du n° précédent, pour $E=17$, on a $k=7$; $-mn=-1365\equiv 12$ est non-résidu de 17; donc les nombres M, N, etc. sont 1, 2, 4, 8, 9, 13, 15, 16, et partant, les nombres α, β, etc. sont 8, 9, 11, 15, 16, 3, 5, 6. Parmi ces derniers, 8, 9, 15 et 16 sont résidus, d'où l'on tire $\pm h$, h', etc. $=\pm 5$, 3, 7, 4.

Ceux qui auront fréquemment occasion de résoudre ce problème, gagneront beaucoup à calculer pour plusieurs nombres premiers p, les valeurs de h, h', etc. correspondantes aux différentes valeurs de k (1, 2, 3....$p-1$), dans la double supposition où $-mn$ est résidu, et où il est non-résidu de p. Au reste, nous observerons encore qu'il y a toujours $\frac{1}{2}(p-1)$ nombres h, $-h$, h', etc. quand k et $-mn$ sont tous deux résidus, ou tous deux non-résidus de p; $\frac{1}{2}(p-3)$, quand le premier est résidu et le second non-résidu; $\frac{1}{2}(p+1)$, quand le premier est non-résidu et le second résidu. Mais, pour éviter la prolixité, nous supprimons la démonstration de ce théorème.

Quant à ce qui regarde les cas où E est un nombre premier qui divise n, ou une puissance d'un nombre premier impair qui divise ou ne divise pas n, nous allons voir qu'ils peuvent être employés d'une manière encore plus expéditive. Nous traiterons tous ces cas ensemble, et conservant la notation du n° 324, nous ferons $n=n'p^{\nu}$, desorte que n' ne soit plus divisible par p. Les nombres a, b, c, etc. seront les produits du nombre $p^{\mu-1}$ par tous les nombres moindres que p, zéro excepté, et par tous les non-résidus de p plus petits que p, suivant que μ est pair ou impair; exprimons les indéfiniment par $up^{\mu-1}$. Soit k une valeur de l'expression $\frac{A}{m}$ (mod. $p^{\mu+\nu}$), il ne sera pas divisible par p,

puisque A ne l'est pas; en outre il est clair que α, β, γ, etc. sont congrus à k suivant le module p, et que partant p^μ n'exclut aucun des nombres ω, si kNp; mais si kRp et partant $kRp^{\mu+\nu}$, soit α la valeur de l'expression $\sqrt{k}\,(\text{mod. } p^{\mu+\nu})$, qui ne sera pas divisible par p, et e la valeur de l'expression $-\frac{n'}{2mr}\,(\text{mod. } p)$ on; aura $\alpha \equiv r^2 + 2erap^\nu\,(\text{mod. } p^{\mu+\nu})$, d'où l'on conclut facilement que α est résidu de $p^{\mu+\nu}$, et que les valeurs de l'expression $\sqrt{\alpha}\,(\text{mod. } p^{\mu+\nu})$ sont $\pm(r+eap^\nu)$; donc tous les nombres h, h', h'', etc. seront exprimés par la formule $r+eup^{\mu+\nu-1}$ (*).

Il est facile de conclure de là que les nombres h, h', h'', etc. se composent de r ajouté aux produits du nombre $p^{\mu+\nu-1}$ par tous les nombres au-dessous de p, zéro excepté, quand μ est pair; ou par tous les non-résidus de p, quand μ est impair et que eRp, ou, ce qui est la même chose, que $-2mrn'Rp$; ou par tous les résidus de p, quand μ est impair, et que $-2mrn'Np$.

Au reste, à mesure que l'on aura trouvé les nombres h, h', h'', etc. pour chacun des excluans que l'on voudra employer, on pourra exécuter l'exclusion par des opérations mécaniques, qu'on découvrira facilement de soi-même, avec un peu d'habitude, si on le trouve avantageux.

(*) On a

$mk \equiv A$, $m\alpha \equiv A - na$, $r^2 \equiv k\,(\text{mod. } p^{\mu+\nu})$ et d'ailleurs $na \equiv n'up^{\mu+\nu-1}$;

on en déduit sur-le-champ, par les deux premières congruences, $mk - m\alpha \equiv na$; multipliant la troisième par m, qui n'est pas divisible par p, on obtient $mr^2 - m\alpha \equiv na\,(\text{mod. } p^{\mu+\nu})$; or en prenant un nombre e tel qu'on ait $2mer \equiv -n'\,(\text{mod. } p)$, il en résulte $na \equiv -2merup^{\mu+\nu-1}\,(\text{mod. } p^{\mu+\nu})$, et partant on tire facilement de là et de la congruence précédente, après avoir divisé par m, $\alpha \equiv r^2 + 2er\mu p^{\mu+\nu-1}\,(\text{mod. } p^{\mu+\nu})$, ou enfin

$$\alpha \equiv (r+eup^{\mu+\nu-1})^2 - e^2u^2p^{2\mu+2\nu-2} \equiv (r+eup^{\mu+\nu-1})^2\,(\text{mod. } p^{\mu+\nu}).$$

(*Note du traducteur.*)

Nous devons observer enfin que toute équation $ax^2+2bxy+cy^2=M$, dans laquelle b^2-ac est négatif et $=-D$, peut être facilement ramenée à la forme que nous avons considérée dans ce qui précède. Désignons en effet par m le plus grand commun diviseur des nombres a et b, et posons

$$a=ma',\quad \frac{D}{m}=a'c-mb'^2=n,\quad a'x+b'y=x';$$

il en résulte l'équation $mx'^2+ny^2=a'M$, des solutions desquelles on ne doit conserver que celles dans lesquelles $x'-b'y$ est divisible par a', ou qui donnent des valeurs entières de x.

327. La solution directe de l'équation $ax^2+2bxy+cy^2=M$, contenue dans la Section V, suppose que l'on connaisse les valeurs de l'expression $\sqrt{(b^2-ac)}$ (mod. M); mais réciproquement, pour le cas où b^2-ac est négatif, la solution indirecte exposée dans les nos précédens fournit, pour trouver ces valeurs, une méthode très-expéditive, qui est bien préférable à celle du n° 322, surtout quand M est un très-grand nombre. Nous supposerons que M est nombre premier, ou du moins, s'il est composé, que ses facteurs sont encore inconnus; en effet, si l'on savait que M fût divisible par un nombre premier p, et que l'on eût $M=p^\mu M'$, de manière que M' ne renfermât plus le facteur p, il serait bien plus commode de chercher séparément les valeurs de $\sqrt{(b^2-ac)}$ pour les modules p^μ et M' (en déduisant les premières des valeurs pour le module p (n° 101)), et d'en conclure, par la combinaison, les valeurs pour le module M (n° 105).

Il faut donc chercher les valeurs de $\sqrt{-D}$ (mod. M), où D et M sont supposés positifs, et M contenu sous la forme des diviseurs de x^2+D (n° 147 et suivans); en effet, autrement il serait évident qu'aucun nombre ne satisferait à l'expression proposée. Soient $\pm r$, $\pm r'$, $\pm r''$, etc. les valeurs cherchées qui seront toujours opposées deux à deux, et

$$D+r^2=Mh,\quad D+r'^2=Mh',\quad D+r''^2=Mh'',\text{ etc.}$$

désignons par K, $-K$, K', $-K'$, K'', $-K''$, etc. les classes auxquelles appartiennent les formes

$$(M,r,h),(M,-r,h),(M,r',h'),(M,-r',h'),(M,r'',h''),(M,-r'',h''),\text{etc.},$$

et par Γ l'ensemble de ces classes. Généralement parlant, ces classes doivent être regardées comme inconnues; cependant il est clair, 1°. qu'elles sont toutes positives et proprement primitives; 2°. qu'elles appartiennent toutes à un même genre, dont le *caractère* peut facilement se conclure de la nature du nombre M, c'est-à-dire, de ses relations avec les différens diviseurs premiers de D, et de plus avec 4 ou 8, quand il y a lieu (n° 230). Puisque nous avons supposé que M est contenu sous une forme de diviseurs de x^2+D, nous sommes sûrs d'avance qu'il répond à ce caractère un genre positif proprement primitif de formes de déterminant $-D$, quand bien même l'expression $\sqrt{-D}$ (mod. M) ne pourrait être satisfaite. Donc, puisque ce genre est connu, on peut trouver toutes les classes qui y sont contenues; désignons-les par C, C', C'', etc., et leur ensemble par G. Les différentes classes K, $-K$, etc. doivent être identiques avec quelque classe comprise dans G; il peut arriver aussi que plusieurs classes de Γ soient identiques entre elles et qu'elles le soient parconséquent avec une même de G, et quand G n'en contient qu'une seule, il est certain que toutes les classes de Γ coïncident avec elle. Donc si des classes C, C', C'', etc., on tire les formes les plus simples f, f', f'', etc. respectivement, une forme de chaque classe de Γ se trouvera parmi elles. Or si $ax^2+2bxy+cy^2$ est une forme contenue dans la classe K, il y aura deux représentations du nombre M, par cette forme, appartenantes à la valeur r, et si l'une est $x=m$, $y=n$, l'autre sera $x=-m$, $y=-n$. On doit excepter le seul cas où $D=1$, dans lequel il y aurait quatre représentations (n° 180).

Il suit de là que si on cherche toutes les représentations du nombre M par les différentes formes f, f', f'', etc., par la méthode indirecte exposée précédemment, et qu'on en tire les valeurs de l'expression $\sqrt{-D}$ (mod. M), auxquelles chacune d'elles appartient (n° 154 et suivans), on aura *toutes* les valeurs de cette expression et même chacune d'elles deux fois, ou quatre fois si $D=1$. Si parmi les formes f, f', etc., il s'en trouve quelques-unes par lesquelles M ne puisse pas être représenté, il s'ensuit qu'elles n'appartiennent à aucune classe de Γ, et que parconséquent elles doivent être négligées; et si M ne pouvait être

représenté par aucune de ces formes, alors D serait certainement non-résidu quadratique de M.

Nous ajouterons encore sur ces opérations les observations suivantes, qui sont essentielles.

1°. Les représentations du nombre M par les formes f, f', etc. que nous employons, sont supposées avoir lieu par des valeurs premières entre elles des indéterminées x, y; s'il s'en présente d'autres dans lesquelles ces valeurs aient un commun diviseur μ, (ce qui ne peut arriver que lorsque μ^2 divise M, et qui arrivera nécessairement si $-DR\frac{M}{\mu^2}$), elles doivent être négligées dans nos Recherches, quoique, sous un autre aspect, elles puissent être utiles.

2°. Toutes choses d'ailleurs égales, le travail sera évidemment d'autant plus facile, que le nombre des classes f, f', f'', etc. sera moins grand, et il est parconséquent le plus court possible quand D est un des soixante-cinq nombres consignés au n°. 303, pour lesquels il n'y a qu'une seule classe dans chaque genre.

3°. Puisqu'il y a toujours deux de ces représentations, $x=m$, $y=n$; $x=-m$, $y=-n$ qui appartiennent à la même valeur, on voit qu'il suffit de considérer celles dans lesquelles y est positif; et de cette manière les représentations différentes correspondent à des valeurs différentes de l'expression $\sqrt{-D}$ (mod. M), et le nombre de toutes les valeurs est égal au nombre des représentations, en exceptant toujours le cas où $D=1$, dans lequel le premier nombre n'est que la moitié du second.

4°. Comme il suffit de connaître l'une des deux valeurs r, $-r$, pour avoir l'autre, les opérations peuvent encore s'abréger; si la valeur r s'obtient par la représentation du nombre M par une forme contenue dans la classe C, la valeur opposée $-r$ se tirera évidemment de la représentation par une forme contenue dans la classe opposée, qui sera différente de la classe C, si celle-ci n'est pas ambiguë. Il suit de là que, quand toutes les classes de G ne sont pas ambiguës, il ne faut considérer que la moitié des autres, c'est-à-dire, que de deux opposées, on prendra l'une et l'on négligera l'autre, que l'on voit d'avance et sans calcul devoir fournir

des valeurs opposées à celle que donne la première. Mais quand C est une classe ambiguë, elle donnera à-la-fois les deux valeurs r et $-r$: si l'on a choisi dans C la forme ambiguë $ax^2+2bxy+cy^2$, et que la valeur r résulte de la représentation $x=m$, $y=n$, la valeur $-r$ résultera de la représentation $x=-m-\frac{2nb}{a}$, $y=n$.

5°. Dans le cas où $D=1$, il n'y a qu'une seule classe dans laquelle on peut supposer qu'on ait choisi la forme x^2+y^2; et si la valeur r résulte de la représentation $x=m$, $y=n$, la même résultera des représentations

$$x=-m, y=-n;\ x=n, y=-m;\ x=-n, y=m,$$

et la valeur opposée $-r$, des représentations

$$x=m, y=-n;\ x=-m, y=n;\ x=n, y=m;\ x=-n, y=-m;$$

ainsi de ces huit représentations, qui ne forment qu'une seule décomposition, une suffit, pourvu qu'à la valeur résultante nous joignions la valeur opposée.

6°. La valeur de l'expression $\sqrt{-D}$ (mod. M), à laquelle appartient la représentation $M=am^2+2bmn+cn^2$, est (n° 155)

$$\mu(mb+nc)-\nu(ma+nb),$$

ou un nombre quelconque congru à celui-là, suivant le module M, μ et ν étant tels qu'on ait $\mu m+\nu n=1$; désignons cette valeur par ρ, on aura

$$\begin{aligned} m\rho &\equiv \mu m(mb+nc)-\nu(M-mnb-n^2c) \\ &\equiv(\mu m+\nu n)(mb+nc)\equiv mb+nc \ (\text{mod. } M); \end{aligned}$$

donc ρ est la valeur de l'expression $\frac{mb+nc}{m}$ (mod. M); on trouve de même que ρ est la valeur de l'expression $-\frac{ma+nb}{n}$ (mod. M).

Ces formules sont souvent préférables à celle dont on les a déduites.

328. *Exemples.* 1°. Soit proposé de trouver les valeurs de l'expression $\sqrt{-1365}$ (mod. $542861=M$). On a ici

$$M\equiv 1,\ 1,\ 1,\ 6,\ 11 \ (\text{mod. } 4,\ 3,\ 5,\ 7,\ 13),$$

et partant il est compris sous la forme des diviseurs de x^2+1,

x^2+3, x^2+5, et sous la forme des non-diviseurs de x^2+7, x^2-13, et partant (n° 150) sous la forme des diviseurs de x^2+1365. Le caractère du genre dans lequel se trouvent les classes Γ est

$$1,4;\quad R3;\quad R5;\quad N7;\quad N13.$$

Il n'y a qu'une classe dans ce genre; nous prendrons dans cette classe la forme $6x^2+6xy+229y^2$. Afin de trouver toutes les représentations du nombre M, nous ferons $2x+y=x'$, d'où il résultera $3x'^2+455y^2=2M$; cette équation admet quatre solutions dans lesquelles y est positif,

$$y=127,\quad x'=\pm 1083;\quad y=119,\quad x'=\pm 1213;$$

d'où il résulte quatre solutions de l'équation $6x^2+6xy+229y^2=M$, dans lesquelles y est positif,

$$\begin{array}{llll} x=478, & -605, & 547, & -666 \\ y=127, & 127, & 119, & 119. \end{array}$$

la première solution donne pour ρ la valeur de l'expression $\frac{30517}{478}$ ou $-\frac{3249}{127}$ (mod. M), d'où l'on tire 2350978; la seconde donne la valeur opposée; la troisième, la valeur 2600262, et la quatrième, la valeur opposée.

2°. Si l'on doit chercher les valeurs de l'expression $\sqrt{-286}$ (mod. $4272943=M$), le caractère du genre dans lequel sont les classes Γ se trouve être 1 *et* 7,8; $R11$; $R13$. C'est donc le genre principal, qui contient trois classes représentées par les formes

$$(1,\ 0,\ 286),\quad (14,\ 6,\ 23),\quad (14,\ -6,\ 23).$$

On doit négliger la troisième, comme opposée à la seconde. On trouve deux représentations du nombre M par la forme x^2+286y^2, dans lesquelles y est positif, savoir, $y=103$, $x=\pm 1113$, qui donnent pour l'expression proposée les valeurs ± 1493445: et comme M n'est pas représentable par la forme (14, 6, 23), il s'ensuit qu'il n'y a que les deux valeurs que nous venons de trouver.

3°. Étant proposée l'expression $\sqrt{-70}$ (mod. 997331), les classes Γ devront être contenues dans le genre dont le caractère est 3 *et* 5,8; $R5$; $N7$. Ce genre ne renferme qu'une classe dont

la représentante est (5,0, 14); or on trouve, en entreprenant le calcul, que 997331 n'est pas représentable par cette forme; donc —70 est nécessairement non-résidu de ce nombre.

329. Le problème où l'on se propose de distinguer les nombres premiers des nombres composés, et de décomposer ceux-ci en leurs facteurs premiers, est connu comme un des plus importans et des plus utiles de toute l'Arithmétique; tout le monde sait qu'il a été l'objet des recherches des géomètres tant anciens que modernes, et il serait inutile de donner des détails à cet égard. Cependant on ne peut s'empêcher de convenir que toutes les méthodes proposées jusqu'à présent sont restreintes à des cas très-particuliers, ou sont si longues et si pénibles, que même pour ceux de ces nombres qui ne dépassent pas les limites des Tables dont on est redevable à quelques mathématiciens, c'est-à-dire, pour les nombres à l'égard desquels ces méthodes sont inutiles, elles fatiguent la patience du calculateur le plus exercé, et qu'elles ne sont pour ainsi dire pas applicables à de plus grands nombres. Quoique ces Tables, qui sont dans les mains de tout le monde, et que l'on doit espérer devoir accroître encore par la suite, suffisent dans la plupart des cas qui se présentent ordinairement; il n'est cependant pas rare qu'un calculateur habile tire de la décomposition des grands nombres en facteurs, des avantages qui compensent au-delà l'emploi du temps. En outre, la dignité de la science semble demander que l'on recherche avec soin tous les secours nécessaires pour parvenir à la solution d'un problème si élégant et si célèbre. Aussi nous ne doutons pas que les deux méthodes suivantes, dont nous pouvons affirmer la briéveté et l'efficacité d'après une longue expérience, ne plaisent aux amateurs de l'Arithmétique. Au reste, il est dans la nature du problème, que les méthodes, *quelles qu'elles soient*, deviennent d'autant plus longues, que les nombres auxquels on les applique sont plus considérables; cependant, pour les méthodes suivantes, les difficultés ne s'accroissent qu'avec beaucoup de lenteur, et les nombres de sept, de huit et même d'un plus grand nombre de chiffres, ont toujours été traités, surtout par la seconde, avec un succès très-heureux, et avec toute la célérité que l'on peut attendre pour de si grands nombres, qui, suivant les méthodes connues jusqu'à présent, exigeraient

un

un travail intolérable, même pour le calculateur le plus infatigable.

Avant de se servir des méthodes suivantes, il est toujours très-utile d'essayer la division du nombre proposé, par quelques-uns des plus petits nombres premiers, comme 2, 3, 5, 7, etc. jusqu'à 19, ou encore plus loin, non-seulement afin de ne pas s'exposer à regretter d'avoir employé des méthodes recherchées et des artifices délicats pour trouver des nombres que la seule division aurait pu donner (*), mais encore parceque dans le cas où aucune division ne réussit, la seconde méthode emploie avec beaucoup de succès les restes qui en résultent. Ainsi, par exemple, si l'on doit décomposer en facteurs le nombre 314159265, la division par 3 réussit deux fois, et ensuite la division par 5 et par 7, d'où l'on tire

$$314159265 = 9.5.7.997331;$$

et il suffit de soumettre à un examen plus méthodique le nombre 997331, qu'on trouve n'être divisible ni par 11, ni par 13, ni par 17, ni par 19. De même, étant proposé le nombre 43429448, nous supprimerons le facteur 8, et nous appliquerons les méthodes au quotient 5428681.

330. Le principe qui sert de base à la PREMIÈRE MÉTHODE est le théorème suivant lequel *tout nombre positif ou négatif qui est résidu quadratique d'un autre nombre* M, *est aussi résidu de tout diviseur de* M. On sait que si M n'est divisible par aucun nombre premier plus petit que $\sqrt{M}$, M est certainement un nombre premier; donc si tous les nombres premiers au-dessous de cette limite, qui divisent M, sont p, q, etc., le nombre M sera composé des seuls nombres p, q, etc. ou de leurs puissances, ou bien il renfermera un seul facteur premier plus grand que $\sqrt{M}$, qui se trouve en divisant M par p, q, etc. autant de fois qu'il est possible. Désignant donc par ω l'ensemble de tous les nombres premiers au-dessous de M, il suffit évidemment d'avoir tous les diviseurs premiers de M qui sont contenus dans ω. Or si l'on

(*) D'autant plus que, généralement parlant, de six nombres il y en a à peine un qui soit non-divisible par tous les nombres 2, 3, 5,....19.

sait d'une manière quelconque qu'un certain nombre r, non-quarré, est résidu de M, on pourra être sûr que tout nombre premier, dont r est non-résidu, ne peut être diviseur de M, et parconséquent rejeter de ω tous les nombres qui se trouveront dans ce cas (ils composent le plus souvent presque la moitié de tous les nombres de ω). Si l'on sait encore qu'un autre nombre r' est résidu de M, on pourra rejeter des nombres que la première exclusion a laissés dans ω, tous ceux dont r' est non-résidu, qui composent encore presque la moitié, du moins si les résidus r et r' sont indépendans, c'est-à-dire, si l'un n'est pas par lui-même et nécessairement résidu de tous les nombres dont l'autre est résidu, ce qui arriverait quand rr' serait un quarré. Si l'on connaît encore d'autres résidus de M, r'', r''', etc. qui soient tous indépendans de ceux qui précèdent (*), on peut faire avec chacun d'eux des exclusions semblables, au moyen desquelles les nombres contenus dans ω décroissent avec tant de rapidité que bientôt, ou ils sont tous effacés, auquel cas le nombre M est premier, ou il en reste si peu que la division peut être essayée sans peine; dans ce dernier cas, parmi les nombres qui restent se trouvent nécessairement les diviseurs de M, s'il en existe. Pour un nombre qui ne surpasse pas beaucoup 1000000, il suffit le plus souvent de six ou sept exclusions; et de neuf ou dix, pour un nombre de huit ou neuf chiffres. Il nous reste maintenant deux choses à faire, 1°. à trouver des résidus de M qui soient convenables et en assez grand nombre; 2°. à effectuer l'exclusion de la manière la plus commode. Mais nous intervertirons l'ordre de ces questions, d'autant plus que la seconde nous apprendra quels sont les résidus qui conviennent le mieux.

331. Nous avons enseigné avec assez de détails dans la Section IV, à distinguer les nombres premiers dont un nombre donné r est résidu (r n'étant divisible par aucun quarré), d'avec ceux dont il est non-résidu, c'est-à-dire, les diviseurs de $x^2 - r$ d'avec les

(*) Si le produit de tant de nombres r, r', r'', etc. qu'on voudra est un quarré, un quelconque d'entre eux, r, par exemple, sera résidu de tout nombre dont les autres seront résidus. Ainsi, pour que les résidus soient indépendans, il faut que leurs produits ne puissent être des quarrés, soit qu'on les prenne deux à deux, ou trois à trois, ou quatre à quatre, etc.

non-diviseurs ; on a vu que les premiers étaient contenus sous des formes de cette espèce :

$$rz+a,\ rz+b,\ \text{etc.},\ \text{ou}\ 4rz+a,\ 4rz+b,\ \text{etc.}$$

et les derniers sous des formules semblables. Toutes les fois que r est un nombre assez petit, les exclusions pourront s'exécuter très-commodément, à l'aide de ces formules; ainsi, par exemple, quand $r=1$, il faut exclure tous les nombres de la forme $4z+3$; tous les nombres de la forme $8z+3$ et $8z+5$, quand $r=2$, etc. Mais comme on n'est pas toujours maître de trouver de tels résidus du nombre proposé, et que l'application des formules n'est plus assez commode quand r est un grand nombre, on gagne beaucoup et l'on diminue prodigieusement le travail des exclusions, si pour une assez grande quantité de nombres (r) non-divisibles par des quarrés, pris positivement et négativement, on construit une table dans laquelle on ait distingué les nombres premiers qui sont résidus des différens nombres (r), d'avec ceux qui en sont non-résidus. Cette table pourra être disposée comme la petite table II qu'on trouve à la fin de cet ouvrage, et dont nous avons déjà donné la description (n° 99); mais pour qu'elle présente toute l'utilité convenable au but que nous nous proposons, les nombres premiers placés en marge, ou les modules, doivent être continués bien plus loin, par exemple, jusqu'à 1000 ou 10000; et en outre, on obtiendra un grand avantage, si l'on place en tête même les nombres composés et les nombres négatifs, quoique cela ne soit pas absolument nécessaire, comme on peut le voir par la Section IV. On atteindrait le plus haut point d'utilité, si les colonnes verticales dont elle est composée étaient détachées et rassemblées sur des lames ou *bâtons* semblables à ceux de *Neper;* desorte que l'on pût considérer séparément celles qui sont nécessaires dans chaque cas, c'est-à-dire, celles qui répondent aux nombres r, r', r'', etc. qui sont résidus du nombre à décomposer. En supposant ces bâtons convenablement placés auprès de la première colonne qui renferme les modules, c'est-à-dire, de manière que les parties de ces bâtons qui correspondent à un même nombre premier de la colonne des modules, soient dans une même ligne horizontale, il est évident que les nombres premiers qui restent dans ω après les exclusions faites avec les résidus r, r', r'', etc.

se reconnaîtront immédiatement à l'inspection: en effet, ce sont ceux de la première colonne auxquels répond dans chaque colonne le petit trait indicateur, tandis que l'on doit rejeter tous ceux auxquels répond un espace vide dans un quelconque des bâtons. Un exemple éclaircira suffisamment cette explication.

Si l'on sait, d'une manière quelconque, que les nombres

$$-6,\ +13,\ -14,\ +17,\ +37,\ -53$$

sont résidus de 997331, on doit rassembler la première colonne, qui, dans ce cas, doit être continuée jusqu'à 997, c'est-à-dire, jusqu'au nombre immédiatement moindre que $\sqrt{997331}$, et les bâtons en tête desquels sont inscrits les nombres -6, $+13$, etc. Voici une partie du tableau que l'on forme de cette manière

	−	+	−	+	+	−
	6	13	14	17	37	53
3	—	—	—		—	—
5	—		—			
7	—		—		—	
11	—				—	
13		—	—	—		—
17		—		—		—
19			—	—		—
23		—	—			—
etc.			etc.			etc.
113		—	—			—
127	—	—	—	—	—	—
131	—	—	—	—	—	—
etc.			etc.			etc.

De la même manière qu'on reconnaît ici à l'inspection, que des nombres premiers contenus dans ce tableau, 127 est le seul qui reste dans ω, après l'exclusion faite avec les nombres -6, 13, etc., on reconnaîtra, en achevant le travail jusqu'à 997, qu'il n'en reste effectivement pas d'autre. En essayant la division par 127,

elle réussit, et l'on a

$$997331 = 127 \times 7853 \ (*).$$

Au reste, il suit de ce que nous venons d'exposer, qu'il faut employer surtout des résidus qui ne soient pas très-grands, ou du moins qui puissent se décomposer en facteurs premiers de grandeur moyenne, puisque l'usage immédiat de la table auxiliaire ne s'étend pas au-delà des nombres placés en tête, et que l'usage médiat ne s'étend qu'aux nombres qui peuvent se décomposer en facteurs premiers contenus dans la table.

332. Nous donnerons trois méthodes différentes pour trouver des résidus du nombre M; mais avant de les exposer, nous présenterons deux observations à l'aide desquelles on pourra déduire des résidus plus simples, lorsque ceux que l'on aura obtenus ne paraîtront pas convenables.

1°. Si le nombre ak^2, divisible par le quarré k^2, que nous supposons premier avec M, est résidu de M, a sera aussi résidu; ainsi les résidus divisibles par de grands quarrés sont aussi utiles que les petits, et nous supposerons que les résidus trouvés par les méthodes suivantes aient été délivrés de leurs facteurs quarrés.

2°. Si deux ou plusieurs nombres sont résidus, leur produit le sera aussi. En combinant cette observation avec la précédente, on peut très-souvent déduire de plusieurs résidus qui ne sont pas tous assez simples, un autre qui le soit beaucoup, pourvu qu'ils aient un grand nombre de facteurs communs. C'est pourquoi il est utile d'avoir des résidus composés de plusieurs facteurs qui ne soient pas trop grands, et il convient de les décomposer sur-le-champ en leurs facteurs. La force de ces observations se reconnaîtra mieux par des exemples et par un usage fréquent, que par des préceptes.

(*) L'auteur a construit pour son propre usage une grande partie de l'appareil de cette table, et il l'aurait publié volontiers, si le petit nombre de ceux auxquels elle serait utile, suffisait aux frais d'une telle entreprise; cependant si quelque amateur, après s'être bien pénétré des principes, desirait se construire une pareille table, l'auteur se ferait un grand plaisir de lui communiquer, par lettres, les différens procédés et les artifices que l'on peut employer.

I. La méthode la plus simple et la plus commode pour ceux à qui l'habitude a donné quelque dextérité, consiste à décomposer le nombre M, ou plus généralement, un multiple quelconque de ce nombre en deux parties quelconques, ensorte qu'on ait $kM = a + b$, a et b étant tous deux positifs, ou l'un positif et l'autre négatif; le produit pris avec un signe contraire sera résidu de M; en effet, on aura $-ab \equiv a^2 \equiv b^2 \pmod{M}$, et partant $-abRM$. On doit prendre les nombres a et b de manière que le produit soit divisible par un grand quarré, et que la division donne un quotient assez petit, ou du moins décomposable en facteurs qui ne soient pas trop grands, ce qu'on peut toujours faire sans peine. On doit surtout recommander de prendre pour a un quarré, ou le double, ou le triple d'un quarré, dont la différence avec M soit petite ou du moins décomposable en facteurs qui puissent être employés commodément.

Ainsi, par exemple, on trouve

$$\begin{aligned} 997331 &= (999)^2 - 2.5.67 &&= (994)^2 + 5.11.13^2 \\ &= 2.(706)^2 + 3.17.3^2 &&= 3.(575)^2 + 11.31.4 \\ &= 3.(577)^2 - 7.13.4^2 &&= 3.(578)^2 - 7.19.37 \\ &= 11.(299)^2 + 2.3.5.29.4^2 &&= 11.(301)^2 + 5.11^2, \text{ etc.} \end{aligned}$$

On tire de là les résidus :

$$2.5.67, -5.11, -2.3.17, -3.11.31, 3.7.13, 3.7.19.37, -2.3.5.11.29;$$

la dernière décomposition donne le résidu -5.11, que nous avons déjà. Au lieu des résidus $-3.11.31$ et $-2.3.5.11.29$, on peut tirer de leur combinaison avec -5.11, les résidus $3.5.31$, $2.3.29$.

II. La seconde et la troisième méthode se déduisent de ce que, si deux formes binaires (A, B, C), (A', B', C') de même déterminant M ou $-M$, ou plus généralement $\pm kM$, appartiennent au même genre, les nombres AA', AC', $A'C$ sont résidus de kM, ainsi qu'il est aisé de le conclure de ce que le nombre caractéristique de l'une des formes est également celui de l'autre, et que parconséquent, si l'on représente ce nombre par m, les nombres mA, mC, mA', mC' sont tous résidus de kM. Si donc (a, b, a') est une forme réduite de déterminant positif M, ou plus généralement, de déterminant kM, et que (a', b', a''),

(a'', b'', a'''), etc. soient des formes de sa période, qui sont par-conséquent équivalentes à (a, b, a') et du même genre qu'elle, les nombres aa', aa'', aa''', etc. sont tous résidus de M. On calcule avec facilité un grand nombre de formes d'une pareille période, à l'aide de l'algorithme du n° 187. On obtient ordinairement les résidus les plus simples en faisant $a = 1$; on rejettera ceux qui seraient composés de trop grands facteurs.

Nous joignons le commencement des périodes des formes

$$(1, 998, -1327) \quad \text{et} \quad (1, 1412, -918),$$

dont les déterminans sont 997331 et 1994662 respectivement, c'est-à-dire, M et $2M$:

(1, 998, —1327)	(1, 1412, —918)
(—1327, 329, 670)	(—918, 1342, 211)
(670, 341, —1315)	(211, 1401, —151)
(—1315, 974, 37)	(—151, 1317, 1723)
(37, 987, —626)	(1723, 406, —1062)
(—626, 891, 325)	(—1062, 656, 1473)
(325, 734, —1411)	(1473, 817, —901)
(—1411, 677, 382)	(—901, 985, 1137)
(382, 851, —715)	etc.

Ainsi tous les nombres: —1327, 670, etc. sont des résidus de 997331; et en négligeant ceux qui renferment de trop grands facteurs, il reste les suivans:

2.5.67, 37, 13, —17.83, —5.11.13, —2.3.17, —2.59, —17.53.

Nous avions déjà trouvé le résidu 2.5.67, ainsi que —5.11, qui résulte de la combinaison du troisième et du cinquième.

III. Si C est une classe quelconque de déterminant négatif $-M$ ou $-kM$ différente de la classe principale, et que sa période (n° 307) soit C^2, C^3, etc.; les classes C^2, C^4, etc. appartiendront au genre principal, et les classes C^3, C^5, etc. appartiendront au même genre que C. Si donc (a, b, c) est la forme la plus simple de C, et (a', b', c') une forme d'une classe de cette période, de C^n, par exemple, on aura $a'RM$, ou $aa'RM$, suivant que n sera pair ou impair; c', dans le premier cas, ac', $a'c$ et cc', dans

le second, seront encore résidus. Le calcul de la période, c'est-à-dire celui des formes les plus simples, s'exécute avec une facilité étonnante, quand a est très-petit, et surtout quand $a=3$, ce que l'on peut toujours obtenir si $kM\equiv 2 \pmod 3$ (*). Voici le commencement de la période de la classe dans laquelle est contenue la forme (3, 1, 332444):

$C=(3, 1, 332444)$, $C^2=(9, -2, 210815)$,
$C^3=(27, 7, 36940)$, $C^4=(81, 34, 12327)$,
$C^5=(243, 34, 4109)$, $C^6=(729, -209, 1428)$,
$C^7=(476, 209, 2187)$, $C^8=(1027, 342, 1085)$,
$C^9=(932, -437, 1275)$, $C^{10}=(425, 12, 2347)$,
etc.

On tire de là les résidus suivans, en rejetant ceux qui sont inutiles,

$$3.476,\quad 1027,\quad 1085,\quad 425,$$

ou, en supprimant les facteurs quarrés,

$$3.7.17,\quad 13.79,\quad 5.7.31,\quad 17.$$

Si l'on combine convenablement ces nombres avec les huit qu'a donnés la méthode II, on obtient facilement les douze suivans:

$$-2.3,\quad 13,\quad -2.7,\quad 17,\quad 37,\quad -53,$$
$$-5.11,\quad 79,\quad -83,\quad -2.59,\quad -2.5.31,\quad 2.5.67.$$

Les six premiers sont ceux dont nous nous sommes servis n° 331. Nous aurions pu ajouter les résidus 19 et -29, si nous avions voulu nous servir de ceux qu'a fournis la méthode I; quant aux autres trouvés par cette méthode, ils sont dépendans des résidus que nous venons de déterminer.

333. La *seconde méthode*, pour décomposer en facteurs un nombre donné, se tire de la considération des valeurs de l'expression $\sqrt{-D} \pmod M$, et repose sur les observations suivantes:

I. Quand M est un nombre premier, ou une puissance d'un nombre premier, impair et non-diviseur de D, $-D$ est résidu ou non-résidu de M, suivant que M est compris dans une forme

(*) Comme le cas où M est divisible par 3, ne peut se présenter (n° 329), il est aisé de voir que l'on est même toujours maître de prendre k tel que kM soit $\equiv 2 \pmod 3$. (*Note du traducteur*).

de

de diviseurs ou de non-diviseurs de x^2+D, et dans le premier cas, l'expression $\sqrt{-D}$ (mod. M) n'aura que deux valeurs qui seront opposées.

II. Mais quand M est composé et $=pp'p''$ etc., p, p', p'', etc. désignant des nombres premiers impairs et non-diviseurs de D, ou des puissances de tels nombres, $-D$ ne sera résidu de M que quand il le sera des nombres p, p', p'', etc., c'est-à-dire, quand tous ces nombres seront contenus dans des formes de diviseurs de x^2+D. Or en désignant toutes les valeurs de l'expression $\sqrt{-D}$, suivant les modules p, p', p'', etc., par r, r', r'', etc. respectivement, on trouvera toutes les valeurs de la même expression, suivant le module M, en déterminant des nombres qui soient $\equiv\pm r$ (mod. p), $\equiv\pm r'$ (mod. p'), etc.; ainsi le nombre de ces valeurs sera 2^μ, si l'on exprime par μ le nombre des facteurs p, p', p'', etc. Si donc ces valeurs sont $R, -R, R', -R', R'$, etc., la congruence $R\equiv R$ a évidemment lieu par elle-même, suivant tous les modules de p, p', p'', etc., et la congruence $R\equiv -R$ n'a lieu suivant aucun de ces nombres; donc le plus grand commun diviseur de $R-R$ et de M est M, et celui de $R+R$ et de M est 1; mais deux valeurs telles que R et R', qui ne sont ni identiques, ni opposées, seront nécessairement congrues, suivant un ou plusieurs des nombres p, p', p'', etc. mais ne le seront pas suivant tous, et l'on aura, suivant les autres, $R\equiv -R'$; donc le produit des premiers est le plus grand commun diviseur des nombres M et $R-R'$, tandis que le produit des derniers est le plus grand commun diviseur des nombres M et $R+R'$. Il est facile de conclure de là que si l'on cherche les plus grands communs diviseurs entre M et les différences d'une valeur donnée de l'expression $\sqrt{-D}$ (mod. M) à toutes les autres, l'ensemble de ces communs diviseurs contiendra les nombres 1, p, p', p'', etc. et les produits de ces nombres pris deux à deux, trois à trois, etc. *On parviendra donc de cette manière à déterminer les nombres* p, p', p'', *etc., à l'aide des valeurs de cette expression.*

Au reste, comme la méthode du n° 327 réduit la recherche des valeurs de l'expression $\sqrt{-D}$ (mod. M) à celle des valeurs qui sont de la forme $\frac{m}{n}$ (mod. M), dans lesquelles le dénomi-

nateur n est premier avec M, il n'est pas nécessaire, pour parvenir à notre but, de trouver ces valeurs; car le plus grand commun diviseur du nombre M et de la différence $R-R'$, R et R' correspondant à $\frac{m}{n}$ et $\frac{m'}{n'}$, sera évidemment le plus grand commun diviseur des nombres M et $nn'(R-R')$, ou des nombres M et $mn'-m'n$, puisque ce dernier est congru à $nn'(R-R')$ suivant le module M.

334. L'application des observations précédentes au problème dont il s'agit, peut se faire de deux manières; la *première* non-seulement décide si le nombre proposé M est premier ou composé, mais encore donne dans le dernier cas les facteurs eux-mêmes; la *seconde* a l'avantage de l'emporter le plus souvent par la briéveté des calculs, mais quelquefois elle ne donne pas les facteurs des nombres composés, à moins qu'on ne la répète plusieurs fois; au reste elle distingue avec autant de facilité que la première, les nombres premiers des nombres composés.

I. On cherchera un nombre négatif $-D$ qui soit résidu quadratique de M, et l'on peut employer à cette recherche les méthodes exposées n° 332, I et II. Il est indifférent en soi de prendre tel ou tel résidu, et il n'est pas nécessaire, comme dans la solution précédente, que D soit un petit nombre; mais comme le calcul deviendra d'autant plus simple, qu'il y aura moins de classes de formes binaires, dans chaque genre proprement primitif de déterminant $-D$, on trouvera de l'avantage à choisir, s'il est possible, un des soixante-cinq nombres cités au n° 303. Ainsi pour $M=997331$, parmi tous les résidus déterminés plus haut, le plus avantageux est -102. On cherchera toutes les valeurs de l'expression $\sqrt{-D}$ (mod. M), et s'il n'y en a que deux qui soient opposées, M sera certainement un nombre premier, ou une puissance d'un nombre premier; s'il y en a un plus grand nombre, 2^{μ}, par exemple, M sera composé de μ facteurs qui sont des nombres premiers, ou des puissances de nombres premiers. Or il sera extrêmement facile de reconnaître si ces nombres sont premiers, ou des puissances de nombres premiers, et dans ce dernier cas, la méthode par laquelle on trouve les valeurs de $\sqrt{-D}$ (mod. M) indique d'elle-même tous les nombres premiers dont une

certaine puissance divise le nombre M; savoir, si M est divisible par le quarré d'un nombre premier π, le calcul conduira certainement à une ou plusieurs représentations du nombre M, telles que $M=am^2+2bmn+cn^2$, dans lesquelles le plus grand commun diviseur des nombres m et n est π, et cela arrive parcequ'alors $-D$ est aussi résidu de $\frac{M}{\pi^2}$; mais quand il n'y a aucune représentation dans laquelle m et n aient un diviseur commun, c'est un indice certain que M n'est divisible par aucun quarré, et que parconséquent p, p', p'', etc. sont des nombres premiers.

Exemple. Par la méthode exposée plus haut, on trouve quatre valeurs de l'expression $\sqrt{-408}$ (mod. 997331) qui coïncident avec celle des expressions $\pm\frac{1664}{113}$, $\pm\frac{2824}{3}$; les plus grands communs diviseurs du nombre 997331, avec

$$3.1664-113.2824 \quad \text{et} \quad 3.1664+113.2824,$$

ou avec 314120 et 324104 sont 7853 et 127, d'où l'on tire, comme ci-dessus, $997331=7853.127$.

II. On prendra un nombre négatif $-D$, tel que M soit contenu dans une des formes de diviseurs de x^2+D; quoiqu'on puisse choisir ce nombre de telle grandeur qu'on voudra, il est avantageux de chercher à rendre le plus petit possible le nombre des classes contenues dans les genres de déterminant $-D$. Au reste on ne rencontre aucune difficulté dans la recherche de ce nombre; en effet, parmi une quantité considérable de nombres essayés, il y en a presque autant pour lesquels M soit dans une forme de diviseurs, qu'il y en a pour lesquels M soit dans une forme de non-diviseurs. Il sera donc convenable de commencer les essais par les soixante-cinq nombres du n° 303, à partir des plus grands, et s'il se trouvait qu'aucun d'eux ne fût convenable (ce qui n'arrive, généralement parlant, qu'une fois sur 16384), on passerait à d'autres pour lesquels il n'y eût que deux classes dans chaque genre.

On cherchera alors les valeurs de l'expression $\sqrt{-D}$ (mod. M), et si l'on en trouve, les facteurs de M se déduiront absolument de la même manière que plus haut; mais si l'on n'obtient aucunes valeurs, c'est-à-dire, si $-D$ n'est pas résidu de M, M ne

sera certainement ni un nombre premier, ni une puissance d'un nombre premier. Quand, dans ce cas, on voudra connaître les facteurs eux-mêmes, il faudra recommencer l'opération avec une autre valeur de D, ou recourir à une autre méthode.

Ainsi, par exemple, on trouve que 997331 est contenu dans une forme de non-diviseurs pour x^2+1848, x^2+1365, x^2+1320, mais dans une forme de diviseurs de x^2+840. On parvient pour les valeurs de l'expression $\sqrt{-840}$ (mod. 997331) aux expressions $\pm\frac{1271}{163}$, $\pm\frac{3288}{125}$, d'où l'on tire les facteurs déjà connus.

Ceux qui desireraient un plus grand nombre d'exemples, peuvent consulter le n° 328, où le premier prouve que $5428681=307.17685$; le second, que 4272 est un nombre premier; le troisième, que 997331 est surement un nombre composé.

Au reste, les limites de cet ouvrage ne nous permettent d'insérer ici que les bases les plus importantes des deux méthodes qui servent à la décomposition en facteurs. Nous réservons pour une autre occasion l'exposition plus détaillée, ainsi que plusieurs tables auxiliaires.

SECTION SEPTIÈME.

Des Equations qui déterminent les Sections circulaires.

335. PARMI les accroissemens importans dont les travaux des modernes ont enrichi les Mathématiques, les fonctions circulaires tiennent sans aucun doute le premier rang. Cette étonnante espèce de quantités, à laquelle nous sommes conduits à chaque instant dans des recherches qui y semblent tout-à-fait étrangères, et du secours desquelles ne peut se passer aucune partie des Mathématiques, a occupé avec tant d'assiduité la pénétration des plus grands géomètres, et ils en ont fait une théorie si vaste, qu'on ne pouvait guère s'attendre qu'une partie de cette théorie, partie élémentaire et pour ainsi dire placée à l'entrée, pût recevoir des accroissemens considérables. Je parle de la théorie des fonctions trigonométriques, qui répondent aux arcs commensurables avec la circonférence, ou de la théorie des polygones réguliers, dont on ne connaît jusqu'à présent que la plus petite partie, ainsi qu'on le verra par cette Section. Le lecteur pourrait s'étonner de rencontrer une semblable recherche dans un ouvrage consacré à une doctrine qui paraît au premier abord absolument hétérogène; mais l'exposition fera voir bien clairement quelle est la liaison de ce sujet et de l'Arithmétique transcendante.

Au reste, les principes de la théorie que nous entreprenons d'exposer, s'étendent bien plus loin que nous ne le faisons voir ici; ils peuvent en effet s'appliquer non-seulement aux fonctions circulaires, mais aussi avec autant de succès à beaucoup d'autres fonctions transcendantes, par exemple, à celles qui dépendent de l'intégrale $\int \frac{dx}{\sqrt{(1-x^4)}}$, et en outre à différens genres de congruences; mais comme nous préparons un Ouvrage assez étendu sur les fonctions transcendantes, et que dans la suite de ces *Recherches*

arithmétiques nous traiterons amplement des congruences, nous avons cru ne devoir considérer ici que les fonctions circulaires, et même quoique nous pussions les embrasser dans toute leur généralité, nous les réduirons au cas le plus simple, comme on va le voir dans le n° suivant, tant dans le dessein d'abréger, que pour rendre d'une intelligence plus facile les principes tout-à-fait nouveaux de cette théorie.

336. Si nous désignons par P la circonférence du cercle, ou quatre angles droits, que nous supposions entiers les nombres m et n, et n égal au produit des facteurs premiers entre eux a, b, c, etc.; l'angle $A=\frac{mP}{n}$ peut, par le n° 310, être mis sous la forme

$$A=\left(\frac{\alpha}{a}+\frac{\beta}{b}+\frac{\gamma}{c}+\text{etc.}\right)P,$$

et les fonctions trigonométriques qui en dépendent se déduiront, par les méthodes connues, des fonctions correspondantes aux parties $\frac{\alpha P}{a}$, $\frac{\beta P}{b}$, etc. Ainsi, comme on peut toujours prendre pour a, b, c, etc. des nombres premiers ou des puissances de nombres premiers, il suffit évidemment de considérer la section du cercle en parties dont le nombre est premier, ou une puissance d'un nombre premier, et le polygone de n côtés se déduira sur-le-champ des polygones de a, b, c, etc. côtés. Cependant ici nous bornerons nos recherches au cas où l'on doit diviser le cercle en un nombre premier impair de parties. En effet, il est constant que les fonctions circulaires qui répondent à l'angle $\frac{mP}{p^2}$, se déduisent de celles qui appartiennent à l'angle $\frac{mP}{p}$ par la solution d'une équation du degré p; des premières on déduira, par une équation de même degré, celles qui appartiennent à l'angle $\frac{mP}{p^3}$; de manière que, si l'on connaît déjà le polygone de p côtés, on a nécessairement besoin de la résolution de $\lambda-1$ équations du degré p pour obtenir le polygone de p^λ côtés; et même si nous pouvions étendre notre théorie à ce cas, nous n'en serions pas moins conduits au même nombre d'équations du degré p,

qui ne peuvent se réduire en aucune manière, si p est un nombre premier.

Ainsi, par exemple, nous ferons voir plus bas que le polygone de 17 côtés peut être construit géométriquement; mais pour déterminer le polygone de 289 côtés, on ne peut éviter d'aucune manière l'équation du dix-septième degré.

337. Tout le monde sait que les fonctions trigonométriques des angles $\frac{kP}{n}$, k désignant indéfiniment les nombres $0, 1, 2, \ldots n-1$, sont les racines d'une équation du degré n; ces équations sont:

pour les *sinus*, $$x^n - \tfrac{1}{4}nx^{n-2} + \tfrac{1}{16}\cdot\frac{n(n-3)}{1.2}x^{n-4} - \tfrac{1}{64}\cdot\frac{n(n-4)(n-5)}{1.2.3}x^{n-6} + \text{etc.} = 0 \ldots\ldots \text{(I)},$$

cosinus, $$x^n - \tfrac{1}{4}nx^{n-2} + \tfrac{1}{16}\cdot\frac{n(n-3)}{1.2}x^{n-4} - \tfrac{1}{64}\cdot\frac{n(n-4)(n-5)}{1.2.3}x^{n-6} + \text{etc.} = \frac{1}{2^{n-1}} \ldots \text{(II)},$$

tangentes, $$x^n - \frac{n(n-1)}{1.2}x^{n-2} + \frac{n(n-1)(n-2)(n-3)}{1.2.3.4}x^{n-4} + \text{etc.}$$
$$\pm nx = 0 \ldots\ldots\ldots\ldots\ldots\ldots \text{(III)}.$$

Ces équations, qui sont toutes vraies quand n est impair (la seconde l'est même quand n est pair), se réduisent facilement au degré m, en faisant $x = 2m + 1$, savoir, pour la première et la troisième, en divisant par x et posant ensuite $x^2 = y$; quant à la seconde, elle renferme nécessairement la racine $x = 1 = \cos. 0$, et les autres sont égales deux à deux, $\cos\frac{P}{n} = \cos\frac{(n-1)P}{n}$, $\cos\frac{2P}{n} = \cos\frac{(n-2)P}{n}$, etc. Donc l'équation est divisible par $x - 1$ et le quotient est un quarré. En extrayant la racine, l'équation devient

$$x^m + \tfrac{1}{2}x^{m-1} - \tfrac{1}{4}(m-1)x^{m-2} - \tfrac{1}{8}(m-2)x^{m-3} + \tfrac{1}{16}\frac{(m-2)(m-3)}{1.2}x^{m-4}$$
$$+ \tfrac{1}{32}\frac{(m-1)(m-4)}{1.2}x^{m-5} - \text{etc.} = 0,$$

dont les racines sont les cosinus des angles $\frac{P}{n}, \frac{2P}{n}, \frac{3P}{n}, \ldots\ldots \frac{nP}{n}$.

On ne connaissait pas jusqu'à présent de réductions ultérieures de ces équations, même pour le cas où n est un nombre premier.

Cependant aucune de ces équations n'est si commode à traiter, ni se prête tant à notre dessein, que l'équation $x^n - 1 = 0$, dont on sait que les racines sont intimement liées avec les racines des premières. En effet, si l'on représente par i la quantité imaginaire $\sqrt{-1}$, les racines de l'équation $x^n - 1 = 0$ sont représentées par la formule

$$\cos\frac{KP}{n} + i\sin\frac{KP}{n} = r,$$

où l'on doit prendre pour K tous les nombres $1, 2, 3, \ldots n-1$; ainsi, comme on a

$$\frac{1}{r} = \cos\frac{KP}{n} - i\sin\frac{KP}{n},$$

les racines de l'équation (I) seront exprimées par

$$\frac{1}{2i}\left(r - \frac{1}{r}\right), \text{ ou } \frac{i(1-r^2)}{2r};$$

celles de l'équation (II) par $\frac{1}{2}\left(r + \frac{1}{r}\right) = \frac{1+r^2}{2r}$;

celles de l'équation (III) par $\frac{i(1-r^2)}{1+r^2}$.

C'est pourquoi nous établirons nos considérations sur l'équation $x^n - 1 = 0$, en supposant que n soit un nombre premier impair; mais pour ne pas interrompre l'ordre de nos recherches, nous commencerons par le lemme suivant.

338. PROBLÈME. *Étant donnée l'équation* (W)$\ldots z^m + Az^{m-\alpha} + \text{etc.} = 0$, *trouver une équation* (W'), *dont les racines soient les puissances* λ *de celles de l'équation* (W), λ *étant un nombre entier positif donné.*

Désignons les racines de l'équation (*W*) par $a, b, c,$ etc., celles de l'équation (*W'*) devront être $a^\lambda, b^\lambda, c^\lambda,$ etc. Or, par le théorème de *Newton*, on peut trouver en fonction des coefficiens de l'équation (*W*), la somme des puissances quelconques des racines $a, b, c,$ etc.; on cherchera donc les sommes

$$a^\lambda + b^\lambda + c^\lambda + \text{etc.}, \quad a^{2\lambda} + b^{2\lambda} + c^{2\lambda} + \text{etc.}, \text{ etc.},$$

jusqu'à $\qquad a^{m\lambda} + b^{m\lambda} + c^{m\lambda} + \text{etc.},$

d'où

d'où par le procédé inverse tiré du même théorème, on pourra déduire les coefficiens de l'équation (W'). On voit en même temps que si les coefficiens de l'équation (W) sont tous rationnels, ceux de l'équation (W') le seront aussi; on pourrait même prouver par une autre voie, que si les premiers sont entiers, les autres le seront; mais comme ce théorème ne nous est pas nécessaire, nous ne nous y arrêterons pas ici.

339. L'équation $x^n - 1 = 0$ (en supposant, comme il faut toujours le faire par la suite, que n est un nombre premier impair), ne renferme qu'une seule racine réelle $x = 1$; les $n - 1$ autres, qui sont donnés par l'équation

$$x^{n-1} + x^{n-2} + \text{etc.} + x + 1 = 0, \ldots\ldots (X)$$

sont toutes imaginaires; nous en désignerons l'ensemble par Ω. Si donc r est une racine quelconque de $X = 0$, on aura

$$1 = r^n = r^{2n} = \text{etc.}, \text{ et généralement } 1 = r^{en}$$

pour toute valeur entière de e, soit positive, soit négative. D'où l'on voit que si λ et μ sont des nombres entiers congrus suivant n, on aura $r^\lambda = r^\mu$; mais si λ et μ sont incongrus suivant le module n, r^λ et r^μ seront inégaux. Dans ce cas, on peut déterminer un nombre entier ν, tel qu'on ait

$$(\lambda - \mu)\nu \equiv 1 \pmod{n}, \text{ et partant, } r^{(\lambda-\mu)\nu} = r;$$

donc $r^{\lambda-\mu}$ ne sera certainement pas $= 1$: or il est clair que toute puissance de r est racine de l'équation $x^n - 1 = 0$; parconséquent comme toutes les quantités $1 = r^0, r, r^2, r^3 \ldots\ldots r^{n-1}$ sont différentes, elles représentent toutes les racines de l'équation $x^n - 1 = 0$, et $r, r^2 \ldots\ldots r^{n-1}$ coïncident avec les racines Ω. On conclut facilement de là que Ω coïncide avec $r^e, r^{2e}, r^{3e}, \ldots\ldots r^{(n-1)e}$, e étant un entier quelconque, positif ou négatif, et non-divisible par n. On aura parconséquent

$$X = (x - r^e)(x - r^{2e})(x - r^{3e}) \ldots\ldots (x - r^{(n-1)e});$$

d'où, $\ldots\ldots r^e + r^{2e} + r^{3e} + \ldots\ldots + r^{(n-1)e} = -1$;

et, $\ldots\ldots 1 + r^e + r^{2e} \ldots\ldots + r^{(n-1)e} = 0$.

Nous appellerons *réciproques* deux racines telles, que r et $\frac{1}{r}$, ou

plus généralement r^{ϵ}, $r^{-\epsilon}$, et il est clair que le produit des deux facteurs simples $x - r$ et $x - \frac{1}{r}$ est

$$x^2 - 2x\cos\omega + 1,$$

l'angle ω étant $= \frac{P}{n}$, ou à un de ses multiples.

340. Ainsi, comme en représentant une racine de $X = 0$ par r, toutes les racines de l'équation $x^n - 1 = 0$ sont exprimées par les différentes puissances de r, le produit de plusieurs d'entre ces racines pourra être exprimé par r^{λ}, de quelque manière qu'il soit composé, λ étant $= 0$, ou positif et $< n$; et si l'on désigne par $\varphi(t, u, v, \ldots)$ une fonction algébrique rationnelle et entière des indéterminées t, u, v, etc., dont les différens termes soient de la forme $ht^{\alpha}u^{\beta}v^{\gamma}$, etc., il est évident, qu'en prenant pour t, u, v, etc. quelques-unes des racines de l'équation $x^n - 1 = 0$, par exemple, $t = a$, $u = b$, $v = c$, etc.; $\varphi(t, u, v\ldots)$ pourra être mise sous la forme

$$A + A'r + A''r^2 + A'''r^3 + \ldots + A^{(\nu)}r^{n-1};$$

de manière que les coefficiens A, A', etc. (dont quelques-uns peuvent être $= 0$), soient des quantités déterminées; et tous ces coefficiens seront entiers, si tous ceux qui sont représentés indéfiniment par h sont des nombres entiers. Si ensuite l'on substitue a^2, b^2, $c^2\ldots$ pour t, u, $v\ldots$ respectivement, le terme tel que $ht^{\alpha}u^{\beta}v^{\gamma}\ldots$ qui se réduisait à r^{λ}, se réduira par la nouvelle substitution, à $r^{2\lambda}$, desorte que l'on aura

$$\varphi(a^2, b^2, c^2, \ldots) = A + A'r^2 + A''r^4 + A'''r^6 + \ldots + A^{(\nu)}r^{2n-2}.$$

On aura de même en général, μ étant un nombre entier quelconque

$$\varphi(a^{\mu}, b^{\mu}, c^{\mu}\ldots) = A + A'r^{\mu} + A''r^{2\mu} + A'''r^{3\mu} \ldots + A^{(\nu)}r^{(n-1)\mu},$$

proposition extrêmement importante, et qui sert de base aux recherches que nous allons faire.

Il suit de là que

$\varphi(1, 1, 1, \ldots) = \varphi(a^n, b^n, c^n, \ldots) = A + A' + A'' \ldots + A^{\nu}$,

et que

$\varphi(a, b, c\ldots) + \varphi(a^2, b^2, c^2\ldots) + \varphi(a^3, b^3, c^3\ldots) + \text{etc.} + \varphi(a^n, b^n, c^n\ldots) = nA.$

Ainsi cette somme est toujours divisible par n, quand tous les coefficiens déterminés (tels que h), dans $\varphi(t, u, v\ldots)$ sont des nombres entiers.

341. THÉORÈME. *Si la fonction* X (*n°* 339) *est divisible par une fonction d'un degré inférieur*

$$P = x^{\lambda} + Ax^{\lambda-1} + Bx^{\lambda-2} + \text{etc.} + Kx + L,$$

les coefficiens A, B,...L *ne peuvent pas être tous entiers ni rationnels.*

Soit $X = PQ$, (π) l'ensemble des racines de l'équation $P = 0$, (χ) l'ensemble des racines de l'équation $Q = 0$, ensorte que Ω soit composé de (π) et de (χ); soit encore (ρ) l'ensemble des racines réciproques aux racines (π), et (σ) l'ensemble des racines réciproques aux racines (χ), et supposons que les racines contenues dans (ρ) soient données par l'équation $R = 0$, qui sera évidemment

$$x^{\lambda} + \frac{K}{L}x^{\lambda-1} + \text{etc.} + \frac{A}{L}x + \frac{1}{L} = 0,$$

tandis que les racines contenues dans (σ) seront données par l'équation $S = 0$. Il est manifeste que les racines (ρ) et (σ) prises ensemble composent Ω, et qu'ainsi l'on aura $RS = X$. Cela posé, nous avons quatre cas à distinguer :

1°. Quand (π) coïncide avec (ρ) et qu'on a parconséquent $P = R$. Dans ce cas les racines (π) seront réciproques deux à deux, et parconséquent P est le produit de $\frac{1}{2}\lambda$ facteurs doubles tels que

$$x^2 - 2x\cos\omega + 1 = (x - \cos\omega)^2 + \sin^2\omega,$$

d'où il suit que quel que soit x, pourvu qu'il soit réel, P obtiendra une valeur réelle positive. Soient

$$P' = 0, \quad P'' = 0, \quad P''' = 0, \ldots . P^{\nu} = 0$$

les équations qui donnent les quarrés, cubes, biquarrés, etc.,

$n-1$ puissances, des racines (π), et $p, p', p'', \ldots p^{\nu}$ les valeurs de $P, P', P'' \ldots P^{\nu}$ respectivement, quand on y fait $x=1$: par ce qui a été dit précédemment $p, p' \ldots p^{\nu}$ seront des quantités réelles et positives. Or p est la valeur qu'obtient la fonction

$$(1-t)(1-u)(1-\nu) \text{ etc.}$$

quand on y substitue pour t, u, ν, etc. les racines (π); p' est la valeur de cette même fonction, quand on substitue pour t, u, ν, etc. les quarrés de ces mêmes racines; et d'ailleurs la valeur qui résulte de la supposition $t=1$, $u=1$, $\nu=1$, etc., est évidemment $=0$; donc la somme $p+p'+p''+$ etc. $+p^{\nu}$ sera entière et divisible par n: en outre on voit facilement que le produit $PP'P'' \ldots = X^{\lambda}$, et partant $pp'p'' \ldots = n^{\lambda}$.

Maintenant si tous les coefficiens de P étaient rationnels, tous ceux de P', P'', etc. le seraient aussi, par le n° 338, et par le n° 42, ils seraient tous entiers; donc p, p', p'', etc. le seraient; comme d'ailleurs le produit de ces derniers nombres est n^{λ}, et que leur nombre est $n-1 > \lambda$, plusieurs d'entre eux devraient être égaux à 1, et les autres seraient égaux à n, ou à une puissance de n. Si donc il y en a g qui soient égaux à 1, on aura

$$p+p'+p''+\text{etc.} \equiv g \pmod{n},$$

et partant non-divisible par n. Donc la supposition ne peut subsister.

2°. Quand (π) et (ρ) ne coïncident pas, mais contiennent quelques racines qui leur sont communes, soit (τ) l'ensemble de ces racines, et $T=0$ l'équation qui les donnerait; il suit de la théorie des équations que T sera le plus grand commun diviseur des fonctions P et R. Or il est évident que les racines comprises dans (τ) sont réciproques deux à deux, d'où l'on conclura par ce qui a été démontré précédemment, que tous les coefficiens de T ne peuvent être rationnels. Mais cela arriverait nécessairement si tous les coefficiens de P et partant ceux de R étaient rationnels, comme on peut le voir par la nature de l'opération par laquelle on cherche le plus grand diviseur commun; donc cette supposition est absurde.

3°. Quand (χ) et (ρ) coïncident, ou du moins renferment des racines communes, on prouvera de la même manière, que tous les coefficiens de Q ne peuvent pas être rationnels; or ils le seraient nécessairement si ceux de P l'étaient; donc cette dernière supposition est impossible.

4°. Si enfin il n'y a aucune racine commune ni à (π) et (ρ), ni à (χ) et (σ), toutes les racines (π) coïncideront nécessairement avec les racines (σ), et les racines (χ) avec les racines (ρ), et partant on aura $P=S$, $Q=R$; donc

$$X=PQ=PR=(x^\lambda+Ax^{\lambda-1}+\ldots+Kx+L)\left(x^\lambda+\frac{K}{L}x^{\lambda-1}+\ldots+\frac{A}{L}x+\frac{1}{L}\right),$$

d'où résulte, en faisant $x=1$,

$$nL=(1+A+\ldots.+K+L)^2.$$

Or si tous les coefficiens de P étaient rationnels, ils seraient entiers (n° 42), partant ceux de R le seraient aussi; donc L, qui devrait diviser l'unité, dernier terme de X, ne pourrait être que ± 1, et il s'ensuivrait que $\pm n$ serait un quarré, ce qui est absurde, puisque n est un nombre premier.

Il suit évidemment de ce théorème, que, de quelque manière que l'on décompose X en facteurs, les coefficiens, ou du moins une partie d'entre eux, sont irrationnels, et parconséquent ne peuvent être déterminés que par des équations qui passent le premier degré.

342. Le but de nos recherches, qu'il n'est pas inutile d'annoncer ici en peu de mots, est de décomposer X *graduellement* en un nombre de facteurs de plus en plus grand, et cela de manière à ce que les coefficiens de ces facteurs puissent être déterminés par des équations du degré le plus bas possible, jusqu'à ce que, de cette manière, on parvienne à des facteurs simples, ou aux racines Ω. Nous ferons voir que si l'on décompose le nombre $p-1$ en facteurs entiers quelconques α, β, γ, etc. (pour lesquels on peut prendre les facteurs premiers), X est décomposable en α facteurs du degré $\frac{n-1}{\alpha}$, dont les coefficiens seront déterminés par une équation du degré α; que chacun de ces facteurs est décomposable en β facteurs du degré $\frac{n-1}{\alpha\beta}$, à l'aide d'une équation de

degré β, etc. Desorte que ν étant le nombre des facteurs α, β, γ, etc., la recherche des racines Ω est ramenée à la résolution de ν équations des degrés α, β, γ, etc.

Par exemple, pour $n=17$, on a $n-1=2.2.2.2$; il faut résoudre quatre équations du second degré; pour $n=73$, il faut en résoudre trois du second et deux du troisième.

Comme nous aurons souvent à considérer par la suite des puissances de r dont les exposans sont eux-mêmes des puissances, et que ces sortes d'expressions se prêtent difficilement à l'impression, nous userons de l'abréviation suivante pour r, r^2, r^3, etc. Nous écrirons $[1]$, $[2]$, $[3]$, etc. et généralement $[\lambda]$ pour r^λ, λ étant un nombre entier quelconque. Ces expressions ne sont pas entièrement déterminées, mais elles le deviennent lorsque l'on prend pour r ou $[1]$ une racine déterminée de Ω. Ainsi $[\lambda]$ et $[\mu]$ seront en général égaux ou inégaux, suivant que λ et μ seront congrus ou incongrus suivant le module n. En outre on a

$$[0]=1, \quad [\lambda].[\mu]=[\lambda+\mu], \quad [\lambda]^\mu=[\lambda\mu],$$

et.....$[0]+[\lambda]+[2\lambda]+[3\lambda]+$etc.$+[(n-1)\lambda]=0$, ou n, suivant que n est non-divisible ou divisible par n.

343. Si, pour le module n, g est un de ces nombres que (Section III) nous avons appelés *racines primitives*, les $n-1$ nombres $1, g, g^2, \ldots g^{n-2}$ seront congrus aux nombres $1, 2, 3, \ldots n-1$, suivant le module n, quoique l'ordre ne soit pas le même, c'est-à-dire que tout nombre de la première suite sera congru à un de ceux de la seconde. Il suit de là que les racines

$$[1], \quad [g], \quad [g^2], \ldots . [g^{n-2}]$$

coïncident avec Ω; et de même plus généralement

$$[\lambda], \quad [\lambda g], \quad [\lambda g^2], \ldots . [\lambda g^{n-2}]$$

coïncident avec Ω, si λ est un nombre entier quelconque, mais non-divisible par n. Et comme on a $g^{n-1}\equiv 1 \pmod{n}$, on voit sans peine que les deux racines $[\lambda g^\mu]$, $[\lambda g^\nu]$ sont identiques ou différentes, suivant que μ et ν sont congrus ou incongrus suivant le module $n-1$.

Si donc G est une autre racine primitive, les racines $[1]$, $[g],\ldots.[g^{n-2}]$ coïncideront ainsi avec les racines $[1]$, $[G],\ldots.$ $[G^{n-2}]$, abstraction faite de l'ordre. Mais en outre, on prouve facilement que si e est un diviseur de $n-1$, et qu'on pose $n-1=ef$, $g^e=h$, $G^e=H$, les f nombres

$$1,\ h,\ h^2,\ h^3,\ldots.h^{f-1}$$

sont congrus, suivant le module n, à ceux-ci :

$$1,\ H,\ H^2,\ H^3,\ldots.H^{f-1},$$

sans avoir égard à l'ordre. Supposons en effet $G\equiv g^\omega \pmod{n}$, et soit μ un nombre quelconque positif et $<f$, et ν le résidu *minimum* de $\mu\omega \pmod{f}$, on aura $\nu e\equiv\mu\omega e \pmod{n-1}$, donc

$$g^{\nu e}\equiv g^{\mu\omega e}\equiv g^{\mu e} \pmod{n} \quad \text{ou} \quad H^\mu\equiv h^\nu,$$

c'est-à-dire que tout nombre de la première suite 1, h, h^2, etc. est congru à un de ceux de la seconde 1, H, H^2, etc., et réciproquement.

Il suit de là évidemment qu'il y a identité entre les racines

$[1]$, $[h]$, $[h^2],\ldots.[h^{f-1}]$ et $[1]$, $[H]$, $[H^2],\ldots.[H^{f-1}]$,

ou plus généralement entre les racines

$[\lambda]$, $[\lambda h^2]$, $[\lambda h],\ldots[\lambda h^{f-1}]$ et $[\lambda]$, $[\lambda H]$, $[\lambda H^2],\ldots[\lambda H^{f-1}]$.

Nous désignerons par (f, λ) la *somme* de semblables racines, telle que

$$[\lambda]+[\lambda h]+[\lambda h^2]+\text{etc.}+[\lambda h^{f-1}];$$

et comme elle ne change pas, lorsque l'on prend pour g une autre racine primitive, elle doit être regardée comme indépendante de g, et l'*ensemble* de ces racines s'appellera *période* (f, λ), dans laquelle on ne considère pas l'ordre des racines (*).

Pour présenter une pareille période, il sera convenable de réduire chacune des racines qui la composent à sa plus simple expression, en remplaçant les nombres λ, λh, λh^2, etc. par leurs

(*) Nous pourrons dorénavant donner à la *somme* le nom de *valeur numérique de la période*, ou même celui de *période*, lorsqu'il n'y aura pas d'ambiguité à craindre.

résidus *minima*, suivant le module n; et si l'on veut, on peut ordonner les termes de la période suivant la grandeur de ces nombres.

Exemple. Pour $n=19$, 2 est racine primitive, et la période (6, 1) est composée des racines

$$[1],\ [8],\ [64],\ [512],\ [4096],\ [32768],$$
$$\text{ou}\ldots\ldots[1],\ [7],\ [8],\ [11],\ [12],\ [18];$$

de même la période (6, 2) est composée des racines

$$[2],\ [3],\ [5],\ [14],\ [16],\ [17];$$

la période (6, 3) coïncide avec la précédente, et la période (6, 4) contient les racines

$$[4],\ [6],\ [9],\ [10],\ [13],\ [15].$$

344. On remarquera, au sujet de ces périodes, les observations suivantes, qui se présentent d'elles-mêmes:

1°. Comme on a $\lambda h^f \equiv \lambda$, $\lambda h^{f+1} \equiv \lambda h$, etc. (mod. n), il est évident que les périodes

$$(f, \lambda),\ (f, \lambda h),\ (f, \lambda h^2),\ \text{etc.}$$

sont composées des mêmes racines, et généralement si λ' est une racine quelconque de (f, λ), cette période sera identique avec (f, λ'). Donc deux périodes, de même nombre de termes (que nous nommerons périodes *semblables*), seront identiques, si elles ont une seule racine commune, et parconséquent il est impossible que de deux racines contenues dans une certaine période, il ne s'en trouve qu'une seule dans une période semblable: et il est clair que si les racines $[\lambda]$, $[\lambda']$ appartiennent à la même période, la valeur de l'expression $\frac{\lambda'}{\lambda}$ (mod. n) sera congrue à une certaine puissance de h, ou que l'on peut supposer $\lambda' \equiv \lambda g^{ve}$ (mod. n).

2°. Si $f=n-1$, on a $e=1$, et la période $(f, 1)$ coïncide avec Ω; mais dans les autres cas Ω sera composé des e périodes $(f, 1)$, (f, g), (f, g^2), etc.,... (f, g^{e-1}), et comme ces périodes sont toutes différentes entre elles, il est clair que toute autre période semblable (f, λ) coïncide avec l'une d'elles, pourvu

pourvu que $[\lambda]$ soit une des racines Ω, c'est-à-dire, que λ ne soit pas divisible par n. Quant à la période (f, o) ou (f, kn), elle est évidemment composée de f unités. On voit même que si λ est un nombre quelconque non-divisible par n, l'ensemble des e périodes

$$(f, \lambda), (f, \lambda g), (f, \lambda g^2), (f, \lambda g^3) \ldots (f, \lambda g^{e-1})$$

coïncide encore avec Ω.

Ainsi, par exemple, pour $n=19$ et $f=6$, Ω est composé des trois périodes (6, 1), (6, 2), (6, 4), à une desquelles toute autre semblable, excepté (6, 0), peut être ramenée.

3°. Si $n-1$ est le produit des trois nombres positifs a, b, c, il est évident que toute période de bc termes est composée de b périodes dont chacune a c termes, c'est-à-dire que (bc, λ) est composée des périodes

$$(c, \lambda), (c, \lambda g^a), (c, \lambda g^{2a}), \ldots . (c, \lambda g^{ab-a});$$

c'est pourquoi nous dirons que ces dernières sont contenues dans (bc, λ).

Ainsi, pour $n=19$, la période (6, 1) est composée des trois (2, 1), (2, 8), (2, 7), dont la première contient les racines r, r^{18}; la seconde, r^8, r^{11}; la troisième, r^7, r^{12}.

345. Théorème. *Soient* (f, λ), (f, μ) *deux périodes semblables, identiques ou différentes, et* $[\lambda]$, $[\lambda']$, $[\lambda'']$, etc. *les racines qui composent* (f, λ); *le produit de* (f, λ) *par* (f, μ) *sera la somme des* f *périodes semblables, c'est-à-dire,*

$$= (f, \lambda+\mu) + (f, \lambda'+\mu) + (f, \lambda''+\mu), \text{ etc.} = W.$$

Soit comme plus haut $n-1=ef$, g une racine primitive pour le module n, et $h=g^e$, on aura par ce qui précède

$$(f, \lambda) = (f, \lambda h) = (f, \lambda h^2), \text{ etc.};$$

le produit cherché sera donc

$$[\mu].(f, \lambda) + [\mu h].(f, \lambda h) + [\mu h^2].(f, \lambda h^2) + \text{etc.},$$

et partant

$$[\lambda+\mu]+[\lambda h+\mu]+[\lambda h^2+\mu]\ldots\ldots+[\lambda h^{f-1}+\mu]$$
$$+[\lambda h+\mu h]+[\lambda h^2+\mu h]+[\lambda h^3+\mu h]\ldots\ldots+[\lambda h^f+\mu h]$$
$$+[\lambda h^2+\mu h^2]+[\lambda h^3+\mu h^2]+[\lambda h^4+\mu h^2]\ldots\ldots+[\lambda h^{f+1}+\mu h^2]$$
$$+\text{ etc.}$$

Cette expression contiendra en tout f^2 racines, et si l'on prend séparément la somme de chaque colonne verticale, on trouve que la somme totale est, comme nous l'avons annoncé, égale à

$$(f,\ \lambda+\mu)+(f,\ \lambda h+\mu)+(f,\ \lambda h^2+\mu)\ldots+(f,\ \lambda h^{f-1}+\mu);$$

or $\lambda' \equiv \lambda h$, $\lambda'' \equiv \lambda h^2$, etc., suivant le module n, et partant

$$\lambda'+\mu \equiv \lambda h+\mu,\quad \lambda''+\mu \equiv \lambda h^2+\mu,\ \text{etc.}$$

Nous joindrons à ce théorème les corollaires suivans :

1°. k étant un nombre entier quelconque, le produit de $(f, k\lambda)$ par $(f, k\mu)$ est

$$(f,\ k(\lambda+\mu))+(f,\ k(\lambda'+\mu))+(f,\ k(\lambda''+\mu))+\text{etc.}$$

2°. Comme les différentes parties qui composent W coïncident évidemment avec $(f,\ 0)=n$, on avec une des périodes

$$(f,\ 1),\quad (f,\ g),\quad (f,\ g^2)\ldots\ldots(f,\ g^{e-1}),$$

il est évident que W peut se ramener à la forme suivante :

$$W=af+b(f,\ 1)+b'(f,\ g)+b''(f,\ g^2)+\text{etc.}+b^{(\sigma)}(f,\ g^{e-1}),$$

où les coefficiens a, b, b', etc. sont entiers et positifs ou quelques-uns $=0$; et en outre, que le produit de $(f, k\lambda)$ par $(f, k\mu)$ devient alors

$$af+b(f,\ k)+b'(f,\ gk)+b''(f,\ g^2k)+\text{etc.}+b^{(\sigma)}(f,\ g^{e-1}k).$$

Ainsi, pour $n=19$, le produit de la somme $(6,\ 1)$ par elle-même, ou le quarré de cette somme, est

$$(6,\ 2)+(6,\ 8)+(6,\ 9)+(6,\ 12)+(6,\ 13)+(6,\ 19),$$

ou.....$6+2(6,\ 1)+(6,\ 2)+2(6,\ 4)$.

3°. Comme le produit de chacun des termes de W par une période semblable (f, ν) peut être ramené à une forme analogue, il est évident que le produit $(f, \lambda).(f, \mu).(f, \nu)$ peut être représenté par

$$cf + d(f, 1) + d'(f, g) + \text{etc.} + d^{(\sigma)}(f, g^{e-1});$$

c, d, d', etc. étant tous entiers et positifs, et qu'en outre, si k est entier, on a

$$(f, \lambda k).(f, \mu k).(f, \nu k) = cf + d(f, k) + \text{etc.} + d^{(\sigma)}(f, g^{e-1}k).$$

On étendra de la même manière ce théorème aux produits de tant de périodes semblables qu'on voudra, et il importe peu que ces périodes soient toutes différentes, ou en partie différentes, et en partie identiques, ou même toutes identiques.

4°. Il suit de là que si dans une fonction algébrique rationnelle et entière $F = \varphi(t, u, v \ldots)$, on substitue pour les indéterminées t, u, v, etc. respectivement, les périodes semblables (f, λ), (f, μ), (f, ν), etc., la valeur de cette fonction est toujours réductible à la forme

$$A + B(f, 1) + B'(f, g) + B''(f, g^2) \ldots + B^{(\sigma)}(f, g^{e-1}),$$

et que les coefficiens A, B, B', etc. seront tous entiers, si les coefficiens de la fonction F le sont eux-mêmes. Si ensuite on substitue pour t, u, v, etc. respectivement les périodes $(f, \lambda k)$, $(f, \mu k)$, $(f, \nu k)$, la valeur de F sera de la forme

$$A + B(f, k) + B'(f, kg) + \text{etc.}$$

346. Théorème. *Si l'on suppose que* λ *est un nombre non-divisible par* n, *et que pour abréger on fasse* $(f, \lambda) = p$, *toute autre période semblable* (f, μ) *où* μ *est aussi non-divisible par* n, *peut être mise sous la forme*

$$\alpha + \beta p + \gamma p^2 + \text{etc.} + \theta p^{e-1},$$

de manière que les coefficiens α, β, γ, $\ldots\theta$, *soient rationnels et déterminés.*

Désignons par p', p'', p''', etc. les périodes $(f, \lambda g)$, $(f, \lambda g^2)$, etc. jusqu'à $(f, \lambda g^{e-1})$, dont le nombre est $e-1$, et avec une desquelles (f, μ) coïncidera nécessairement. On aura sur-le-champ l'équation

$$0 = 1 + p + p' + p'' + p''' + \text{etc.} \ldots\ldots\ldots\ldots (\text{I}),$$

et en formant, d'après le n° précédent, les puissances de p jusqu'à p^{e-1}, on aura les $e-2$ autres équations

$$0 = p^2 + A + ap + a'p' + a''p'' + a'''p''' + \text{etc.}\ldots\text{(II)}$$
$$0 = p^3 + B + bp + b'p' + b''p'' + b'''p''' + \text{etc.}\ldots\text{(III)}$$
$$0 = p^4 + C + cp + c'p' + c''p'' + c'''p''' + \text{etc.}\ldots\text{(IV)},$$
$$\text{etc.}$$

où tous les coefficiens A, a, a', etc., B, b, b', etc., etc. sont entiers et indépendans de λ, ainsi qu'on peut le conclure du n° précédent; c'est-à-dire, que les mêmes équations auront lieu quelle que soit la valeur que l'on donne à λ: cette remarque s'étend à l'équation (I), pourvu que λ ne soit pas divisible par n.

Supposons maintenant $(f, \mu) = p'$; si (f, μ) était égale à une autre des périodes p'', p''', etc., il est évident que l'on pourrait employer des raisonnemens analogues. Comme le nombre des équations (I), (II), (III), etc. est $e-1$, les quantités p'', p''', etc., dont le nombre est $e-2$, pourront être éliminées de manière à ce qu'on ait une équation telle que

$$0 = A' + B'p + C'p^2 + \text{etc.} + M'p^{e-1} + N'p' \ldots\ldots (Z),$$

dans laquelle A', B', $\ldots N'$ sont entiers et ne sont pas tous nuls à-la-fois. Or si N' n'est pas $= 0$, il est clair que cette équation donnera pour p' une valeur de la forme annoncée; ainsi il ne nous reste plus qu'à démontrer que l'on ne peut avoir $N' = 0$.

En supposant $N' = 0$, l'équation Z devient

$$M'p^{e-1} + \text{etc.} + C'p^2 + B'p + A' = 0,$$

à laquelle ne peut satisfaire au plus qu'un nombre $e-1$ de valeurs de p. Mais comme les équations dont on a tiré Z sont indépendantes de λ, il est clair que l'équation Z elle-même ne dépend pas de λ, c'est-à-dire qu'elle a lieu pour toute valeur de λ entière et non-divisible par n. Cette équation sera donc satisfaite par les valeurs des e périodes

$$(f, 1),\ (f, g),\ (f, g^2), \ldots (f, g^{e-1});$$

d'où il suivrait que les valeurs de deux de ces périodes au moins seraient égales entre elles. Supposons qu'elles contiennent respectivement les racines

$$[\zeta],\ [\zeta'],\ [\zeta''],\ \text{etc.};\quad [\eta],\ [\eta'],\ [\eta''],\ \text{etc.},$$

et que les nombres ζ, ζ', ζ'', etc., η, η', η'', etc. soient positifs et $<n$, ce qui est permis; il est évident qu'ils seront tous différens, et qu'aucun d'eux ne sera $=0$. Désignons par Y la fonction

$$x^{\zeta}+x^{\zeta'}+x^{\zeta''}+\text{etc.}-x^{\eta}-x^{\eta'}-x^{\eta''}-\text{etc.},$$

dont le terme le plus élevé ne surpassera pas x^{n-1}; il est clair qu'on aurait $Y=0$, si l'on faisait $x=[1]$; donc Y contiendrait le facteur $x-[1]$, qui lui serait *commun* avec la fonction déjà désignée par X (n° 339): or il est facile de démontrer l'absurdité de cette dernière supposition. En effet, si X et Y avaient un diviseur commun, il s'ensuivrait, par la nature de l'opération, qui sert à chercher le plus grand commun diviseur de deux fonctions semblables dont les coefficiens sont rationnels, que ce plus grand commun diviseur aurait tous ses coefficiens rationnels; car il est d'ailleurs évident qu'il ne peut être du degré $n-1$, puisque Y est divisible par x. Mais nous avons fait voir (n° 341) que X ne peut être divisible par une fonction de degré inférieur à $n-1$, dont les coefficiens soient rationnels; donc on ne peut supposer que l'on ait $N'=0$.

Exemple. Pour $n=19$ et $f=6$, on a

$$0=1+p+p'+p'', \qquad p^2=6+2p+p'+2p'',$$

d'où l'on tire.....$p'=4-p^2$, $\qquad p''=-5-p+p^2$;

ainsi

$$(6,2)=4-(6,1)^2;\quad (6,4)=-5-(6,1)+(6,1)^2$$
$$(6,4)=4-(6,2)^2;\quad (6,1)=-5-(6,2)+(6,2)^2$$
$$(6,1)=4-(6,4)^2;\quad (6,2)=-5-(6,4)+(6,4)^2.$$

347. THÉORÈME. *Si* $F=\varphi(t,u,v...)$ *est une fonction* invariable (*) *algébrique rationnelle et entière de* f *indéterminées* t, u, v, *etc., et qu'en substituant à la place de ces indéterminées les* f *ra-*

(*) On appelle fonctions *invariables* celles où toutes les indéterminées entrent de la même manière, ou plus clairement, celles qui ne changent pas, de quelque manière que les indéterminées soient permutées entre elles; telles sont la somme des indéterminées, leur produit, la somme de leurs produits deux à deux, etc.

cines contenues dans la période (f, λ), *on ramène cette fonction à la forme*

$$A + A'[1] + A''[2] + etc. = W,$$

d'après ce qui a été dit (*n°* 340); *les racines qui, dans cette expression, appartiendront à une même période quelconque de* f *termes, auront des coefficiens égaux.*

Soient $[p]$, $[q]$ deux racines qui appartiennent à une même période, et supposons p et q positifs et moindres que n; il s'agit de démontrer que $[p]$ et $[q]$ auront dans W le même coefficient. Soit encore $q \equiv pg^{\nu e} \pmod{n}$, et nommons $[\lambda]$, $[\lambda']$, $[\lambda'']$, etc.; les racines contenues dans (f, λ), où nous supposons λ, λ', λ'', etc. positifs et moindres que n; soient enfin μ, μ', μ'', etc. les résidus *minima* positifs des nombres $\lambda g^{\nu e}$, $\lambda' g^{\nu e}$, $\lambda'' g^{\nu e}$, etc. suivant le module n; μ, μ', etc. seront évidemment identiques avec λ, λ', etc., si l'on ne fait pas attention à l'ordre. Or il suit du n° 340, que la fonction

$$\varphi\{[\lambda g^{\nu e}], [\lambda' g^{\nu e}], [\lambda'' g^{\nu e}], \ldots\} \qquad (I)$$

peut être ramené à la forme

$$A + A'[g^{\nu e}] + A''[2g^{\nu e}] + \text{etc. ou } A + A'[\theta] + A''[\theta'] + \text{etc.} = W';$$

en désignant par θ, θ', θ'', etc. les résidus *minima* des nombres $g^{\nu e}$, $2g^{\nu e}$, etc. suivant le module n; il est évident, d'après cela, que $[q]$ aura dans W' le même coefficient que $[p]$ dans W. Mais on voit sans peine que le développement de l'expression (I) donne le même résultat que le développement de l'expression

$$\varphi\{[\mu], [\mu'], [\mu''], \text{etc.}\},$$

puisque $\mu \equiv \lambda g^{\nu e}$, $\mu' \equiv \lambda' g^{\nu e}$, etc. (mod. n); mais cette expression donne le même résultat que

$$\varphi\{[\lambda], [\lambda'], [\lambda''], \text{etc.}\},$$

parceque les nombres μ, μ', μ'', etc. ne diffèrent des nombres λ, λ', λ'', etc. que relativement à l'ordre, qui n'influe en rien

dans une fonction invariable; donc W' et W seront identiques, et partant $[p]$ et $[q]$ auront même coefficient dans W.

Il suit évidemment de là que W peut être ramené sous la forme

$$A+a(f,\,1)+a'(f,\,g)+a''(f,\,g^2)+\text{etc.}+a^{(\varepsilon)}(f,\,g^{\varepsilon-1}):$$

les coefficiens A, a, a', etc. seront entiers et déterminés, si tous les coefficiens de F sont rationnels et entiers.

Ainsi, par exemple, si $n=19$, $f=6$ et $\lambda=1$, et que la fonction φ désigne la somme des produits des indéterminées prises deux à deux, sa valeur se ramène à

$$3+(6,\,1)+(6,\,4).$$

De plus, il est facile de voir que si l'on substitue ensuite pour t, u, v, etc. les racines d'une autre période $(f,\,k\lambda)$, la valeur de F devient

$$A+a(f,\,k)+a'(f,\,kg)+a''(f,\,kg^2),\ \text{etc.}$$

348. Comme dans toute équation

$$x^f-\alpha x^{f-1}+\beta x^{f-2}-\gamma x^{f-3}+\text{etc.}=0$$

les coefficiens α, β, γ, etc. sont des fonctions invariables des racines, savoir, α la somme, β la somme des produits des racines prises deux à deux, γ la somme des produits trois à trois, etc.; il en résulte que dans l'équation qui donne les racines contenues dans la période $(f,\,\lambda)$, le premier coefficient sera $(f,\,\lambda)$, et chacun des autres pourra être ramené à la forme

$$A+a(f,\,1)+a'(f,\,g)+a''(f,\,g^2)+\text{etc.}+a^{(\varepsilon)}(f,\,g^{\varepsilon-1}),$$

où A, a, a', etc. sont des entiers. D'ailleurs il est clair que l'équation qui donnerait les racines que contient toute autre période $(f,\,\lambda k)$ se déduirait de celle-là, si dans chacun des coefficiens on substituait $(f,\,k)$ pour $(f,\,1)$, $(f,\,kg)$ pour (f,g), et généralement $(f,\,kp)$ pour $(f,\,p)$. On pourra donc de cette manière assigner un nombre e d'équations

$$z=0,\quad z'=0,\quad z''=0,\ \text{etc.}$$

qui donneront respectivement les racines contenues dans les périodes

$$(f,\,1),\quad (f,\,g),\quad (f,\,g^2),\ \text{etc.};$$

aussitôt que l'on connaîtra les sommes $(f, 1)$, (f, g), (f, g^2), etc., ou même, que l'on en connaîtra une seule, puisque (n° 346), la valeur de chacune d'elles peut s'exprimer rationnellement en fonction d'une seule. Cela fait, la fonction X sera décomposée en e facteurs du degré f: le produit des fonctions z, z', z'', etc. sera évidemment $= X$.

Exemple. Pour $n = 19$, la somme de toutes les racines contenues dans la période $(6, 1)$ est $= (6, 1) = \alpha$; la somme des produits deux à deux est $= 3 + (6, 1) + (6, 4) = \beta$; la somme des produits trois à trois est $= 2 + 2(6, 1) + (6, 2) = \gamma$; la somme des produits quatre à quatre est $= 3 + (6, 1) + (6, 4,) = \delta$; la somme des produits cinq à cinq est $= (6, 1) = \varepsilon$; le produit de toutes $= 1$; donc l'équation

$$z = x^6 - \alpha x^5 + \beta x^4 + \gamma x^3 + \delta x^2 - \varepsilon + 1 = 0$$

donnera toutes les racines contenues dans la période $(6, 1)$. Si, dans les coefficiens α, β, γ, etc. on substitue

$$(6, 2),\ (6, 4),\ (6, 1) \quad \text{pour} \quad (6, 1),\ (6, 2),\ (6, 4)$$

respectivement, il en résulte l'équation $z' = 0$, qui donnera les racines contenues dans $(6, 2)$; si l'on fait dans celle-ci le même changement, on a l'équation $z'' = 0$, qui donnera les racines contenues dans $(6, 4)$, et le produit $zz'z''$ sera égal à X.

349. Il est souvent plus commode, surtout quand f est un grand nombre, de déduire les coefficiens α, β, γ, etc., des sommes des puissances des racines. Il est évident que la somme des quarrés des racines contenues dans (f, λ) est $= (f, 2\lambda)$, que la somme des cubes est $= (f, 3\lambda)$, etc.; ainsi en faisant pour abréger,

$$(f, \lambda) = q, \quad (f, 2\lambda) = q', \quad (f, 3\lambda) = q'', \text{ etc.},$$

on aura

$$\alpha = q, \quad 2\beta = \alpha q - q', \quad 3\gamma = \beta q - \alpha q' + q'', \text{ etc.};$$

expressions dans lesquelles on doit convertir sur-le-champ (n° 345), les produits de deux périodes en sommes de périodes. Ainsi, dans notre exemple, si l'on fait pour abréger,

$$(6, 1) = p, \quad (6, 2) = p', \quad (6, 4) = p'',$$

on trouve $q = p$, $q' = q'' = q^{IV} = p'$, $q''' = q^{V} = p''$;

donc

donc $\alpha = p$,

$2\beta = p^2 - p' = 6 + 2p + 2p''$,

$3\gamma = (3 + p + p'')p - pp' + p' = 6 + 6p + 3p'$,

$4\delta = (2 + 2p + p')p - (3 + p + p'')p' + pp' - p'' = 12 + 4p + 4p''$,

etc.

Au reste, il suffit de calculer de cette manière la moitié des coefficiens, car on prouve sans difficulté que les derniers sont égaux aux premiers dans l'ordre inverse, savoir le dernier $= 1$, l'avant-dernier $= \alpha$, l'antépénultième $= \beta$, etc.; ou qu'ils s'en déduisent en substituant pour $(f, 1)$, (f, g), etc., les périodes $(f, -1)$, $(f, -g)$, etc., c'est-à-dire $(f, n-g)$, $(f, n-1)$. Le premier cas a lieu quand f est pair, le second quand f est impair; mais le dernier coefficient est toujours $= 1$. Cette propriété se tire du théorème du n° 79, mais nous sommes forcés de ne pas nous arrêter sur ce sujet.

350. THÉORÈME. *Si* $n - 1$ *est le produit de trois nombres entiers positifs* α, β, γ, *et que la période* $(\beta\gamma, \lambda)$, *qui a* $\beta\gamma$ *termes, soit composée de* β *périodes* (γ, λ), (γ, λ'), (γ, λ''), *etc., dont chacune a* γ *termes; si de plus, en substituant les sommes* (γ, λ), (γ, λ'), (γ, λ''), *etc. à la place de* t, u, v, *etc., dans une fonction* $F = \varphi(t, u, v\ldots)$ *telle qu'au n° 347, elle se réduit à* $A + a(\gamma, 1) + a'(\gamma, g) \ldots a + {}^{(\zeta)}(\gamma, g^{\alpha\beta-\alpha}) \ldots + a^{(\theta)}(\gamma, g^{\alpha\beta-1}) = W$; *en supposant d'ailleurs que* F *soit une fonction invariable; les périodes comprises dans* (W), *qui appartiendront à une même période de* $\beta\gamma$ *termes, c'est-à-dire, en général celles qui seront telles que* (γ, g^{μ}) et $(\gamma, g^{\alpha\nu+\mu})$, ν *étant un entier quelconque, auront nécessairement les mêmes coefficiens.*

La période $(\beta\gamma, \lambda g^{\alpha})$ étant identique avec la période $(\beta\gamma, \lambda)$, les périodes plus petites $(\gamma, \lambda g^{\alpha})$, $(\gamma, \lambda' g^{\alpha})$, $(\gamma, \lambda'' g^{\alpha})$, etc. dont la première est évidemment composée, doivent coïncider avec celles qui composent la seconde, abstraction faite de l'ordre. Si donc on suppose que par la substitution de ces périodes à la place des indéterminées t, u, v, etc., le facteur F se change en W', W' devra coïncider avec W. Mais (n° 347) on a

$$W' = A + a(\gamma, g^{\alpha}) + a'(\gamma, g^{\alpha+1}) \ldots + a^{(\zeta)}(\gamma, g^{\alpha\beta}) \ldots + a^{(\theta)}(\gamma, g^{\alpha\beta+\alpha-1})$$
$$= A + a(\gamma, g^{\alpha}) + a'(\gamma, g^{\alpha+1}) \ldots + a^{(\zeta)}(\gamma, 1) \ldots + a^{(\theta)}(\gamma, g^{\alpha-1}).$$

Ainsi, puisque cette expression doit coïncider avec W, le premier coefficient de W (en commençant par a) devra être identique avec le $\alpha+1^{ème}$, le second avec le $\alpha+2^{ème}$, le troisième avec le $\alpha+3^{ème}$, etc., et généralement les coefficiens des périodes

$$(\gamma, g^{\mu}), (\gamma, g^{\alpha+\mu}), (\gamma, g^{2\alpha+\mu}), \ldots\ldots (\gamma, g^{\nu\alpha+\mu}),$$

qui sont les

$$\mu+1^{ème}, \alpha+\mu+1^{ème}, 2\alpha+\mu+1^{ème}, \ldots \nu\alpha+\mu+1^{ème}$$

respectivement, devront être identiques.

Il suit de là évidemment que W peut être ramené à la forme

$$A + a(\beta\gamma, 1) + a'(\beta\gamma, g) + \ldots\ldots + a^{(\varepsilon)}(\beta\gamma, g^{\alpha-1}),$$

où tous les coefficiens A, a, etc. seront entiers, si tous ceux de F le sont. On voit en outre que si l'on substitue dans F à la place des indéterminées, les β périodes de γ termes qui constituent une autre période de $\beta\gamma$ termes, telle par exemple que $(\beta\gamma, \lambda k)$, périodes qui sont $(\gamma, \lambda k)$, $(\gamma, \lambda' k)$, $(\gamma, \lambda'' k)$, etc., la valeur qui en résulte est

$$A + a(\beta\gamma, k) + a'(\beta\gamma, gk) \ldots\ldots + a^{(\varepsilon)}(\beta\gamma, g^{\alpha-1}k).$$

Au reste, il est clair que ce théorème s'étend aussi au cas où $\alpha = 1$, c'est-à-dire, où $\beta\gamma = n - 1$. Alors tous les coefficiens de W sont égaux, et V se ramènera à la forme

$$A + a(\beta\gamma, 1).$$

351. Ainsi, en conservant la notation du n° précédent, on conclura que les différens coefficiens de l'équation qui donnerait les β sommes (γ, λ), (γ, λ'), (γ, λ''), etc. peuvent être mis sous la forme

$$A + a(\beta\gamma, 1) + a'(\beta\gamma, g) + \ldots\ldots + a^{(\varepsilon)}(\beta\gamma, g^{\alpha-1}),$$

et que les nombres A, a, etc. seront entiers. Or l'équation qui donnerait les β périodes de γ termes qui composent une autre période $(\beta\gamma, k\lambda)$, se déduira de la première, en remplaçant dans tous les coefficiens la période quelconque $(\beta\gamma, \mu)$ par $(\beta\gamma, k\mu)$.

Si donc $\alpha = 1$, les β périodes de γ termes se détermineront par une équation de degré β, dont les coefficiens peuvent être mis sous la forme $A + a(\beta\gamma, 1)$, et sont parconséquent des quantités connues. Si $\alpha > 1$, les coefficiens de l'équation dont les racines sont toutes les périodes de γ termes contenues dans une période donnée de $\beta\gamma$ termes, seront des quantités connues, dès que l'on connaîtra les valeurs numériques des périodes de $\beta\gamma$ termes.

Au reste le calcul devient souvent plus facile, surtout quand β n'est pas un petit nombre, en calculant d'abord les sommes des puissances des racines, et en déduisant les coefficiens par le théorème de Newton, comme ci-dessus, n° 349.

Exemple I. On demande pour $n = 19$, l'équation dont les racines sont les sommes $(6, 1)$, $(6, 2)$, $(6, 4)$.

Désignons ces racines par p, p', p'' respectivement, et l'équation cherchée, par

$$x^3 - Ax^2 + Bx - C = 0;$$

on aura

$$A = p + p' + p'', \quad B = pp' + pp'' + p'p'', \quad C = pp'p'';$$

donc $A = (18, 1) = -1$; or on a

$$pp' = p + 2p' + 3p'', \quad pp'' = 2p + 3p' + p'', \quad p'p'' = 3p + p' + 2p'';$$

donc $B = 6(p + p' + p'') = 6(18, 1) = -6$;

enfin $C = (p + 2p' + 3p'')p'' = 3(6, 0) + 11(18, 1) = 18 - 11 = 7$;

donc l'équation cherchée est

$$x^3 + x^2 - 6x - 7 = 0.$$

En employant l'autre méthode, nous avons

$$p + p' + p'' = -1;$$

$$p^2 = 6 + 2p + p' + 2p'', \; p'^2 = 6 + 2p' + p'' + 2p, \; p''^2 = 6 + 2p'' + p + 2p';$$

d'où..... $p^2 + p'^2 + p''^2 = 18 + 5(p + p' + p'') = 13.$

De même.. $p^3 + p'^3 + p''^3 = 36 + 34(p + p' + p'') = 2.$

De là, à l'aide du théorème de Newton, on tire la même équation que ci-dessus.

Exemple 2. On demande pour $n = 19$, l'équation dont les racines sont les sommes $(2, 1)$, $(2, 7)$, $(2, 8)$.

Désignons-les par q, q', q'' respectivement, on aura

$$q+q'+q''=(6,1),\ qq'+qq''+q'q''=(6,1)+(6,4),\ qq'q''=2+(6,2);$$

donc en conservant la notation de l'exemple précédent, l'équation cherchée sera

$$x^3-px^2+(p+p'')x-2-p'=0.$$

L'équation dont les racines sont les sommes $(2,2)$, $(2,3)$, $(2,5)$ contenues dans $(6,2)$, se déduit de la précédente, en substituant p', p'', p pour p, p', p'' respectivement; et en faisant encore une fois la même substitution, on obtient l'équation dont les racines sont les sommes $(2,4)$, $(2,6)$, $(2,9)$ contenues dans $(6,4)$.

352. Les théorèmes précédens, avec leurs corollaires, contiennent les bases principales de toute la théorie, et le moyen de trouver les racines Ω peut s'exposer maintenant en peu de mots.

On doit, avant tout, prendre un nombre g qui soit racine primitive pour le module n, et trouver les résidus *minima* des puissances de g jusqu'à g^{n-2}. On décomposera $n-1$ en facteurs, et même en facteurs premiers, si l'on veut réduire le problème à des équations du degré le plus simple possible. Soient α, β, γ, ... ζ les facteurs de $n-1$, et soit fait

$$\frac{n-1}{a}=\beta\gamma\ldots.\zeta=a,\ \frac{n-1}{a\beta}=\gamma\ldots.\zeta=b,\ \text{etc.}$$

On distribuera les racines Ω en α périodes de a termes; chacune de celles-ci en β périodes de b termes; chacune de ces dernières en γ périodes, etc. On cherchera, par le n° 350, l'équation (A) de degré α qui aura pour racines ces α sommes de a termes, sommes dont on connaîtra les valeurs par la résolution de cette équation.

Mais il se présente ici une difficulté; car on ne voit pas à quelles périodes on doit égaler chaque racine de l'équation (A), c'est-à-dire, quelle est la racine qui doit être représentée par $(a,1)$, quelle est celle qui doit être représentée par (a,g), etc. On remédiera à cet inconvénient de la manière suivante. On peut désigner par $(a,1)$, une racine quelconque de l'équation (A); en effet, comme une racine quelconque de l'équation (A) est la somme de a racines Ω, et qu'il est absolument indifférent que

l'on ait représenté par [1] telle racine de Ω plutôt que telle autre, on sera libre de supposer que [1] soit une des racines qui constituent une racine quelconque donnée de l'équation (A), desorte qu'alors cette racine de l'équation (A) deviendra $(a, 1)$. Mais la racine [1] n'est pas encore par-là tout-à-fait déterminée, et le choix de celle des racines comprises dans $(a, 1)$ que nous prendrons pour [1], est absolument arbitraire. Au reste, une fois que $(a, 1)$ est déterminé, toutes les autres sommes de a racines peuvent en être déduites rationnellement (n° 346); d'où il suit qu'il n'y a qu'une racine de l'équation (A) qu'il soit nécessaire de trouver. On peut aussi employer pour faire cette distinction, la méthode suivante qui est moins directe. On prendra pour [1] une racine indéterminée, c'est-à-dire, qu'on fera

$$[1]=\cos\frac{kP}{n}+i\sin\frac{kP}{n},$$

l'entier k étant pris à volonté, pourvu qu'il ne soit pas divisible par n. Alors [2], [3], etc. indiquent des racines déterminées, et parconséquent $(a, 1)$, (a, g), etc. Si par les tables des sinus on calcule ces quantités, seulement avec assez de précision pour pouvoir décider quelles sont les plus grandes et les plus petites, il ne restera plus de doute sur la distinction à faire entre les racines de l'équation (A).

Quand on aura trouvé de cette manière les α sommes de a racines, on cherchera (n° 350) l'équation (B), dont les racines sont les β sommes de b termes contenues dans $(a, 1)$; les coefficiens de cette équation seront des quantités connues. Comme il y a encore de l'indétermination dans le choix de celle des racines contenues dans $(a, 1)$, que l'on désignera par [1], toute racine de l'équation (B) peut être représentée par $(b, 1)$, parceque l'on peut évidemment supposer qu'une des racines qui la compose soit désignée par [1]. On cherchera donc une racine quelconque de l'équation (B) par sa résolution; on la supposera égale à $(b, 1)$, et on en déduira, par le n° 346, toutes les autres sommes de b racines. De cette manière, nous avons un moyen de vérifier le calcul, puisque les périodes de b racines qui appartiennent à une même période de a termes, doivent produire des sommes que l'on connaît. Dans quelques cas, il est aussi expéditif de former

les $\alpha - 1$ autres équations de degré β, dont les racines sont respectivement les β différentes périodes de b termes contenues dans les autres périodes de a termes (a, g), (a, g^{α}), etc., et de chercher par la résolution les racines de l'équation (B) et de ces différentes équations. Mais alors il faudra, comme plus haut, décider à l'aide de la table de sinus, à quelles périodes de b termes doivent être égalées les racines qui en résultent. Au reste, il existe encore pour cette détermination différens autres artifices, que nous ne pouvons pas expliquer ici complétement. On pourra seulement dans les exemples suivans, remarquer un de ces procédés, pour le cas où $\beta = 2$, qui est le plus utile, et qui sera mieux connu par des exemples que par des préceptes.

Quand on aura trouvé de cette manière les valeurs de $\alpha\beta$ périodes de b termes, on déterminera de même par des équations de degré γ les $\alpha\beta\gamma$ périodes de c termes, et cela par deux procédés : 1°. en formant (n° 350) une équation du degré γ dont les racines soient les γ périodes de c termes qui composent $(b, 1)$, cherchant une des racines de cette équation, l'égalant à $(c, 1)$, et déduisant de là (n° 346) toutes les autres périodes semblables ; 2°. en formant les $\alpha\beta$ équations de degré γ, dont les racines sont respectivement les γ périodes de c termes qui sont contenues dans les différentes périodes de b termes, résolvant toutes ces différentes équations, et déterminant l'ordre des racines, comme plus haut, par les tables de sinus, ou comme dans les exemples suivans, si $\gamma = 2$.

En continuant de cette manière, on parviendra enfin nécessairement à connaître les $\frac{n-1}{\zeta}$ périodes de ζ termes. Cherchant donc par le n° 348, l'équation de degré ζ qui donne le ζ racines de Ω contenues dans $(\zeta, 1)$, les coefficiens de cette équation seront des quantités connues ; et si l'on tire une seule racine par la résolution, en faisant cette racine $= [1]$, ses puissances donneront toutes les racines Ω. Si on le préfère, on peut chercher toutes les racines de cette équation, et la résolution de $\frac{n-1}{\zeta} - 1$ autres équations semblables, donnera toutes les racines Ω.

Au reste, il est clair que dès qu'on a résolu l'équation (A), c'est-à-dire, dès qu'on a les valeurs des α périodes de a termes,

on est parvenu à décomposer la fonction X en α facteurs de a dimensions; de la résolution de l'équation (B), suit la décomposition de chacun de ces facteurs en β, et partant, celle de X en $\alpha\beta$ facteurs de b dimensions; etc.

353. *Exemple* 1. *Pour* $n = 19$.

Comme on a ici $n - 1 = 3.3.2$, la recherche des racines Ω doit pouvoir se ramener à la solution de deux équations du troisième degré et d'une du second. Cet exemple se comprendra d'autant plus facilement, que les opérations nécessaires sont contenues pour la plus grande partie dans ce qui précède. En prenant 2 pour la racine primitive g, on trouve

pour les puissances 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17,

les résidus *minima* 1, 2, 4, 8, 16, 13, 7, 14, 9, 18, 17, 15, 11, 3, 6, 12, 5, 10.

De là, par les nos 344, 345, on déduit facilement la distribution suivante de toutes les racines Ω en trois périodes de six termes, et de chacune de ces périodes en trois autres de deux termes.

$$\Omega = (18,1)\ldots\ldots \begin{cases} (6,1) \begin{cases} (2,1)\ldots\ldots[1],[18] \\ (2,8)\ldots\ldots[8],[11] \\ (2,7)\ldots\ldots[7],[12] \end{cases} \\ (6,2) \begin{cases} (2,2)\ldots\ldots[2],[17] \\ (2,16)\ldots\ldots[3],[16] \\ (2,14)\ldots\ldots[5],[14] \end{cases} \\ (6,4) \begin{cases} (2,4)\ldots\ldots[4],[15] \\ (2,13)\ldots\ldots[6],[13] \\ (2,9)\ldots\ldots[9],[10]. \end{cases} \end{cases}$$

L'équation (A) dont les racines sont les sommes (6, 1), (6, 2), (6, 4) se trouve être (*Voy.* n° 351, *ex.* 1.)

$$x^3 + x^2 - 6x + 7 = 0,$$

et une de ses racines $= -1{,}2218761623$; en exprimant cette racine par (6, 1), on trouve

$$(6,2)=4-(6,1)^2=2{,}507018644\,1\;;$$
$$(6,4)=-5-(6,1)+(6,1)^2=-2{,}285142481\,8.$$

Donc, si l'on substitue ces valeurs dans les formules du n° 348, X sera décomposé en facteurs du sixième degré.

L'équation (B), qui a pour racines les sommes $(2,1)$, $(2,7)$, $(2,8)$ est (n° 351, *ex.* 2),

$$x^3-(6,1)x^2+\{(6,1)+(6,4)\}x-2-(6,2)=0,$$

ou....$x^3+1{,}221876162\,3x^2-3{,}507018644\,1x-4{,}507018644\,1=0.$

On trouve pour une de ses racines $x=-1{,}354563143\,3$; nous l'exprimerons par $(2,1)$, et si l'on fait pour abréger $(2,1)=q$ on aura (n° 346)

$(2,2)=q^2-2$, $(2,3)=q^3-3q$,
$(2,4)=q^4-4q^2+2$, $(2,5)=q^5-5q^3+5q$,
$(2,6)=q^6-6q^4+9q^2-2$, $(2,7)=q^7-7q^5+14q^3-7q$,
$(2,8)=q^8-8q^6+20q^4-16q^2+2$, $(2,9)=q^9-9q^7+27q^5-30q^3+9q$.

On peut, dans le cas actuel, trouver ces valeurs plus commodément, de la manière suivante :

Supposons $$[1]=\cos\frac{kP}{19}+i\sin\frac{kP}{19};$$

on aura

$$[18]=\cos\frac{18kP}{19}+i\sin\frac{18kP}{19}=\cos\frac{kP}{19}-i\sin\frac{kP}{19};$$

et partant

$$(2,1)=2\cos\frac{kP}{19}:$$

on a de même en général,

$$[\lambda]=\cos\frac{\lambda kP}{19}+i\sin\frac{\lambda kP}{19},$$

et partant

$$(2,\lambda)=[\lambda]+[18\lambda]=[\lambda]+[-\lambda]=2\cos\frac{\lambda kP}{19}.$$

Si donc $\frac{1}{2}q=\cos\omega$, il en résulte

$$(2,2)=2\cos 2\omega,\qquad (2,3)=2\cos 3\omega,\quad \text{etc.};$$

d'où, par les équations connues qui donnent les cosinus des arcs multiples, on tirera les mêmes formules que ci-dessus. Ces formules donneront les valeurs numériques suivantes :

(2, 2)

$(2, 2) = -0{,}1651586909$, $(2, 6) = 0{,}4909709743$,
$(2, 3) = 1{,}5782810188$, $(2, 7) = -1{,}7589475024$,
$(2, 4) = -1{,}9727226068$, $(2, 8) = 1{,}8916344834$,
$(2, 5) = 1{,}0938963162$, $(2, 9) = 0{,}8033908493$.

Les valeurs de $(2, 7)$, $(2, 8)$, peuvent aussi se tirer de l'équation (B) dont elles sont les deux autres racines, et l'on déterminera laquelle des deux appartient à $(2, 7)$ et laquelle appartient à $(2, 8)$, ou par un calcul approché d'après les formules suivantes, ou par les tables des sinus, qui, avec une légère attention, prouvent que si l'on fait $\omega = \frac{7P}{19}$, on a $(2, 1) = \cos\omega$; donc il faut faire

$$(2, 7) = 2\cos\frac{49}{19}P = 2\cos\frac{8P}{19}, \quad \text{et} \quad (2, 8) = 2\cos\frac{56}{19}P = 2\cos\frac{P}{19}.$$

Les sommes $(2, 2)$, $(2, 3)$, $(2, 5)$ se trouveront de même par l'équation

$$x^3 - (6, 2)x^2 + \{(6, 1) + (6, 2)\}x - 2 - (6, 4) = 0,$$

dont elles sont les racines, en levant d'ailleurs l'incertitude; comme nous venons de le faire. Les sommes $(2, 4)$, $(2, 6)$, $(2, 9)$ se trouveront par l'équation

$$x^3 - (6, 4)x^2 + \{(6, 2) + (6, 4)\}x - 2 - (6, 1) = 0.$$

Enfin [1] et [18] sont racines de l'équation

$$x^2 - (2, 1)x + 1 = 0,$$

dont l'une est

$$x = \tfrac{1}{2}(2, 1) + i\sqrt{\{1 - \tfrac{1}{4}(2, 1)^2\}} = \tfrac{1}{2}(2, 1) + i\sqrt{\{\tfrac{1}{2} - \tfrac{1}{4}(2, 2)\}},$$

et l'autre..... $x = \tfrac{1}{2}(2, 1) - i\sqrt{\{\tfrac{1}{2} - \tfrac{1}{4}(2, 2)\}}$,

d'où résultent les valeurs numériques

$$-0{,}6772815716 \pm 0{,}7357239107\, i.$$

Les seize autres racines se tireront de l'élévation aux puissances de l'une ou de l'autre de ces deux premières, ou de la solution de huit équations semblables, dans laquelle, si l'on emploie la seconde méthode, on décidera du signe de la partie imaginaire, soit par les tables de sinus, soit par l'artifice que nous allons expliquer dans l'exemple suivant. C'est de cette manière qu'ont été

trouvées les valeurs suivantes, dans lesquelles le signe supérieur appartient à la première, et le signe inférieur à la seconde.

$$\begin{aligned}
[1]\ et\ [18] &= -0{,}677281571\,6 \pm 0{,}735723910\,7\ i\\
[2]\ et\ [17] &= -0{,}082579345\,5 \mp 0{,}996584493\,0\ i\\
[3]\ et\ [16] &= \ \ 0{,}789140509\,4 \pm 0{,}614212712\,7\ i\\
[4]\ et\ [15] &= -0{,}986361303\,4 \pm 0{,}164594590\,3\ i\\
[5]\ et\ [14] &= \ \ 0{,}546948158\,1 \mp 0{,}837166478\,3\ i\\
[6]\ et\ [13] &= \ \ 0{,}245485487\,1 \pm 0{,}969400265\,9\ i\\
[7]\ et\ [12] &= -0{,}879473751\,2 \mp 0{,}475947393\,0\ i\\
[8]\ et\ [11] &= \ \ 0{,}945817241\,7 \mp 0{,}324699469\,2\ i\\
[9]\ et\ [10] &= -0{,}401695424\,7 \pm 0{,}915773326\,7\ i.
\end{aligned}$$

354. *Exemple II. Pour* n = 17.

On a ici $n-1=2.2.2.2$, ainsi le calcul des racines Ω peut se ramener à quatre équations du second degré. Nous choisirons 3 pour racine primitive; ses puissances fournissent, suivant le module 17, les résidus *minima* suivans:

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15
1, 3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6,

d'où résulte la distribution suivante en deux périodes de huit termes, quatre périodes de quatre termes et huit de deux termes:

$$\Omega=(16,\ 1)\begin{cases}(8,\ 1)\begin{cases}(4,\ 1)\begin{cases}(2,\ 1).....[1],\ [16]\\(2,\ 13).....[4],\ [13]\end{cases}\\(4,\ 9)\begin{cases}(2,\ 9).....[8],\ [9]\\(2,\ 15).....[2],\ [15]\end{cases}\end{cases}\\(8,\ 3)\begin{cases}(4,\ 3)\begin{cases}(2,\ 3).....[8],\ [14]\\(2,\ 5).....[5],\ [12]\end{cases}\\(4,\ 10)\begin{cases}(2,\ 10).....[7],\ [10]\\(2,\ 11).....[6],\ [11].\end{cases}\end{cases}\end{cases}$$

L'équation (*A*) dont les racines sont les sommes (8, 1), (8, 3), se trouve (n° 351) être

$$x^2+x-4=0,$$

et ses racines sont:

$$-\tfrac{1}{2}+\tfrac{1}{2}\sqrt{17}=1{,}561552812\,8 \text{ et } -\tfrac{1}{2}-\tfrac{1}{2}\sqrt{17}=-2{,}561552812\,8;$$

nous supposerons que la première soit $(8, 1)$, l'autre sera nécessairement $(8, 3)$.

L'équation (B), dont les racines sont les sommes $(4, 1)$ et $(4, 9)$, est

$$x^2 - (8, 1)x - 1 = 0,$$

et ses racines sont

$$x = \tfrac{1}{2}(8, 1) \pm \tfrac{1}{2}\sqrt{\{4 + (8, 1)^2\}} = \tfrac{1}{2}(8, 1) \pm \tfrac{1}{2}\sqrt{\{12 + 3(8, 1) + 4(8, 3)\}};$$

nous supposerons égale à $(4, 1)$ celle de ces deux racines dans laquelle le radical est affecté du signe plus; on aura ainsi

$$(4, 1) = 2{,}0494811777, \qquad (4, 9) = -0{,}4879283649.$$

Les autres périodes de quatre termes, $(4, 3)$ et $(4, 10)$ peuvent être calculées de deux manières, savoir:

1°. Par la méthode du n° 346, qui donne les formules suivantes, en faisant, pour abréger, $(4, 1) = p$,

$$(4, 3) = -\tfrac{3}{2} + 3p - \tfrac{1}{2}p^3 = 0{,}3441507314,$$
$$(4, 10) = \tfrac{3}{2} + 2p - p^2 - \tfrac{1}{2}p^3 = -2{,}9057035442.$$

La même méthode donne aussi la formule

$$(4, 9) = -1 - 6p + p^2 + p^3,$$

d'où l'on tire la même valeur que plus haut.

2°. En résolvant l'équation dont $(4, 3)$, $(4, 10)$ sont les racines; cette équation est

$$x^2 - (8, 3)x - 1 = 0$$

et donne

$$x = \tfrac{1}{2}(8, 3) \pm \tfrac{1}{2}\sqrt{\{4 + (8, 3)^2\}},$$

ou..... $x = \tfrac{1}{2}(8, 3) + \tfrac{1}{2}\sqrt{\{12 + 4(8, 1) + 3(8, 3)\}}$,

et..... $x = \tfrac{1}{2}(8, 3) - \tfrac{1}{2}\sqrt{\{12 + 4(8, 1) + 3(8, 3)\}}$;

nous déciderons, par l'artifice suivant annoncé au n° 352, laquelle de ces deux racines doit être prise pour $(4, 3)$. Faisons le produit de $(4, 1) - (4, 9)$ par $(4, 3) - (4, 10)$, il est, calcul fait, $= 2(8, 1) - 2(8, 3)$. Or la valeur de cette expression est positive, puisqu'elle est $= 2\sqrt{17}$; d'ailleurs le premier facteur $(4, 1) - (4, 9)$ est aussi positif, comme égal à $\sqrt{\{12 + 4(8, 1) + 3(8, 3)\}}$; donc le second facteur doit aussi être positif, et partant $(4, 3)$

doit être la racine dans laquelle le radical est positif, et $(4, 10)$ l'autre racine (*). Au reste, il en résulte les mêmes valeurs que plus haut.

Connaissant toutes les sommes de quatre termes, nous passons maintenant à la recherche des sommes de deux termes. L'équation (C), dont les racines sont $(2, 1)$, $(2, 13)$, périodes contenues dans $(4, 1)$, est

$$x^2 - (4, 1)x + (4, 3) = 0,$$

qui donne

$$x = \tfrac{1}{2}(4, 1) \pm \tfrac{1}{2}\sqrt{\{-4(4, 3) + (4, 1)^2\}}$$
$$= \tfrac{1}{2}(4, 1) \pm \tfrac{1}{2}\sqrt{\{4 + (4, 9) - 2(4, 3)\}};$$

nous prendrons pour valeur de $(2, 1)$ celle de ces deux racines dans laquelle le radical est positif, et il en résulte

$$(2, 1) = 1,8649444588, \quad (2, 13) = 0,1845367189;$$

si l'on veut chercher les autres sommes de deux termes par la méthode du n° 346, on pourra employer pour

$$(2, 2), (2, 3), (2, 4), (2, 5), (2, 6), (2, 7), (2, 8),$$

les formules que nous avons données pour les quantités désignées de la même manière dans l'exemple précédent, savoir :

$$(2, 2) \text{ (ou } (2, 15)) = (2, 1)^2 - 2, \text{ etc.};$$

mais, si l'on préfère les déterminer deux à deux par des équations du second degré, on trouve pour $(2, 9)$ et $(2, 15)$ l'équation

$$x^2 - (4, 9)x + (4, 10) = 0,$$

qui donne

$$x = \tfrac{1}{2}(4, 9) \pm \tfrac{1}{2}\sqrt{\{4 + (4, 13) - 2(4, 3)\}},$$

et l'on déterminera le signe comme plus haut, savoir : le développement du produit de $(2, 1) - (2, 13)$ par $(2, 9) - (2, 15)$ donne

$$-(4, 1) + (4, 9) - (4, 3) + (4, 10),$$

(*) Le fond de cet artifice consiste dans une propriété facile à prévoir, d'après laquelle le développement de ce produit ne contient plus de périodes de quatre termes, mais se trouve exprimé par des périodes de huit termes ; les gens instruits en découvriront facilement la raison que l'envie d'abréger nous force d'omettre.

quantité évidemment négative; mais $(2, 1)-(2, 13)$ est positif; donc $(2, 9)-(2, 15)$ doit être négatif; ainsi, dans la valeur de x que nous avons trouvée, le signe supérieur doit être pris pour $(2, 15)$, et le signe inférieur pour $(2, 9)$.. Il en résulte

$$(2, 9)=-1{,}965946\,1994, \quad (2, 15)=1{,}478017\,8344.$$

De même, comme on a

$$\{(2, 1)-(2, 13)\}\times\{(2, 3)-(2, 5)\}=(4, 9)-(4, 10),$$

quantité positive, nous en concluons que $(2, 3)-(2, 5)$ doit être positif. De là, en faisant le calcul nécessaire, on trouve

$$(2, 3)=\tfrac{1}{2}(4, 3)+\tfrac{1}{2}\sqrt{\{4+(4, 10)-2(4, 9)\}}= \quad 0{,}891476\,7116$$
$$(2, 5)=\tfrac{1}{2}(4, 3)-\tfrac{1}{2}\sqrt{\{4+(4, 10)-2(4, 9)\}}=-0{,}547325\,9801;$$

on obtient enfin, par des opérations tout-à-fait analogues,

$$(2, 10)=\tfrac{1}{2}(4, 10)-\tfrac{1}{2}\sqrt{\{4+(4, 3)-2(4, 1)\}}=-1{,}700434\,2715$$
$$(2, 11)=\tfrac{1}{2}(4, 10)+\tfrac{1}{2}\sqrt{\{4+(4, 3)-2(4, 1)\}}=-1{,}205269\,2728.$$

Il reste encore à descendre aux racines Ω elles-mêmes. L'équation (D), dont $[1]$ et $[16]$ sont les racines, se trouve être

$$x^2-(2, 1)\,x+1=0,$$

qui donne

$$x=\tfrac{1}{2}(2, 1)\pm\tfrac{1}{2}\sqrt{\{(2, 1)^2-4\}}=\tfrac{1}{2}(2, 1)\pm\tfrac{1}{2}i\sqrt{\{4-(2, 1)^2\}}$$
$$=\tfrac{1}{2}(2, 1)\pm\tfrac{1}{2}i\sqrt{\{2-(2, 15)\}}.$$

Nous prendrons le signe supérieur pour $[1]$, et partant le signe inférieur pour $[16]$. Les quatorze autres racines se déduiront des puissances de $[1]$, ou de la résolution de sept équations du second degré, dont chacune donnera deux racines, pour lesquelles on lèvera l'incertitude, comme nous l'avons fait plus haut. Par exemple, $[4]$ et $[13]$ sont les racines de l'équation

$$x^2-(2, 13)+1=0,$$

qui donne

$$x=\tfrac{1}{2}(2, 13)\pm\tfrac{1}{2}i\sqrt{\{2-(2, 9)\}};$$

or on trouve

$$([1]-[16])\times([4]-[13])=(2, 5)-(2, 3),$$

quantité réelle négative; ainsi comme $[1]-[16]=i\sqrt{\{2-(2, 15)\}}$, c'est-à-dire le produit de l'imaginaire i par une quantité réelle

positive, [4] — [13] devra être aussi, à cause de $i^3 = -1$, le produit de i par une quantité réelle positive; d'où l'on conclura que l'on doit prendre pour [4] le signe supérieur, et pour [13] le signe inférieur. De la même manière, on trouve pour les racines [8] et [9],

$$\tfrac{1}{2}(2, 9) \pm \tfrac{1}{2} i \sqrt{\{2 - (2, 1)\}},$$

et comme

$$([1] - [16]) \times ([8] - [9]) = (2, 9) - (2, 10),$$

quantité négative, on prendra pour [8] le signe supérieur, pour [9] le signe inférieur. En calculant de la même manière les autres racines, on trouve les valeurs numériques suivantes, dans lesquelles le signe supérieur appartient à la première, et le signe inférieur à la seconde.

[1], [16]..... 0,9324722294 ± 0,3612416662 i,
[2], [15]..... 0,7390089172 ± 0,6736956436 i,
[3], [14]..... 0,4457383558 ± 0,8951633914 i,
[4], [13]..... 0,0922683595 ± 0,9957341763 i,
[5], [12]...— 0,2736629901 ± 0,9618256432 i,
[6], [11]...— 0,6026346364 ± 0,7980172273 i,
[7], [10]...— 0,8502171357 ± 0,5264321629 i,
[8], [9]...— 0,9829730997 ± 0,1837495178 i.

Ce qui précède pourrait suffire pour la solution de l'équation $x^n - 1 = 0$, et parconséquent pour trouver les fonctions trigonométriques qui correspondent aux arcs commensurables avec la circonférence. Cependant, à cause de l'importance du sujet, nous ne pouvons terminer nos recherches sans ajouter quelques-unes des nombreuses observations qui peuvent l'éclaircir, et des conséquences aussi nombreuses que l'on en peut déduire. Nous choisirons de préférence celles qui n'exigent pas beaucoup de recherches étrangères, et l'on ne doit voir dans ce que nous allons exposer, qu'un aperçu de cette immense doctrine dont nous nous proposons de parler par la suite avec détail.

355. Comme n est toujours supposé impair, 2 sera facteur de

$n-1$, et Ω sera composé de $\frac{n-1}{2}$ périodes de deux termes. Une pareille période, telle par exemple que $(2, \lambda)$, sera formée par les deux racines $[\lambda]$ et $[\lambda g^{\frac{n-1}{2}}]$, g étant, comme ci-dessus, une racine primitive quelconque suivant le module n. Mais $g^{\frac{n-1}{2}} \equiv -1 \pmod{n}$; donc $\lambda g^{\frac{n-1}{2}} \equiv -\lambda$ (n° 62), et partant, $[\lambda g^{\frac{n-1}{2}}] = [-\lambda]$; donc si l'on suppose

$$[\lambda] = \cos\frac{kP}{n} + i\sin\frac{kP}{n}, \text{ et partant, } [-\lambda] = \cos\frac{kP}{n} - i\sin\frac{kP}{n},$$

la somme $(2, \lambda) = 2\cos\frac{kP}{n}$. Nous nous bornons ici à conclure de là que la valeur de toute période de deux termes est une quantité réelle. Comme d'ailleurs toute période dont le nombre de termes est pair et $= 2a$, peut être décomposée en périodes de deux termes, il est clair qu'en général la valeur de toute période dont le nombre de termes est pair, est une quantité réelle. Si donc, dans le n° 352, on réserve 2 pour le dernier des facteurs α, β, γ, etc., toutes les opérations s'exécuteront sur des quantités réelles, jusqu'à ce qu'on soit arrivé aux périodes de deux termes, et les imaginaires ne s'introduiront, que lorsque l'on voudra passer de ces périodes aux racines elles-mêmes.

356. On doit surtout remarquer les équations auxiliaires par lesquelles on détermine, pour une valeur quelconque de n, les sommes des périodes qui forment l'ensemble Ω: elles sont liées d'une manière étonnante avec les propriétés les plus abstraites du nombre n. Mais ici nous restreindrons nos considérations aux deux cas suivans: 1° à l'équation du second degré qui donne les sommes des périodes de $\frac{n-1}{2}$ termes; 2° quand $n-1$ est divisible par 3, à l'équation du troisième degré qui donne les sommes des périodes de $\frac{n-1}{3}$ termes.

Faisons, pour abréger, $\frac{1}{2}(n-1) = m$, et désignons par g une racine primitive quelconque, Ω sera composé de deux périodes $(m, 1)$ et (m, g); la première contenant les racines $[1]$, $[g^2]$,

$[g^4], \ldots [g^{n-3}]$, et la seconde les racines $[g], [g^3], [g^5], \ldots [g^{n-2}]$. Supposons que les résidus *minima* positifs des nombres g^2, $g^4, \ldots g^{n-3}$ suivant le module n, soient R, R', R'', etc., abstraction faite de l'ordre, et que les résidus des nombres $g, g^3 \ldots g^{n-2}$ soient N, N', N'', etc.; les racines des périodes $(m, 1)$ et (m, g) coïncideront avec

$$[1], [R], [R'], [R''], \text{ etc.}, \quad [N], [N'], [N''], \text{ etc.}$$

respectivement. Or il est clair que tous les nombres $1, R, R', R''$, etc. sont *résidus quadratiques* de n; comme ils sont différens, moindres que n et au nombre de $\frac{n-1}{2}$, il s'ensuit que ce sont effectivement tous les résidus quadratiques de n, positifs et plus petits que lui (n° 96). Il suit de là en même temps, que les nombres N, N', N'', etc. qui sont tous différens entre eux, et des nombres $1, R, R'$, etc., et qui, joints à ces derniers, épuisent les nombres $1, 2, 3 \ldots n-1$, sont tous les non-résidus quadratiques positifs de n et plus petits que lui. Si l'on suppose maintenant que l'équation dont $(m, 1)$, (m, g) sont racines, soit

$$x^2 - Ax + B = 0,$$

on a

$$A = (m, 1) + (m, g) = -1, \quad B = (m, 1) \times (m, g);$$

or (n° 345),

$$(m,1)\times(m,g) = (m,N+1) + (m,N'+1) + (m,N''+1) + \text{etc.} = W,$$

et peut parconséquent être mis sous la forme

$$\alpha(m, 0) + \beta(m, 1) + \gamma(m, g).$$

Pour déterminer les coefficiens α, β, γ, observons : 1°. qu'on a $\alpha + \beta + \gamma = 0$, puisque le nombre des périodes de W est m; 2°. que $\beta = \gamma$ (n° 350), puisque $(m, 1) \times (m, g)$ est une fonction invariable des sommes $(m, 1)$ et (m, g) qui composent la période plus grande $(n-1, 1)$; 3°. que tous les nombres $N+1, N'+1, N''+1$, etc. étant compris entre les limites 2 et $n+1$, il est clair que nulle période de W ne coïncidera avec $(n, 0)$, ou qu'il n'y en aura qu'une, par exemple (m, n); on aura donc $\alpha = 1$, ou $= 0$, suivant que $n-1$ sera ou ne sera pas parmi les nombres N, N', etc.; il suit de là que dans le premier cas on aura $\alpha = 1$,

$\beta = \gamma$

$\beta=\gamma=\frac{m-1}{2}$, et dans le second $\alpha=0$, $\beta=\gamma=\frac{m}{2}$; et comme β et γ doivent être entiers, le premier cas aura lieu, c'est-à-dire que $n-1$ ou -1 se trouvera parmi les non-résidus de n lorsque m sera impair, c'est-à-dire lorsque n sera de la forme $4n+3$; le second aura lieu au contraire quand m sera pair, c'est-à-dire quand n sera de la forme $4n+1$. Ainsi, comme on a $(m, 0)=m$, et $(m, 1)+(m, g)=-1$, le produit cherché sera donc, suivant les mêmes circonstances, $\frac{1}{2}(m+1)$, ou $\frac{-1}{2}m$, et l'équation sera, dans le premier cas,

$$x^2+x+\tfrac{1}{4}(n+1)=0, \text{ qui donne } x=-\tfrac{1}{2}\pm\tfrac{1}{2}i\sqrt{n},$$

et dans le second

$$x^2+x-\tfrac{1}{4}(n-1)=0, \text{ qui donne } x=-\tfrac{1}{2}\pm\tfrac{1}{2}\sqrt{n}.$$

Ainsi, quelle que soit la racine que l'on ait prise pour $[1]$, si l'on désigne par $\Sigma[R]$ la somme de toutes les racines $[1]$, $[R]$, $[R']$, etc., et par $\Sigma[N]$ celle des racines $[N]$, $[N]'$, etc. On aura

$$\Sigma[R]-\Sigma[N]=\pm\sqrt{n}, \text{ ou } =\pm i\sqrt{n},$$

suivant que $n\equiv 1$ ou $\equiv 3 \pmod 4$. Il suit facilement de là que k étant un nombre entier quelconque non-divisible par n, on a

$$\Sigma\cos\frac{kRP}{n}-\Sigma\cos\frac{kNP}{n}=\pm\sqrt{n}, \text{ ou } =0,$$

$$\Sigma\sin\frac{kRP}{n}-\Sigma\sin\frac{kNP}{n}=0, \qquad \text{ou } \pm\sqrt{n},$$

suivant que $n\equiv 1$ ou $\equiv 3 \pmod 4$, théorèmes remarquables par leur élégance.

Au reste, nous ferons observer que le signe supérieur a lieu quand k est l'unité, ou plus généralement quand k est résidu quadratique de n, et le signe inférieur, quand k est non-résidu. Ces théorèmes conservent toute leur élégance, ou plutôt en acquièrent encore davantage, lorsque n est un nombre composé quelconque; mais nous sommes forcés de supprimer ces recherches qui demanderaient trop de développement, et de les réserver pour une autre occasion.

357. Soit

$$x^m-ax^{m-1}+bx^{m-2}-\text{etc.}=0, \text{ ou } z=0,$$

l'équation de degré m qui donne les racines contenues dans la

période $(m, 1)$; on aura $a = (m, 1)$, et chacun des autres coefficiens pourra être ramené à la forme

$$A + B(m, 1) + C(m, g),$$

où A, B, C sont des entiers (n° 348). Désignons par z' ce que devient z, quand on y remplace $(m, 1)$ par (m, g), et (m, g) par $(m, g^2) = (m, 1)$; l'équation $z' = 0$ donnera les racines contenues dans (m, g), et l'on aura

$$zz' = \frac{x^m - 1}{x - 1} = X.$$

On peut donc mettre z sous la forme

$$z = R + S(m, 1) + T(m, g),$$

où R, S, T seront des fonctions entières de x, dont les coefficiens seront entiers. Cela fait, on aura

$$z' = R + S(m, g) + T(m, 1).$$

Faisons, pour abréger, $(m, 1) = p$, $(m, g) = q$; on tire de ces équations

$$2z = 2R + (S + T)(p + q) - (T - S)(p - q) = 2R - S - T - (T - S)(p - q),$$
$$2z' = \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots = 2R - S - T + (T - S)(p - q);$$

donc posant $2R - S - T = Y$, $T - S = Z$, on a

$$4X = Y^2 - (p - q)^2 Z^2 = Y^2 \mp nZ^2,$$

puisque $(p - q)^2 = \pm n$ (n° précéd.), le signe supérieur ayant lieu quand n est de la forme $4k + 1$, et le signe inférieur quand n est de la forme $4k + 3$. C'est le théorème dont nous avons promis la démonstration au n° 124.

On voit facilement que les deux premiers termes de Y sont $2x^m + x^{m-1}$, et que le premier terme de Z est x^{m-1}; quant aux autres coefficiens, qui sont évidemment entiers, ils varient suivant la nature du nombre n, et ne peuvent être soumis à une formule analytique générale.

Exemple. Pour $n = 17$, l'équation qui donne les huit racines contenues dans $(8, 1)$, se trouve être (n° 348),

$$x^8 - px^7 + (4 + p + 2q)x^6 - (4p + 3q)x^5 + (6 + 3p + 5q)x^4$$
$$- (4p + 3q)x^3 + (4 + p + 2q)x^2 - px + 1 = 0,$$

qui donne

$$R = x^8 + 4x^6 + 6x^4 + 4x^2 + 1,$$
$$S = -x^7 + x^6 - 4x^5 + 3x^4 - 4x^3 + x^2 - x,$$
$$T = 2x^6 - 3x^5 + 5x^4 - 3x^3 + 2x^2;$$

et partant,

$$Y = 2x^8 + x^7 + 5x^6 + 7x^5 + 4x^4 + 7x^3 + 5x^2 + x + 2,$$
$$Z = x^7 + x^6 + x^5 + 2x^4 + x^3 + x^2 + x.$$

Voici encore d'autres exemples :

n	Y	Z
3	$2x + 1$	1.
5	$2x^2 + x + 2$	x.
7	$2x^3 + x^2 - x - 2$	$x^2 + x$.
11	$2x^5 + x^4 - 2x^3 + 2x^2 - x - 2$	$x^4 + x$.
13	$2x^6 + x^5 + 4x^4 - x^3 + 4x^2 + x + 2$	$x^5 + x^3 + x$.
19	$2x^9 + x^8 - 4x^7 + 3x^6 + 5x^5 - 5x^4 - 3x^3 + 4x^2 - x - 2$	$x^8 - x^6 + x^5 + x^4 - x^3 + x$.
23	$2x^{11} + x^{10} - 5x^9 - 8x^8 - 7x^7 - 4x^6 + 4x^5 + 7x^4 + 8x^3 + 5x^2 - x - 2$	$x^{10} + x^9 - x^7 - 2x^6 - 2x^5 - x^4 + x^2 + x$.

358. Passons à la considération des équations du troisième degré qui, dans le cas où n est de la forme $3k + 1$, donne les trois périodes de $\frac{n-1}{3}$ termes dont Ω est composé. Soit g une racine primitive quelconque pour le module n, et $\frac{n-1}{3} = m$ qui sera un nombre pair; les trois périodes qui composent Ω seront $(m, 1)$, (m, g), (m, g^2) que nous désignerons par p, p', p'', et qui contiennent respectivement les racines

$$[1], [g^3], [g^6], \ldots [g^{n-4}]; [g], [g^4], [g^7], \ldots [g^{n-3}];$$
$$[g^2], [g^5], [g^8], \ldots [g^{n-2}].$$

Supposons que l'équation cherchée soit

$$x^3 - Ax^2 + Bx - C = 0,$$

on aura

$$A = p + p' + p'', \quad B = pp' + pp'' + p'p'', \quad C = pp'p'',$$

d'où l'on tire sur-le-champ $A = -1$. Soient α, β, γ, etc., les

résidus *minima* des nombres $g^3, g^6, \ldots g^{n-4}$ suivant le module n, abstraction faite de l'ordre, et K leur ensemble, en y comprenant 1; soient de même α', β', γ', etc. les résidus *minima* des nombres g^2, $g^3, \ldots g^{n-4}$, et K' leur ensemble; $\alpha'', \beta'', \gamma''$, etc. les résidus *minima* de $g^2, g^5 \ldots g^{n-2}$, et K'' leur ensemble. Tous les nombres de K, K', K'' seront différens, et ils coïncideront avec la suite $1, 2, 3, \ldots n-1$. On doit observer avant tout que le nombre $n-1$ se trouve toujours dans K, puisqu'il est facile de voir qu'il est résidu de $g^{\frac{3}{2}m}$. Il suit de là aussi que les deux nombres h et $n-h$ se trouvent toujours dans la même des trois suites K, K', K''; en effet, si l'un est résidu de la puissance g^{λ}, l'autre sera résidu de la puissance $g^{\lambda+\frac{3}{2}m}$, ou $g^{\lambda-\frac{3}{2}m}$, si $\lambda > \frac{3}{2}m$. Désignons par le signe (KK) la multitude des nombres de la série $1, 2, 3 \ldots p-1$, qui tant par eux-mêmes qu'étant augmentés de l'unité, sont contenus dans K; par (KK') la multitude de ceux qui sont contenus dans K par eux-mêmes, et dans K' lorsqu'on les augmente de l'unité; on jugera assez par là de la signification des symboles

$$(KK''), (K'K), (K'K'), (K'K''), (K''K), (K''K'), (K''K'').$$

Cela posé, je dis d'abord qu'on a $(KK') = (K'K)$. Supposons en effet que h, h', h'', etc. soient tous les nombres de la suite $1, 2, 3, \ldots p-1$, qui par eux-mêmes sont contenus dans K et dans K' lorsqu'on les augmente de l'unité; c'est-à-dire que $h+1, h'+1, h''+1$, etc. sont supposés tous contenus dans K'; il est évident que $n-h-1$, $n-h'-1$, $n-h''-1$, etc. seront tous contenus dans K', et que ces nombres augmentés de l'unité, savoir, $n-h$, $n-h'$, $n-h''$, etc., le seront dans K; d'où il suit que $(K'K)$ n'est certainement pas plus petit que (KK'); mais comme on démontre de la même manière qu'on ne peut avoir $(KK') < (K'K)$, il s'ensuit qu'on a nécessairement $(KK') = (K'K)$, et de même $(KK'') = (K''K')$, $(K'K'') = (K''K')$.

Ensuite, comme en considérant un nombre quelconque de K, $n-1$ excepté, le nombre immédiatement plus grand doit être contenu ou dans K, ou dans K', ou dans K'', il s'ensuit que la somme

$$(KK) + (KK') + (KK'') = m - 1,$$

c'est-à-dire, au nombre de termes de K diminué d'une unité. Par

une raison semblable, on aura

$$(K'K)+(K'K')+(K'K'')=m,\ (K''K)+(K''K')+(K''K'')=m.$$

Développons maintenant d'après les règles du n° 345, le produit pp' en

$$(m, \alpha'+1)+(m, \beta'+1)+(m, \gamma'+1)+\text{etc.};$$

on verra facilement que cette expression peut se ramener à la forme

$$(K'K)p+(K'K')p'+(K'K'')p'';$$

et comme (n° 345) le produit $p'p''$ naît de pp', en changeant $(m, 1)$, (m, g), (m, g^a) en (m, g), (m, g^a), $(m, 1)$ respectivement, c'est-à-dire, p, p', p'', en p', p'', p, on aura

$$p'p''=(K'K)p'+(K'K')p''+(K'K'')p,$$

et de même

$$pp''=(K'K)\,p''+(K'K')p+(K'K'')p';$$

d'où résulte sur-le-champ

$$B=m\,(p+p'+p'')=-m.$$

De plus, comme on aurait pu développer directement pp'' de même qu'on a développé pp', ce qui aurait donné

$$pp''=(K''K)\,p+(K''K')\,p'+(K''K'')\,p'',$$

et que cette expression doit être identique avec la précédente, il s'ensuit qu'on a nécessairement $(K''K)=(K'K')$ et $(K''K'')=(K'K)$. Si donc nous faisons

$$(K''K')=(K'K'')=a,\ (K''K'')=(K'K)=(KK')=b,$$
$$(K'K')=(K''K)=(KK'')=c,$$

nous aurons

$$(KK)+(KK')+(KK'')=(KK)+b+c=m-1,$$

et
$$a+b+c=m,$$

d'où
$$(KK)=a-1.$$

Desorte que ces neuf quantités inconnues se réduisent à trois, ou plutôt à deux, à cause de l'équation $a+b+c=m$.

Enfin il est clair que le quarré p^s se développe en

$(m, 1+1)+(m, \alpha+1)+(m, \beta+1)+(m, \gamma+1)+$ etc.

Parmi les différens termes de cette expression, on trouvera (m, n) qui se ramène à $(m, o)=m$; le reste se réduira évidemment à

$$(KK)p+(KK')p'+(KK'')p'',$$

d'où l'on tire... $p^2=m+(a-1)p+bp'+cp''$.

Ainsi, par les réductions précédentes, nous avons trouvé les quatre équations

$$\begin{aligned} p^2 &= m+(a-1)p+bp'+cp'', \\ pp' &= \quad\ bp+cp'+ap'', \\ pp'' &= \quad\ cp+ap'+bp'', \\ p'p'' &= \quad\ ap+pb'+cp'', \end{aligned}$$

où les trois inconnues a, b, c sont liées par la relation

$$a+b+c=m.....(I),$$

et sont certainement des nombres entiers. On tire de là

$$C=p\times p'p''=ap^2+bpp'+cpp''=am+(a^2+b^2+c^2-a)p +(ab+bc+ac)p'+(ab+bc+ac)p''.$$

Mais comme $pp'p''$ est une fonction invariable de p, p', p'', les coefficiens de ces trois périodes doivent être les mêmes (n° 350), ce qui donne une nouvelle équation

$$a^2+b^2+c^2-a=ab+ac+bc.....(II),$$

et partant

$$C=am+(ab+ac+bc)(p+p'+p'')=a^2-bc.....(III),$$

à cause de l'équation (I), et de l'équation $p+p'+p''=-1$.

Quoique C dépende de trois inconnues qui ne sont liées que par deux équations, la condition qui exige que a, b, c soient des entiers, suffit pour les déterminer. Afin de le prouver, nous mettrons l'équation (II) sous la forme

$$12a+12b+12c+4=36a^2+36b^2+36c^2-36ab-36ac-36bc-24a +12b+12c+4,$$

qui devient

$$4n=(6a-3b-3c-2)^2+27(b-c)^2,$$

à cause de $n=3m+1=3a+3b+3c+1$; ou, en faisant $2a-b-c=k$,

$$4n=(3k-2)^2+27(b-c)^2.$$

Il suit de là que le nombre $4n$, c'est-à-dire le quadruple de tout nombre premier de la forme $3m+1$, peut être représenté par la forme x^2+27y^2; et quoique ce résultat puisse se tirer sans difficulté de la théorie générale des formes binaires, il n'en est pas moins étonnant qu'une telle décomposition soit liée si intimement avec les nombres a, b, c. Or nous démontrerons, comme il suit, que le nombre $4n$ ne peut être décomposé que d'une seule manière en un quarré et le produit d'un autre quarré par 27 (*). Si l'on supposait

$$t^2+27u^2=4n \quad \text{et} \quad t'^2+27u'^2=4n,$$

on en tirerait

$$1^\circ.....(tt'-27uu')^2+27(tu'+t'u)^2=16n^2$$
$$2^\circ.....(tt'+27uu')^2+27(tu'-t'u)^2=16n^2$$
$$3^\circ.....(tu'+t'u)(tu'-t'u)=4n(u'^2-u^2).$$

La troisième équation prouve que n, qui est un nombre premier, divise l'un des deux nombres $tu'+t'u$, $tu'-t'u$; mais la première et la seconde font voir que chacun de ces nombres est plus petit que n; donc celui que n divise est nécessairement nul, ce qui donne $u'^2-u^2=0$, ou $u^2=u'^2$ et $t^2=t'^2$, c'est-à-dire que les deux décompositions sont les mêmes. Si donc nous supposons connue la décomposition du nombre $4n$ en un quarré, et le produit d'un autre quarré par 27, décomposition que l'on peut trouver soit par la méthode directe de la Section V, soit par la méthode indirecte des nos 323, 324; si, par exemple, on a $4n=M^2+27N^2$, les quarrés $(3k-2)^2$, $(b-c)^2$ seront déterminés, et on aura deux équations au lieu de l'équation II. On voit clairement, non-seulement que le quarré $(3k-2)^2$ est déterminé, mais que la racine $3k-2$ l'est aussi; en effet, k devant être un nombre entier, on devra prendre $3k-2=+M$ ou $=-M$, suivant que M sera de la forme

(*) Cette proposition peut être démontrée plus directement par les principes de la Section V.

$3z+1$ ou $3z+2$ (*). Cela posé, comme on a

$$k = 2a - b - c = 3a - m,$$

on en tire

$$a = \frac{k+m}{3}, \qquad b+c = m-a = \tfrac{1}{3}(2m-k),$$

d'où

$$C = a^2 - bc = a^2 - \tfrac{1}{4}(b+c)^2 + \tfrac{1}{4}(b-c)^2 = \tfrac{1}{9}(m+k)^2 - \tfrac{1}{36}(2m-k)^2 + \tfrac{1}{4}N^2$$
$$= \tfrac{1}{12}k^2 + \tfrac{1}{3}km + \tfrac{1}{4}N^2;$$

et ainsi tous les coefficiens de l'équation cherchée se trouvent déterminés.

Cette formule devient encore plus simple, en substituant pour N^2 sa valeur tirée de l'équation

$$(3k-2)^2 + 27N^2 = 4n = 12m + 4;$$

ce qui donne

$$C = \tfrac{1}{9}(m + k + 3km) = \tfrac{1}{9}(m + kn).$$

Cette valeur peut encore se représenter sous la forme

$$C = (3k-2)N^2 + k^3 - 2k^2 + k - km + m,$$

qui est d'une application moins facile, mais qui fait voir par elle-même que C est un nombre entier, comme il le faut.

Exemple. Pour $n = 19$, on a $4n = 49 + 27$, d'où $3k-2 = 7$; $k = 3$, $C = \frac{1}{9}(6+57) = 7$, et l'équation cherchée est

$$x^3 + x^2 - 6x - 7 = 0,$$

comme ci-dessus (n° 351).

De même, pour $n = 7, 13, 31, 37, 43, 61, 67$, on trouve respectivement $k = 1, -1, 2, -3, -2, 1, -1$ et

$$C = 1, -1, 8, -11, -8, 9, -5.$$

Au reste, quoique le problème que nous venons de résoudre soit

(*) M ne peut être de la forme $3z$, car alors $4n$ serait divisible par 3. Quant à l'ambiguité de signe qui porte sur $b-c$, il est inutile de s'y arrêter, et même cette détermination est impossible par la nature même de la chose, puisqu'elle dépend du choix de la racine g, de manière que pour quelques racines primitives $b-c$ est positif, tandis que pour d'autres il est négatif.

assez

assez compliqué, nous n'avons pas voulu le supprimer, tant à cause de l'élégance de la solution, que parceque les artifices qu'il nous a donné occasion d'employer peuvent être d'une très-grande utilité dans d'autres problèmes.

359. Les recherches précédentes avaient pour but de trouver les équations auxiliaires; nous allons maintenant exposer sur leur résolution une propriété digne de remarque. On sait que tous les travaux des plus grands géomètres ont échoué contre la résolution générale des équations qui passent le premier degré, ou pour mieux définir l'objet de la recherche, contre la réduction des équations complètes à des équations à deux termes, et il est à peine douteux si ce problème ne renferme pas quelque chose d'impossible, plutôt qu'il ne surpasse les forces actuelles de l'analyse. (Voyez ce que nous avons dit sur ce sujet dans le Mémoire intitulé *Demonstratio nova, etc. p.* 22). Il est certain néanmoins qu'il y a une infinité d'équations composées dans chaque degré, qui admettent une telle réduction, et nous espérons faire plaisir aux géomètres, en prouvant que nos équations auxiliaires sont toujours dans ce cas. Mais à cause de l'étendue du sujet, nous ne présenterons que les principes les plus importans qui sont nécessaires pour démontrer cette possibilité, différant à un autre temps l'exposition plus complète. Nous mettrons en avant quelques observations générales sur les racines de l'équation $x^e - 1 = 0$, en comprenant le cas où e est un nombre composé.

1°. Ces racines sont données, comme on le sait, par les élémens, par la formule

$$x = \cos\frac{kP}{e} + i\sin\frac{kP}{e},$$

dans laquelle on doit prendre pour e les nombres $0, 1, 2, 3 \ldots e-1$, ou d'autres nombres quelconques congrus avec eux. Une seule racine est $= 1$, celle que l'on obtient en faisant $k = 0$, ou plus généralement $k \equiv 0 \pmod{e}$; mais à toute autre valeur de i répondra une valeur de x différente de 1.

2°. Comme on a

$$\left(\cos\frac{kP}{e} + i\sin\frac{kP}{e}\right)^\lambda = \cos\frac{\lambda kP}{e} + i\sin\frac{\lambda kP}{e},$$

si R est une racine qui corresponde à une valeur de k première avec e, le terme de numéro e dans la progression R, R^2, R^3, etc. sera $=1$, mais tous les autres seront différens de 1; il suit de là que toutes les quantités R, R^2, R^3, etc. sont différentes, et comme chacune satisfait à l'équation $x^e - 1 = 0$, elles sont les racines de cette équation.

3°. Enfin dans la même supposition, on a

$$1 + R^\lambda + R^{2\lambda} + R^{3\lambda} + \ldots + R^{(e-1)\lambda} = 0,$$

pour toute valeur de λ entière et non divisible par e; en effet cette expression équivaut à $\frac{1-R^{\lambda e}}{1-R^\lambda}$, et le numérateur de cette fraction est $=0$, tandis que le dénominateur ne l'est pas. Mais quand λ est divisible par e, cette somme est évidemment $=e$.

360. Soit, comme dans tout ce qui précède, n un nombre premier, g une racine primitive pour le module n, et $n-1$ les produits de trois nombres entiers positifs α, β, γ. Pour abréger, nous comprendrons en même temps dans nos recherches le cas, où l'on aurait α ou $\gamma = 1$; quand $\gamma = 1$, il faut remplacer $(\gamma, 1), (\gamma, g)$, etc. par $[1], [g]$, etc. Supposons donc que les α périodes de $\beta\gamma$ termes, $(\beta\gamma, 1), (\beta\gamma, g), (\beta\gamma, g^2) \ldots (\beta\gamma, g^{\alpha-1})$ soient connues, et que l'on veuille en déduire les valeurs des périodes de γ termes, opération que nous avons réduite plus haut à la résolution d'une équation complète du degré β, et qu'il s'agit maintenant de ramener à une équation à deux termes de même degré. Pour abréger, nous représenterons respectivement les valeurs des périodes

$$\begin{array}{lll}
(\gamma, 1), (\gamma, g^\alpha), (\gamma, g^{2\alpha}), \ldots (\gamma, g^{\alpha\beta-\alpha}) & \text{par} & a, b, c, \ldots m, \\
(\gamma, g), (\gamma, g^{\alpha+1}), \ldots\ldots\ldots (\gamma, g^{\alpha\beta-\alpha+1}) & & a', b', \ldots\ldots m', \\
(\gamma, g^2), (\gamma, g^{\alpha+2}), \ldots\ldots\ldots (\gamma, g^{\alpha\beta-\alpha+2}) & & a'', b'', \ldots\ldots m'',
\end{array}$$

jusqu'à celles qui composent la période $(\beta\gamma, g^{\alpha-1})$.

1°. Soit R une racine indéfinie de l'équation $x^\beta - 1 = 0$, et

supposons que le développement de la puissance β de la fonction

$$t = a + Rb + R^2c + \ldots . R^{\beta-1}m.$$

soit, par ce qui a été dit (n° 345),

$$\left.\begin{array}{l} N + Aa + Bb + Cc \ldots\ldots + Mm \\ + A'a' + B'b' + C'c' \ldots\ldots + M'm' \\ + A''a'' + B''b'' + C''c'' \ldots\ldots + M''m'' \\ + \text{etc.} \end{array}\right\} = T,$$

où les coefficiens N, A, B, A', etc. seront des fonctions rationnelles entières de R. Supposons aussi que la puissance β des deux autres fonctions

$$u = R^{\beta}a + Rb + R^2c \ldots\ldots + R^{\beta-1}m,$$

$$u' = \quad b + Rc + R^2d \ldots\ldots + R^{\beta-2}m + R^{\beta-1}a$$

se développe en U et U', on verra facilement (n° 350) que u' se tirant de t en changeant $a, b, c \ldots . m$ en $b, c, d \ldots . a$ respectivement, on aura

$$\left.\begin{array}{l} N + Ab + Bc + Cd \ldots\ldots + Ma \\ + A'b' + B'c' + C'd' \ldots\ldots + M'a' \\ + A''b'' + B''c'' + C''d'' \ldots\ldots + M''a'' \\ + \text{etc.} \end{array}\right\} = U' :$$

d'ailleurs $u = Ru'$, ainsi $U = R^{\beta}U'$; et comme $R^{\beta} = 1$, les coefficiens correspondans seront les mêmes dans U et U' ; enfin, comme t et u ne diffèrent qu'en ce que a est multiplié par l'unité dans t, et dans u par R^{β}, on voit facilement que les coefficiens correspondans, c'est-à-dire ceux qui multiplient les mêmes périodes, sont les mêmes dans T et dans U, et partant dans T et dans U'. On a donc

$A = B = C$, etc. $= M$, $A' = B' = C'$, etc., $A'' = B'' = C''$, etc. etc.

et partant, T se trouve réduit à la forme

$$T = N + A(\beta\gamma, 1) + A'(\beta\gamma, g) + A''(\beta\gamma, g^2) + \text{etc.},$$

où chacun des coefficiens N, A, A', etc. peut être ramené à la forme

$$pR^{\beta-1} + p'R^{\beta-2} + p''R^{\beta-3} + \text{etc.},$$

p, p', p'', etc., étant des nombres entiers donnés.

2°. Si l'on prend pour R une racine déterminée de l'équation $x^\beta - 1 = 0$ (dont nous supposons avoir déjà la solution), et telle que sa puissance β soit la plus petite qui soit égale à l'unité, T sera aussi une quantité déterminée dont on pourra tirer t par l'équation à deux termes $t^\beta - T = 0$. Comme cette équation a β racines.

$$t, Rt, R^2t \ldots\ldots Rt^{\beta-1},$$

le choix de la racine que l'on doit employer reste douteux; mais on peut prouver comme il suit que cela est indifférent. On doit se souvenir que, toutes les valeurs des périodes de $\beta\gamma$ termes étant supposées connues, la racine [1] n'est déterminée que par la condition d'être une des $\beta\gamma$ racines contenues dans $(\beta\gamma, 1)$, et que parconséquent nous sommes parfaitement maîtres de représenter par a la valeur d'une quelconque des périodes qui composent $(\beta\gamma, 1)$; et si la valeur d'une de ces périodes étant représentée par a, on a $t = \tau$, et qu'ensuite on représente par a la valeur de la période que l'on représentait par $b, c, d, \ldots a, b$, deviendra $b, c \ldots m, a$, ce qui donnerait alors $t = \frac{\tau}{R} = \tau R^{\beta-1}$. De même, si l'on veut représenter par a la valeur de la période qui était auparavant représentée par c, la valeur de t deviendra $\tau R^{\beta-2}$, et ainsi de suite; t pourra donc être supposé égal à une quelconque des quantités τ, $\tau R^{\beta-1}$, $\tau R^{\beta-2}$, etc., c'est-à-dire à celle qu'on voudra des racines de l'équation $x^\beta - T = 0$, pourvu que nous supposions que l'on prenne pour $(\gamma, 1)$, tantôt l'une, tantôt l'autre des périodes contenues dans $(\beta\gamma, 1)$.

3°. Lorsque la quantité t a été déterminée de cette manière, il faut chercher les $\beta - 1$ autres qui se déduisent de t, en substituant successivement $R^2, R^3, R^4, \ldots R^\beta$ à la place de R, c'est-à-dire,

$$t' = a + R^2 b + R^4 c \ldots + R^{2\beta-2} m,$$

$$t'' = a + R^3 b + R^6 c \ldots + R^{3\beta-3} m, \text{ etc.}$$

On connaît déjà la dernière, puisqu'elle devient évidemment $= a + b + c \ldots + m = (\beta\gamma, 1)$, et les autres se détermineront comme il suit.

Si, en suivant les règles du n° 345, on forme le produit $t^{\beta-2} t'$, comme (1°.) on a formé t^{β}, on prouvera d'une manière absolument analogue à la précédente, qu'il peut se ramener à la forme

$$N_1 + A_1(\beta\gamma, 1) + A_1'(\beta\gamma, g) + A_1''(\beta\gamma, g^2) + \text{etc.} = T',$$

N_1, A_1, A_1', etc. étant des fonctions rationnelles et entières de R, et parconséquent T' une quantité connue; d'où l'on tire $t' = \frac{T' t^2}{T}$.

De même si le développement du produit $t^{\beta-3} t''$ est supposé égal à T'', T'' aura une forme semblable, et une fois sa valeur connue, on aura $t'' = \frac{T'' t^3}{T}$; t'' se déterminera par l'équation $t''' = \frac{T''' t^4}{T}$, où T''' sera une quantité connue, etc.

Cette méthode cesserait d'être applicable, si l'on pouvait avoir $t = 0$, ce qui donnerait $T = T' = T'' = \text{etc.} = 0$; mais nous pourrions prouver que cette supposition est inadmissible, si nous n'étions forcés d'abréger. Il existe aussi des artifices particuliers par lesquels les fractions $\frac{T'}{T}$, $\frac{T''}{T}$, etc. peuvent être converties en fonctions entières de R, et des méthodes plus abrégées pour trouver t', t'', etc. lorsqu'on a $\alpha = 1$; mais nous ne pouvons nous arrêter à ces détails.

4°. Enfin, dès que l'on connaîtra t, t', t'', etc., on aura sur-le-champ, par la troisième observation du n° précédent,

$$t + t' + t'' + \text{etc.} = \beta a,$$

équation qui donnera la valeur de a, et de cette valeur on pourra (n° 346) déduire celle de toutes les périodes de γ termes. Les valeurs de b, c, d, etc. peuvent aussi se trouver, comme chacun pourra s'en assurer par une légère attention, au moyen des équations suivantes:

$$\beta b = R^{\beta-1}t + R^{\beta-2}t' + R^{\beta-3}t'' + \text{etc.},$$
$$\beta c = R^{2\beta-2}t + R^{2\beta-4}t' + R^{2\beta-6}t'' + \text{etc.},$$
$$\beta d = R^{3\beta-3}t + R^{3\beta-6}t' + \text{etc., etc.}$$

Parmi les nombreuses observations relatives à la recherche précédente, nous ne nous arrêterons que sur une seule.

On voit facilement que T obtient le plus souvent une valeur imaginaire de la forme $P+iQ$, desorte que la solution de l'équation dépend de la division en β parties, 1° d'un angle dont la tangente est $\frac{Q}{P}$; 2° d'un rapport qui est celui de 1 à $\sqrt{(P^2+Q^2)}$; et il est digne de remarque que la valeur de $\sqrt[\beta]{(P^2+Q^2)}$ peut toujours s'exprimer rationnellement par des quantités déjà connues, desorte que l'on n'a besoin que de la division de l'angle et de l'extrtacion d'une racine quarrée (nous ne faisons qu'indiquer cette remarque, que nous ne pouvons détailler ici), par exemple, pour $\beta = 3$ on n'a besoin que de la trisection de l'angle, tandis que pour la plupart des équations du troisième degré dont toutes les racines sont réelles, on ne peut éviter d'employer la trisection de l'angle et du rapport.

Enfin, comme rien n'empêche que nous ne supposions $\alpha = 1$, $\gamma = 1$, et partant $\beta = n-1$, il est évident que la solution de l'équation $x^n - 1 = 0$ peut être réduite à la solution de l'équation à deux termes du degré $n-1$, $x^{n-1} - T = 0$, où T se déterminera par les racines de l'équation $x^{n-1} - 1 = 0$. D'où il résulte, à l'aide de l'observation que nous venons de faire, que la division du cercle en n parties exige:

1°. La division du cercle en $n-1$ parties;

2°. La division en $n-1$ parties d'un arc qui peut se construire, lorsque la première division est faite;

3°. Enfin l'extraction d'une racine quarrée, et l'on peut prouver que cette racine est toujours $\sqrt{n}$.

351. Il nous reste à examiner de plus près la liaison qui existe entre les racines Ω et les fonctions trigonométriques des

angles

$$\frac{P}{n}, \frac{2P}{n}, \frac{3P}{n} \ldots\ldots \frac{(n-1)P}{n}.$$

La méthode que nous avons exposée pour trouver les racines Ω, laisse de l'incertitude sur celles de ces racines qui répondent à ces différens angles, c'est-à-dire, sur celle que l'on doit égaler à $\cos\frac{P}{n} + i\sin\frac{P}{n}$, celle que l'on doit égaler à $\cos\frac{2P}{n} + i\sin\frac{2P}{n}$, etc., à moins que l'on ne fasse usage des tables de sinus, ainsi que nous l'avons indiqué, ce qui peut ne pas sembler assez direct. Mais cette incertitude disparaît aisément, si l'on fait attention que les cosinus des angles

$$\frac{P}{n}, \frac{2P}{n}, \frac{3P}{n} \ldots\ldots \frac{(n-1)P}{2n},$$

vont continuellement en décroissant, pourvu que l'on tienne compte du signe, et que les sinus sont positifs, tandis que pour les angles

$$\frac{(n-1)P}{n}, \frac{(n-2)P}{n}, \frac{(n-3)P}{n} \ldots\ldots \frac{(n+1)P}{2n},$$

qui ont mêmes cosinus que les premiers, les sinus sont tous négatifs, quoique de même grandeur que les autres. Ainsi, parmi les racines Ω, les deux qui ont même partie réelle et pour lesquelles cette partie est la plus grande, répondront aux angles $\frac{P}{n}$ et $\frac{(n-1)P}{n}$, savoir, au premier celle où la quantité imaginaire est positive, au second celle où elle est négative. Parmi les $n-3$ autres racines, les deux qui auront la plus grande partie réelle répondront aux angles $\frac{2P}{n}$, $\frac{(n-2)P}{n}$, et ainsi de suite. D'ailleurs, aussitôt que l'on connaît la racine à laquelle répond l'angle $\frac{P}{n}$, on pourra distinguer les autres, en remarquant que si on la désigne par $[\lambda]$, aux angles $\frac{2P}{n}$, $\frac{3P}{n}$, $\frac{4P}{n}$, etc. répondront évidemment les racines $[2\lambda]$, $[3\lambda]$, $[4\lambda]$, etc. Ainsi dans l'exemple du n° 353, on voit sur-le-champ qu'il n'y a pas d'autre racine que [11] qui puisse répondre à l'angle $\frac{1}{19}P$, et à l'angle $\frac{18}{19}P$ la racine [8]. De même aux angles $\frac{2}{19}P$, $\frac{17}{19}P$, $\frac{3}{19}P$, $\frac{16}{19}P$, etc. répondent les racines [3], [16], [14], [5], etc. Dans

l'exemple du n° 354, la racine [1] répond évidemment à l'angle $\frac{1}{17}P$, la racine [2] à l'angle $\frac{2}{17}P$, etc. Ainsi de cette manière les sinus et cosinus des angles $\frac{P}{n}$, $\frac{2P}{n}$, etc. sont entièrement déterminés.

361. Quant à ce qui regarde les autres fonctions trigonométriques de ces angles, on pourrait les tirer des valeurs des sinus et cosinus, par les méthodes connues, savoir, les sécantes et les tangentes en divisant respectivement l'unité ou les sinus par les cosinus, et les cosécantes et les cotangentes, en divisant le rayon ou les cosinus par les sinus. Mais le plus souvent il sera plus commode d'employer les formules suivantes, qui n'exigent que de simples additions.

Soit ω un quelconque des angles $\frac{P}{n}$, $\frac{2P}{n}$ ..... $\frac{(n-1)P}{n}$, et $\cos\omega + i\sin\omega = R$; R sera une des racines Ω, et l'on aura

$$\cos\omega = \tfrac{1}{2}\left(R+\frac{1}{R}\right) = \frac{1+R^2}{2R}, \quad \sin\omega = \frac{1}{2i}\left(R-\frac{1}{R}\right) = \frac{i(1-R^2)}{2R},$$

et partant

$$\text{séc}\,\omega = \frac{2R}{1+R^2}, \quad \text{tang}\,\omega = \frac{i(1-R^2)}{1+R^2}, \quad \text{cosec}\,\omega = \frac{2Ri}{R^2-1}, \quad \cot\omega = \frac{i(R^2+1)}{R^2-1}.$$

Nous allons donner le moyen de transformer les numérateurs de ces quatre fractions, de manière à les rendre divisibles par les dénominateurs.

1°. Comme on a $R = R^{n+1} = R^{2n+1}$, il en résulte $2R = R + R^{2n+1}$, expression qui est divisible par $1+R^2$, puisque n est un nombre impair; donc

$$\text{séc}\,\omega = R - R^3 + R^5 - R^7 + \ldots + R^{2n-1};$$

et partant, puisqu'on a $\sin\omega = -\sin(2n-1)\omega$, $\sin 3\omega = -\sin(2n-3)\omega$, etc., et parconséquent $\sin\omega - \sin 3\omega + \sin 5\omega \ldots + \sin(2n-1)\omega = 0$,

$$\text{séc}\,\omega = \cos\omega - \cos 3\omega + \cos 5\omega \ldots + \cos(2n-1)\omega,$$

ou enfin, puisque $\cos\omega = \cos(2n-1)\omega$, $\cos 3\omega = \cos(2n-3)\omega$, etc.,

$$\text{séc}\,\omega = 2\{\cos\omega - \cos 3\omega + \cos 5\omega \ldots \mp \cos(n-2)\omega\} \pm \cos n\omega,$$

le signe supérieur ou inférieur ayant lieu, suivant que n est

de

de la forme $4n+1$ ou $4n+3$. Cette formule peut évidemment se présenter comme il suit :

$$\text{séc}\,\omega = \pm\{1 - 2\cos 2\omega + 2\cos 4\omega \ldots \pm 2\cos(n-1)\omega\}.$$

2°. Substituant de même $1-R^{n+2}$ pour $1-R^2$, on trouve

$$\text{tang}\,\omega = i(1 - R^2 + R^4 - R^6 \ldots - R^{2n}),$$

ou, comme $1-R^{2n}=0$, $R^2-R^{2n-2}=2i\sin 2\omega$, $R^4-R^{2n-4}=2i\sin 4\omega$, etc.

$$\text{tang}\,\omega = 2\{\sin 2\omega - \sin 4\omega + \sin 6\omega \ldots \mp \sin(n-1)\omega\}.$$

3°. Comme on a

$$1 + R^2 + R^4 \ldots\ldots + R^{2n-2} = 0,$$

on en tire

$$n = n - 1 - R^2 - R^4 \ldots - R^{2n-2} = (1-R^2) + (1-R^4) \ldots + (1-R^{2n-2}),$$

expression dont les différentes parties sont divisibles par $1-R^2$, d'où il résulte

$$\frac{n}{1-R^2} = 1 + (1+R^2) + (1+R^2+R^4) \ldots + (1+R^2+R^4 \ldots R^{2n-4})$$
$$= n - 1 + (n-2)R^2 + (n-3)R^4 \ldots + R^{2n-4};$$

si l'on multiplie par 2, que l'on retranche le produit

$$(n-1)(1+R^2+R^4 \ldots + R^{2n-2}) = 0,$$

et que l'on multiplie de nouveau par R, on a

$$\frac{2nR}{1-R^2} = (n-1)R + (n-3)R^3 + (n-5)R^5 \ldots - (n-3)R^{2n-3} - (n-1)R^{2n-1},$$

d'où résulte sur-le-champ,

$$\text{coséc}\,\omega = \frac{1}{n}\{(n-1)\sin\omega + (n-3)\sin 3\omega \ldots\ldots - (n-1)\sin(2n-1)\omega\}$$
$$= \frac{2}{n}\{(n-1)\sin\omega + (n-3)\sin 3\omega - \text{etc.} + 2\sin(n-2)\omega\},$$

formule qui peut encore se présenter ainsi

$$\text{coséc}\,\omega = -\frac{2}{n}\{2\sin 2\omega + 4\sin 4\omega + 6\sin 6\omega \ldots + (n-1)\sin(n-1)\omega\}.$$

4°. En multipliant par $1+R^2$ la valeur de $\frac{n}{1-R^2}$ que nous avons donnée plus haut, et en retranchant le produit

$$(n-1)(1+R^2+R^4+\ldots\ldots R^{2n-2}) = 0.$$

il vient

$$\frac{n(1+R^2)}{1-R^2} = (n-2)R^2 + (n-4)R^4 + (n-6)R^6 \ldots . - (n-2)R^{2n-2},$$

d'où

$$\cot\omega = \frac{1}{n}\{(n-2)\sin 2\omega + (n-4)\sin 4\omega + (n-6)\sin 6\omega \ldots . - (n-2)\sin(2n-2\omega)\}$$

$$= \frac{2}{n}\{(n-2)\sin 2\omega + (n-4)\sin 4\omega \ldots \ldots + 3\sin(n-3)\omega + \sin(n-1)\omega\},$$

formule qui peut encore se présenter ainsi qu'il suit :

$$\cot\omega = -\frac{1}{n}\{\sin\omega + 3\sin 3\omega \ldots . + (n-2)\sin(n-2)\omega\}.$$

363. De même qu'en supposant $n-1 = ef$, la fonction X peut être décomposée en e facteurs de degré f, aussitôt que l'on connaît les valeurs des e périodes de f termes (n° 348), si nous supposons maintenant que $Z = 0$ soit une équation du degré $n-1$ dont les racines soient les sinus, ou toute autre fonction trigonométrique des angles $\frac{P}{n}, \frac{2P}{n}, \ldots \frac{(n-1)P}{n}$, la fonction Z pourra se décomposer en e facteurs de degré f.

Soient $p = (f, 1)$, p', p'', etc. les périodes de f termes dont Ω est composé, et que p, p', p'', etc. contiennent respectivement les racines

$[1]$, $[a]$, $[b]$, $[c]$, etc.; $[a']$, $[b']$, $[c']$, etc.; $[a'']$, $[b'']$, $[c'']$, etc.;

supposons encore que l'angle ω réponde à la racine $[1]$, et partant les angles

$$a\omega,\ b\omega,\ \text{etc.};\quad a'\omega,\ b'\omega,\ \text{etc.};\quad a''\omega,\ b''\omega,\ \text{etc.}$$

aux racines

$$[a],\ [b],\ \text{etc.};\quad [a'],\ [b'],\ \text{etc.};\quad [a''],\ [b''],\ \text{etc.}$$

On verra facilement que ces angles pris ensemble coïncident (*), quant à leurs fonctions trigonométriques, avec les angles

$$\frac{P}{n},\quad \frac{2P}{n},\quad \frac{3P}{n}, \ldots \ldots \frac{(n-1)P}{n};$$

(*) Deux angles coïncident sous ce point de vue, quand leur différence est égale à la circonférence ou à un de ses multiples, c'est-à-dire, lorsqu'ils sont congrus suivant la circonférence, si nous voulons prendre l'expression de congruence dans un sens plus étendu.

si donc la fonction dont il s'agit est désignée par le signe φ placé devant l'angle, et que l'on fasse

$(x-\varphi\omega)(x-\varphi a\omega)$ etc. $=V$, $(x-\varphi a'\omega)(x-\varphi b'\omega)$ etc. $=V'$,
$(x-\varphi a''\omega)(x-\varphi b''\omega)$ etc. $=V''$, etc.,

on aura nécessairement

$$VV'V''\ldots\ldots=Z.$$

Il nous reste à faire voir que tous les coefficiens, dans les fonctions V, V', V'', etc. peuvent être ramenés à la forme

$$A+B(f,1)+C(f,g)+D(f,g^2)\ldots\ldots+L(f,g^{\epsilon-1});$$

car alors ils devront être regardés comme connus, dès que l'on connaîtra les valeurs de p, p', p'', etc. Or nous le prouverons de la manière suivante.

Le n° précédent fait voir que de la même manière que l'on a

$$\cos\omega=\tfrac{1}{2}[1]+\tfrac{1}{2}[1]^{n-1},\qquad \sin\omega=-\tfrac{i}{2}[1]+\tfrac{i}{2}[1]^{n-1},$$

les autres fonctions trigonométriques de l'angle ω sont réductibles à la forme

$$A'+B'[1]+C'[1]^2+D'[1]^3+\text{etc.},$$

et l'on voit sans la moindre difficulté, que la même fonction pour l'angle $k\omega$ est alors

$$A'+B'[k\omega]+C'[k\omega]^2+D'[k\omega]^3+\text{etc.},$$

k étant un entier quelconque. Or comme les différens coefficiens de V sont des fonctions invariables rationnelles et entières de $\varphi\omega$, $\varphi a\omega$, $\varphi b\omega$, etc., il est manifeste que si, à la place de ces quantités, on substitue leurs valeurs, les différens coefficiens deviendront des fonctions invariables de $[1]$, $[a]$, $[b]$, etc., et partant (n° 347) réductibles à la forme

$$A+B(f,1)+C(f,g)+D(f,g^2)+\text{etc.};$$

il en est de même des coefficiens V', V'', etc.

364. Nous ajouterons encore quelques observations à l'égard du problème du n° précédent.

1°. Comme les racines de la période $P'=(f,a')$ entrent dans les coefficiens de V', de la même manière que les racines de la période P entrent dans les coefficiens de V, il suit du n° 347 que V' peut se déduire de V, pourvu que l'on substi-

tue dans Y

(f, a'), $(f, a'g)$, $(f, a'g^2)$, etc. au lieu de $(f, 1)$, (f, g), (f, g^2), etc. De la même manière Y'' se déduira de Y en substituant

(f, a''), $(f, a''g)$, $(f, a''g^2)$, etc. au lieu de $(f, 1)$, (f, g), (f, g^2), etc. Ainsi, dès que la fonction Y est trouvée, les autres suivent de celle-là sans aucune peine.

2°. Soit $$Y = x^f - \alpha x^{f-1} + \beta x^{f-2} - \text{etc.}$$

Les coefficiens α, β, γ, etc. seront respectivement la somme des racines de l'équation $Y = 0$, la somme de leurs produits deux à deux, etc. Mais souvent ces coefficiens se déterminent plus commodément par une méthode semblable à celle du n° 349, c'est-à-dire, en calculant la somme des racines $\varphi\omega$, $\varphi\alpha\omega$, $\varphi\beta\omega$, etc., la somme de leurs quarrés, la somme de leurs cubes, etc., et déduisant de là ces coefficiens par le théorème de *Newton*. Toutes les fois que φ désigne la tangente, sécante, cotangente ou cosécante, on peut encore employer d'autres moyens d'abréviation, mais nous sommes forcés de les passer sous silence.

3°. Le cas où f est un nombre pair mérite une attention particulière; alors chacune des périodes P, P', P'', etc. est composée de $\frac{f}{2}$ périodes de 2 termes. Soient $(2, 1)$, $(2, a_1)$, $(2, b_1)$, $(2, c_1)$, etc. celles qui composent P, les nombres $1, a_1, b_1, c_1$, etc. et $n-1$, $n-a_1$, $n-b_1$, etc. pris ensemble, coïncideront avec la suite $1, a, b, c$, etc., ou du moins, ce qui revient au même quant à nos considérations, seront congrus à ceux-ci, suivant le module n. Mais on a $\varphi(n-1)\omega = \pm\varphi\omega$, $\varphi(n-a_1)\omega = \pm\varphi a_1\omega$, etc. en prenant les signes supérieurs, quand φ exprime le cosinus ou la sécante, et les signes inférieurs, quand φ exprime le sinus, la tangente, la cotangente ou la cosécante. Il suit de là que dans les deux premiers cas, les facteurs de Y seront égaux deux à deux, et que parconséquent Y sera un quarré $= y^2$, si l'on fait

$$y = (x-\varphi\omega)(x-\varphi a_1\omega)(x-\varphi b_1\omega), \text{ etc.}$$

Dans les mêmes cas, Y', Y'', etc. seront des quarrés, et si l'on suppose que P' soit composé des périodes $(2, a_1')$, $(2, b_1')$, $(2, c_1')$, etc., P'' des périodes $(2, a_1'')$, $(2, b_1'')$, $(2, c_1'')$, etc.,

et que l'on fasse

$$y' = (x - \varphi a_1' \omega)\,(x - \varphi b_1' \omega)\,(x - \varphi c_1' \omega), \text{ etc.},$$
$$y'' = (x - \varphi a_1'' \omega)\,(x - \varphi b_1'' \omega)\,(x - \varphi c_1'' \omega), \text{ etc.},$$

on aura $Y' = y'^2$, $Y'' = y''^2$, etc., et la fonction Z elle-même sera un quarré (*voyez* n° 337) dont la racine est égale à $yy'y''$, etc. Au reste, on voit facilement que y', y'', etc. se dérivent de y de la même manière que Y', Y'', etc. de Y (I); et que chaque coefficient de y peut aussi se ramener à la forme

$$A + B(f, 1) + C(f, g) + D(f, g^2), \text{ etc.},$$

puisque les sommes des puissances des racines de l'équation $y = 0$ sont les moitiés des sommes des puissances des racines de l'équation $Y = 0$, et partant réductibles à cette forme.

Dans les quatre autres cas, Y sera le produit des facteurs $x^2 - (\varphi\omega)^2$, $x^2 - (\varphi a_1 \omega)^2$, $x^2 - (\varphi b_1 \omega)^2$, etc. et parconséquent de la forme

$$x^f - \lambda x^{f-2} + \mu x^{f-4} - \text{etc.};$$

les coefficiens λ, μ, etc. peuvent se déduire de la somme des quarrés, des biquarrés, etc. des racines $\varphi\omega$, $\varphi a_1 \omega$, $\varphi b_1 \omega$, etc., et de même pour les fonctions Y', Y'', etc.

Exemple I. Soit $n = 17$, $f = 8$, et que φ désigne le cosinus. On a

$$Z = (x^8 + \tfrac{1}{2}x^7 - \tfrac{7}{4}x^6 - \tfrac{3}{4}x^5 + \tfrac{15}{16}x^4 + \tfrac{5}{16}x^3 - \tfrac{5}{32}x^2 - \tfrac{1}{32}x + \tfrac{1}{256})^2,$$

et il faut parconséquent décomposer $\sqrt{Z}$ en deux facteurs du quatrième degré y et y'. La période $P = (8, 1)$ est composée des périodes

$$(2, 1),\ (2, 9),\ (2, 13),\ (2, 15),$$

d'où

$$y = (x - \varphi\omega)\,(x - \varphi 9\omega)\,(x - \varphi 13\omega)\,(x - \varphi 15\omega).$$

Substituons $\frac{1}{2}[k] + \frac{1}{2}[n-k]$ pour $\varphi k\omega$, et désignons indéfiniment par S_m la somme des puissances m des racines $\varphi\omega$, $\varphi 9\omega$, etc., nous trouverons

$S_1 = \frac{1}{2}(8, 1)$; $S_2 = 2 + \frac{1}{4}(8, 1)$; $S_3 = \frac{3}{8}(8,1) + \frac{1}{8}(8, 1)$; $S_4 = \frac{3}{2} + \frac{5}{16}(8, 1)$:

et déterminant par là les coefficiens de y, à l'aide du théorème de *Newton*,

$y=x^4-\frac{1}{2}(8,1)x^3+\frac{1}{4}\{(8,1)+2(8,3)\}x^2-\frac{1}{8}\{(8,1)+3(8,3)\}x+\frac{1}{16}\{(8,1)+(8,3)\}$.

y' se déduit de y en changeant $(8, 1)$ en $(8, 3)$ et réciproquement; ainsi substituant les valeurs

$$(8, 1)=-\tfrac{1}{2}+\tfrac{1}{2}\sqrt{17}, \quad (8, 3)=-\tfrac{1}{2}-\tfrac{1}{2}\sqrt{17},$$

on a

$$y=x^4+(\tfrac{1}{4}-\tfrac{1}{4}\sqrt{17})x^3-(\tfrac{3}{8}+\tfrac{1}{8}\sqrt{17})x^2+(\tfrac{1}{4}+\tfrac{1}{8}\sqrt{17})x-\tfrac{1}{16},$$
$$y'=x^4+(\tfrac{1}{4}+\tfrac{1}{4}\sqrt{17})x^3-(\tfrac{3}{8}-\tfrac{1}{8}\sqrt{17})x^2+(\tfrac{1}{4}-\tfrac{1}{8}\sqrt{17})x-\tfrac{1}{16}.$$

$\sqrt{Z}$ peut de la même manière être décomposé en quatre facteurs du second degré, qui seront

$$(x-\varphi\omega)(x-\varphi 13\omega), \quad (x-\varphi 9\omega)(x-\varphi 15\omega),$$
$$(x-\varphi 3\omega)(x-\varphi 5\omega), \quad (x-\varphi 10\omega)(x-\varphi 11\omega),$$

et tous les coefficiens de ces facteurs s'exprimeront au moyen des quatre périodes $(4, 1)$, $(4, 9)$, $(4, 3)$, $(4, 10)$. Or il est évident que le produit des deux premiers facteurs est y, et celui des deux derniers y'.

Exemple II. Si, toutes choses d'ailleurs égales, φ est supposé désigner le sinus, ensorte qu'on ait

$$Z=x^{16}-\tfrac{17}{4}x^{14}+\tfrac{119}{16}x^{12}-\tfrac{221}{32}x^{10}+\tfrac{935}{256}x^8-\tfrac{561}{512}x^6+\tfrac{357}{2048}x^4-\tfrac{51}{4096}x^2+\tfrac{17}{65536},$$

à décomposer en facteurs du huitième degré y et y', y sera le produit des quatre facteurs du second degré

$$x^2-(\varphi\omega)^2, \quad x^2-(\varphi 9\omega)^2, \quad x^2-(\varphi 13\omega)^2, \quad x^2-(\varphi 15\omega)^2.$$

Or comme on a... $\varphi k\omega=-\frac{i}{2}[k]+\frac{i}{2}[n-k]$, il en résulte

$$(\varphi k\omega)^2=-\tfrac{1}{4}[2k]+\tfrac{1}{2}[n]-\tfrac{1}{4}[2n-2k]=\tfrac{1}{2}-\tfrac{1}{4}[2k]-\tfrac{1}{4}[2n-2k];$$

de là, en désignant indéfiniment par S_m la somme des puissances m des racines $\varphi\omega$, $\varphi 9\omega$, $\varphi 13\omega$, $\varphi 15\omega$, on tire

$$S_2=2-\tfrac{1}{4}(8, 1); \qquad S_4=\tfrac{3}{2}-\tfrac{3}{16}(8, 1);$$
$$S_6=\tfrac{5}{4}-\tfrac{9}{64}(8, 1)-\tfrac{1}{64}(8, 3); \quad S_8=\tfrac{35}{32}-\tfrac{27}{256}(8, 1)-\tfrac{1}{32}(8, 3),$$

et partant

$$y=x^8-\{2-\tfrac{1}{4}(8, 1)\}x^6+\{\tfrac{3}{2}-\tfrac{5}{16}(8, 1)+\tfrac{1}{8}(8, 3)\}x^4$$
$$-\{\tfrac{1}{2}-\tfrac{9}{64}(8, 1)+\tfrac{5}{64}(8, 3)\}x^2+\tfrac{1}{16}-\tfrac{5}{256}(8, 1)+\tfrac{3}{256}(8, 3).$$

y' se déduit de y en échangeant entre eux $(8, 1)$ et $(8, 3)$, desorte que par la substitution des valeurs de ces périodes,

on a

$$y=x^8-(\tfrac{17}{8}-\tfrac{1}{8}\sqrt{17})x^6+(\tfrac{51}{32}-\tfrac{7}{32}\sqrt{17})x^4-(\tfrac{17}{32}-\tfrac{7}{64}\sqrt{17})x^2+\tfrac{17}{256}-\tfrac{1}{64}\sqrt{17},$$
$$y'=x^8-(\tfrac{17}{8}+\tfrac{1}{8}\sqrt{17})x^6+(\tfrac{51}{32}+\tfrac{7}{32}\sqrt{17})x^4-(\tfrac{17}{32}+\tfrac{7}{64}\sqrt{17})x^2+\tfrac{17}{256}+\tfrac{1}{64}\sqrt{17};$$

On pourra de la même manière décomposer Z en quatre facteurs, dont les coefficiens s'exprimeront au moyen des valeurs des périodes de quatre termes; le produit de deux d'entre eux sera y, le produit des autres y'.

365. Nous avons ainsi réduit par les recherches précédentes la division du cercle en n parties, si n est un nombre premier, à la solution d'autant d'équations qu'il y a de facteurs dans le nombre $n-1$, et dont le degré est déterminé par la grandeur des facteurs. Ainsi, toutes les fois que $n-1$ est une puissance de 2, ce qui arrive pour les valeurs de n

$$3,\ 5,\ 17,\ 257,\ 65537,\ \text{etc.},$$

la division du cercle est réduite à des équations du second degré seulement, et les fonctions trigonométriques des angles $\frac{P}{n}$, $\frac{2P}{n}$, etc. peuvent être exprimées par des racines quarrées plus ou moins compliquées, suivant la grandeur de n; donc, dans ces différens cas, la division du cercle en n parties, ou la description du polygone régulier de n côtés, peut s'exécuter par des constructions géométriques. Par exemple, pour $n=17$, on tire facilement des nos 354, 361

$$\cos\frac{P}{17}=-\tfrac{1}{16}+\tfrac{1}{16}\sqrt{17}+\tfrac{1}{16}\sqrt{(34-2\sqrt{17})}-\tfrac{1}{8}\sqrt{\{(17+3\sqrt{17})-\sqrt{(34-2\sqrt{17})}-2\sqrt{(34+2\sqrt{17})}\}};$$

les cosinus des multiples de cet angle ont une forme semblable, les sinus ont un radical de plus. Il y a certainement bien lieu de s'étonner que la divisibilité du cercle en 3 et 5 parties ayant été connue dès le temps d'*Euclide*, on n'ait rien ajouté à ces découvertes dans un intervalle de deux mille ans, et que tous les géomètres aient annoncé comme certain, qu'excepté ces divisions et celles qui s'en déduisent (les divisions en 2^μ, 15, 3.2^μ, 5.2^μ, 15.2^μ parties), on ne pouvait en effectuer aucune par des constructions géométriques.

Au reste on prouve facilement que si un nombre premier n est $=2^m+1$, le nombre m lui-même ne peut avoir d'autres diviseurs que 2, et qu'il est parconséquent de la forme 2^ν. En effet si m était divisible par un nombre impair ζ plus grand que l'unité, et qu'on eût ainsi $m=\zeta\eta$, 2^m+1 serait divisible par $2^\eta+1$, et partant composé. Toutes les valeurs de n qui ne conduisent qu'à des équations du second degré, sont donc contenues sous la forme $2^{2^\nu}+1$; ainsi les cinq nombres 3, 5, 17, 257, 65537 s'en déduisent en faisant $\nu=0$, 1, 2, 3, 4 ou $m=1$, 2, 4 8, 16. Mais la réciproque n'est pas vraie, et la division du cercle n'a lieu géométriquement que pour les nombres *premiers* compris dans cette formule. A la vérité *Fermat*, trompé par l'induction, avait affirmé que tous les nombres compris sous cette forme étaient nécessairement premiers; mais *Euler* a remarqué le premier que cette règle était en défaut dès la supposition $\nu=5$ ou $m=32$, qui donne

$$2^{32}+1=4294967297,$$

nombre divisible par 641.

Toutes les fois que $n-1$ renferme des facteurs différens de 2, on est toujours conduit à des équations plus élevées, par exemple, à une ou plusieurs équations du troisième degré, si 3 est une ou plusieurs fois facteur; à des équations du cinquième degré, quand $n-1$ est divisible par 5, etc., et NOUS POUVONS DÉMONTRER EN TOUTE RIGUEUR QUE CES ÉQUATIONS NE SAURAIENT EN AUCUNE MANIÈRE ÊTRE ÉVITÉES NI ABAISSÉES, et quoique les limites de cet Ouvrage ne nous permettent pas de développer ici la démonstration de cette vérité, nous avons cru devoir en avertir, pour éviter que quelqu'un ne voulût essayer de réduire à des constructions géométriques d'autres divisions que celles données par notre théorie, et n'employât inutilement son temps à cette recherche.

366. Si l'on veut diviser le cercle en a^α parties, a étant un nombre premier et $\alpha>1$, il est aisé de voir que la construction géométrique n'est possible qu'autant que $a=2$. En effet, si $a>2$, outre les équations nécessaires pour la division du cercle en a parties,

il

il faut encore résoudre $a-1$ équations du degré a, que l'on ne peut non plus ni éviter, ni abaisser. Ainsi le degré des équations nécessaires se connaîtra généralement par les facteurs premiers du nombre $(a-1)a^{\alpha-1}$ (y compris le cas où $\alpha=1$).

Enfin si l'on doit diviser le cercle en $N=a^{\alpha}b^{\beta}c^{\gamma}\ldots$ parties, a, b, c, etc. étant des nombres premiers, il suffit de savoir effectuer les divisions en a^{α}, b^{β}, c^{γ}, etc. parties (n° 336). Ainsi, pour connaître le degré des équations nécessaires, on doit considérer les facteurs premiers des nombres

$$(a-1)a^{\alpha-1},\quad (b-1)b^{\beta-1},\quad (c-1)c^{\gamma-1},\quad \text{etc.},$$

ou, ce qui revient au même, les facteurs de leur produit. On remarquera que ce produit indique combien il y a de nombres moindres que N et premiers avec lui (n° 38). Ainsi la division ne pourra s'exécuter géométriquement que lorsque ce nombre est une puissance de 2; mais quand il renferme d'autres facteurs premiers p, p', etc., on ne peut éviter en aucune manière les équations de degré p, p', etc.

Il suit de là généralement que pour que la division géométrique du cercle en N parties soit possible, N doit être 2 ou une puissance de 2, *ou bien* un nombre premier de la forme 2^m+1, *ou encore* le produit d'une puissance de 2 par un ou plusieurs nombres premiers différens de cette forme; ou d'une manière plus abrégée, il est nécessaire que N ne renferme aucun diviseur impair qui ne soit de la forme 2^m+1, ni plusieurs fois un même diviseur premier de cette forme.

On trouve de cette manière, au-dessous de 300, les trente-huit valeurs suivantes pour le nombre N:

2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34, 40, 48, 51, 60, 64, 68, 80, 85, 96, 102, 120, 128, 136, 160, 170, 192, 204, 240, 255, 256, 257, 272.

ADDITIONS DE L'AUTEUR.

N° 28. La solution de l'équation indéterminée $ax + by = \pm 1$ n'a pas été trouvée pour la première fois par *Euler*, comme nous l'avons dit, mais par *Bachet de Meziriac*, géomètre du dix-septième siècle, célèbre par l'édition de *Diophante* qu'il a publiée avec des Commentaires. C'est *Lagrange* qui lui en a restitué l'honneur, dans ses *Additions à l'Algèbre d'Euler*, *p.* 525, où il indique en même temps le fond de la méthode. *Bachet* a publié sa découverte dans la seconde édition de son ouvrage intitulé : *Problèmes plaisans et délectables qui se font par les nombres*, 1624; elle n'existe pas dans la première édition (imprimée à Lyon en 1712), qui est la seule que j'aie vue, mais elle y est annoncée.

N°s 151, 296, 297. *Legendre* a nouvellement exposé sa démonstration dans un excellent ouvrage intitulé : *Essai d'une théorie des nombres*, *p.* 214 *et suiv.*, mais cependant de manière à n'y rien changer d'essentiel, ensorte que cette méthode est encore sujette à toutes les objections que nous avons faites n° 297. Il est vrai que le théorème (qui sert de base à une supposition) que dans toute progression arithmétique l, $l+k$, $l+2k$, etc., on trouvera des nombres premiers, si k et l n'ont pas de diviseur commun, a été exposé avec plus de détail dans cet ouvrage, p. 12 et suiv.; mais il ne paraît pas encore avoir satisfait à la rigueur géométrique. D'ailleurs, quand même ce théorème serait complétement démontré, il resterait encore l'autre supposition, qu'il existe des nombres premiers de la forme $4n+3$, dont un nombre premier donné positif de la forme $4n+1$ est non-résidu quadratique, et j'ignore s'il est possible de démontrer cette proposition sans supposer le théorème fondamental lui-même. Au reste, nous devons faire remarquer que ce célèbre géomètre

n'a pas fait tacitement cette supposition, et qu'il en convient lui-même, page 221.

N°s 288—293. Ce sujet, qui est présenté ici comme une application particulière des formes ternaires, et qui, sous le rapport de la rigueur et de la généralité, semble ne rien laisser à desirer, a été traité bien plus amplement par *Legendre*, dans la troisième partie de son ouvrage (*), p. 321—400. Il s'est servi de principes tout-à-fait différens des nôtres; mais par la route qu'il a suivie, il a rencontré plusieurs difficultés qui l'ont empêché de démontrer rigoureusement les théorèmes principaux. Il a lui-même indiqué avec franchise ces difficultés; mais, si nous ne sommes dans l'erreur, elles pourraient être levées plus facilement que celle qu'il rappelle encore dans cette recherche (p. 371, en note à la fin), savoir que *dans toute progression arithmétique*, etc.

N° 306, *VIII*. Dans la troisième chiliade de déterminans négatifs, *nous en* avons trouvé trente-sept irréguliers, parmi lesquels dix-huit ont 2 pour indice d'irrégularité, et les dix-neuf autres l'indice 3.

Idem, *X*. Nous venons de parvenir à résoudre complétement la question que nous proposions ici, et nous publierons cette recherche, qui éclaire singulièrement plusieurs parties de l'arithmétique transcendante et de l'analyse, lorsque nous aurons occasion de mettre au jour la continuation de cet ouvrage. Nous avons trouvé en même temps, que le coefficient m (n° 304, p. 376) est

$$m = \gamma\pi = 2{,}3458847616,$$

γ étant le même qu'au n° 302, et π toujours la demi-circonférence du cercle dont le rayon est 1.

(*) Les lecteurs ont à peine besoin d'être prévenus de ne pas confondre nos formes ternaires avec ce que *Legendre* appelle *les formes ternaires d'un nombre*, car il n'entend par là que la décomposition d'un nombre en trois quarrés.

NOTES DU TRADUCTEUR.

Note relative au n° 162.

Nous hasardons de placer ici une solution différente du même problème, solution qui nous paraît à quelques égards plus simple que celle de l'auteur. Le principe dont nous nous servons se présentait naturellement, mais nous devons observer qu'il est employé dans l'ouvrage pour un problème analogue (n° 285, 3°).

Supposons d'abord que la forme F et la forme f soient équivalentes.

Si l'on connaissait toutes les transformations propres de la forme F en elle-même, et une transformation de f en F, en combinant chacune des premières avec la seconde (n° 159), on obtiendrait évidemment des transformations semblables à cette dernière. Or il est extrêmement facile de démontrer, 1° que chaque combinaison donnera une transformation différente des autres; 2° que toute transformation pourra naître de la combinaison d'une transformation de F en elle-même avec la transformation donnée de F en f.

Cherchons donc d'abord quels doivent être les nombres p, q, r, s, pour que la forme F se change proprement en elle-même par la substitution

$$x = px' + qy', \quad y = rx' + sy',$$

on aura les équations

$$Ap^2 + 2Bpr + Cr^2 = A \ldots\ldots (a), \quad Apq + B(ps + qr) + Crs = B \ldots\ldots (b),$$
$$Aq^2 + 2Bqs + Cs^2 = C \ldots\ldots (c), \quad ps - qr = 1 \ldots\ldots (d).$$

Les équations (a) et (c) peuvent se mettre sous la forme

$$(Ap + Br)^2 - Dr^2 = A^2, \quad (Cs + Bq)^2 - Dq^2 = C^2,$$

ou bien, m étant le plus grand commun diviseur des nombres A, $2B$, C, et en divisant la première par $\frac{A^2}{m^2}$, la seconde par $\frac{C^2}{m^2}$,

$$\left(\frac{m(Ap+Br)}{A}\right)^2 - D\left(\frac{mr}{A}\right)^2 = m^2; \quad \left(\frac{m(Cs+Bq)}{C}\right)^2 - D\left(\frac{mq}{C}\right)^2 = m^2.$$

Si l'on fait

$$\frac{m(Ap+Br)}{A}=t,\quad \frac{mr}{A}=u;\quad \frac{m(Cs+Bq)}{C}=t',\quad \frac{mq}{C}=u',$$

ces équations deviennent

$$t^2-Du^2=m^2,\qquad t'^2-Du'^2=m'^2;$$

or on a

$$p=\frac{t-Bu}{m},\quad r=\frac{Au}{m},\quad q=\frac{Cu'}{m},\quad s=\frac{t'-Bu'}{m};$$

substituant ces valeurs dans les équations (*b*) et (*d*), il en résulte

$$Btt'-D(ut'+u't)+BDuu'=Bm^2,\quad tt'-B(ut'+u't)+Duu'=m^2;$$

qui donnent $ut'+u't=0$; donc $u'=-\frac{ut'}{t}$. Cette valeur, substituée dans l'équation $tt'-Duu'=m^2$, donne $t'=t$, et partant $u=-u'$.

Il en résulte donc

$$p=\frac{t-Bu}{m},\quad q=-\frac{Cu}{m},\quad r=\frac{Au}{m},\quad s=\frac{t+Bu}{m},$$

or il est aisé de démontrer que t, u doivent être entiers, si p, q, r, s le sont, et réciproquement.

1°. Si p, q, r, s sont entiers, comme il est nécessaire pour notre question, comme on tire des valeurs précédentes

$$u=\frac{mr}{A}=\frac{r}{\frac{A}{m}},\quad u=-\frac{q}{\frac{C}{m}},\quad u=\frac{s-p}{\frac{2B}{m}},$$

on peut en conclure

$$\frac{r}{q}=-\frac{\frac{A}{m}}{\frac{C}{m}},\quad \frac{r}{s-p}=\frac{\frac{A}{m}}{\frac{2B}{m}};$$

mais l'une des deux fractions qui servent de second membre est nécessairement irréductible, donc r est divisible par $\frac{A}{m}$, où $\frac{rm}{A}=u$ sera un nombre entier, $\frac{mq}{C}$ en sera un aussi; de là il est aisé de voir que t est également un nombre entier.

2°. On démontrera, comme l'auteur le fait au même numéro (4°.), que toutes les valeurs entières de t, u donneront des valeurs entières pour p, q, r, s.

Il suit donc de tout ce qui précède, que la solution de notre question dépend de la résolution de l'équation $t^2-Du^2=m^2$ en nombres entiers, et que réciproquement une transformation d'une forme quelconque de déterminant D en elle-même, fournira une solution en nombres entiers de l'équation $t^2-Du^2=m^2$, pourvu que m soit le plus grand commun diviseur des trois coefficiens de cette forme.

Si maintenant $\alpha, \beta, \gamma, \delta$ sont des nombres pour lesquels F se change en f, on trouvera par le n° 159, pour les nombres $\alpha', \beta', \gamma', \delta'$, qui donnent une transformation quelconque semblable,

$$m\alpha' = \alpha t - (B\alpha + C\gamma)u, \quad m\beta' = \beta t - (B\beta + C\delta)u,$$
$$m\gamma' = \gamma t + (A\alpha + B\gamma)u, \quad m\delta' = \delta t + (A\beta + B\delta)u;$$

or il faut observer qu'ici les valeurs de $\alpha', \beta', \gamma', \delta'$ sont nécessairement entières, puisque $\alpha, \beta, \gamma, \delta$ et p, q, r, s le sont.

Si l'on compare les valeurs de T et de U, que l'auteur déduit (n° 199), avec celles auxquelles nous parvenons directement, on verra qu'elles sont identiques, *mutatis mutandis*.

Mais si F et f n'étaient pas équivalentes, on se convaincra aisément que ces formules ne donneraient plus toutes les transformations, à moins que l'on n'admette des valeurs fractionnaires de t et u dans lesquelles le dénominateur serait le quotient du plus grand commun diviseur des nombres $a, 2b, c$, divisé par le plus grand commun diviseur des nombres $A, 2B, C$. Si nous nommons m' le plus grand commun diviseur des nombres $a, 2b, c$, et que nous fassions $\frac{m'}{m} = \mu$, on trouvera pour ce cas, en substituant dans les formules $\frac{t}{\mu}$ et $\frac{u}{\mu}$, à la place de t et u, des formules semblables dans lesquelles, à la place de m, on doit mettre m', et où t et u seront des nombres qui satisfassent à l'équation $t^2 - Du^2 = m'^2$, comme il résulte de l'analyse de l'auteur. Nous insistons peu sur ce second cas, qui est d'une moins grande utilité.

Note relative au n° 164.

On peut encore faire cette recherche d'une manière qui nous paraît en quelque sorte plus directe.

Nous supposerons qu'on ait démontré, comme l'auteur, les relations qui existent entre $\alpha, \beta, \gamma, \delta, \alpha', \beta', \gamma', \delta'$, et qui sont, en faisant usage de sa notation,

$$a + d = 0, \quad e + e' = 0, \quad bc - ad = e^2, \text{ ou } a^2 + bc = e^2.$$

Cela posé, soit (F, G, H) la forme ambiguë cherchée, que nous désignerons par φ; faisons $\frac{2G}{F} = k$, k sera un nombre entier. Or puisque F doit se changer en φ, F renfermera φ proprement et improprement, et si la transformation propre est

$$x = mt + nu, \quad y = pt + qu,$$

on obtiendra une transformation impropre, en combinant la transformation propre avec une transformation impropre de φ en elle-même. Alors si φ se change en F' par la transformation propre

$$t = m'x' + n'y', \quad u = p'x' + q'y';$$

en passant d'abord de F à φ, et ensuite de φ à F', on obtiendra deux transformations de F en F', l'une propre et l'autre impropre (n° 159), et qui devront coïncider avec les transformations données.

La forme φ se change en elle-même par la transformation impropre $t = t' + ku'$, $u = -u'$; ainsi : 1°. F se change en F' par la transformation propre

$$x = (mm' + np')x' + (mn' + nq')y', \quad y = (pm' + qp')x' + (pn' + qq')y';$$

et partant, on aura

$$mm' + np' = \alpha, \; mm' + nq' = \beta, \; pm' + qp' = \gamma, \; pn' + qq' = \delta \ldots\ldots (1).$$

2°. F se change en F' par la transformation impropre

$$x = \{mm' + (mk - n)p'\}x' + \{mn' + (mk - n)q'\}y',$$
$$y = \{pm' + (pk - q)p'\}x' + \{pn' + (pk - q)q'\}y',$$

et l'on a parconséquent

$$mn' + (mk - n)p' = \alpha', \quad mn' + (mk - n)q' = \beta',$$
$$pm' + (pk - q)p' = \gamma', \quad pn' + (pk - q)q' = \delta' \ldots\ldots\ldots\ldots (2)$$

Les équations (1) donnent par l'élimination, en faisant $mq - np = h$,

$$m' = \frac{\alpha q - \gamma n}{h}, \; n' = \frac{\beta q - \delta n}{h}, \; p' = \frac{\gamma m - \alpha p}{h}, \; q' = \frac{\delta m - \beta p}{h}.$$

Les équations (2) donnent

$$m' = \frac{\alpha' q' - \gamma' n' + k(\gamma' m - \alpha' p)}{h}, \quad n' = \frac{\beta' q - \delta' n + k(\delta' m - \beta' p)}{h},$$
$$p' = \frac{\alpha' p - \gamma' m}{h} \qquad q' = \frac{\beta' p - \delta' m}{h}.$$

De ces doubles valeurs de m', n', p', q', on tire les équations

$$(\gamma + \gamma')m = (\alpha + \alpha')p, \quad (\delta + \delta')m = (\beta + \beta')p \ldots\ldots (3)$$
$$(\alpha - \alpha')q - (\gamma - \gamma')n = k(\gamma' m - \alpha' p), \; (\beta - \beta')q - (\delta - \delta')n = k(\delta' m - \beta' p) \ldots (4)$$

Les équations (3) donnent $\frac{m}{p} = \frac{\alpha + \alpha'}{\gamma + \gamma'}$; $\frac{m}{p} = \frac{\beta + \beta'}{\delta + \delta'}$. Or il est aisé de voir que l'équation de condition qui résulte de ces deux valeurs est toujours satisfaite, car elle revient à

$$(\alpha + \alpha')(\delta + \delta') - (\beta + \beta')(\gamma + \gamma') = 0, \quad \text{ou} \quad e + e' + a + d = 0,$$

en essayant d'éliminer q ou n entre les équations (4), on voit facilement qu'elles rentrent l'une dans l'autre ; car il en résulterait dans l'un ou l'autre cas des équations qui s'anéantissent d'elles-mêmes, leur premier membre étant multiplié par $(\alpha - \alpha')(\delta - \delta') - (\beta - \beta')(\gamma - \gamma')$ qui est égal à $e + e' - a - d$, quantité nulle, et leur second membre étant multiplié, pour l'une, par $cm + (d + e)p$, pour l'autre, par $(a + e)m + bp$, quantités également nulles, comme on peut s'en assurer facilement. Il suffirait pour cela de multiplier par δ la première des équations (3), et d'en retrancher la seconde multipliée par γ; de multiplier encore la première par β, et d'en retrancher la seconde multipliée par α. On trouverait

$$cm + (d + e)p = 0, \quad (a + e)m + bp = 0 \ldots\ldots\ldots (5)$$

Il suit de là qu'entre les cinq inconnues m, n, p, q, k, il n'y a réellement que deux équations. Ainsi le problème est indéterminé ; mais il faut que les valeurs de ces inconnues soient telles que m', n', p', q' soient entiers.

Disposons des nombres m et p dont le rapport seul est connu et égal à $\frac{\alpha' + \alpha'}{\gamma + \gamma'}$

ou $\frac{\beta+\beta'}{\delta+\delta'}$, et prenons pour m et p les termes de ce rapport réduit à sa plus simple expression.

On aura évidemment dans tous les cas des nombres entiers pour m' et p', si l'on fait $q=\mu h$; $n=\pi h$, où h est indéterminé jusqu'à présent. Cette supposition change l'équation $mq-np=h$ en $m\mu-p\pi=1$ qui servira à trouver μ et π.

Quant à p' et q', au moyen des valeurs de a, b, c, d ou $-a$, on tire facilement par l'élimination

$$\alpha' e=-(\gamma b+\alpha a),\quad \beta' e=-(\delta b+\beta a),\quad \gamma' e=\gamma a-\alpha c,\quad \delta' e=\delta a-\beta c;$$

or à l'aide des équations (5), on a

$$p'h=\gamma m-\alpha p=\gamma m-\frac{\alpha(a+e)m}{b}=\frac{1}{b}(\gamma b+\alpha a+\alpha e)m=\frac{(\alpha-\alpha')me}{b}$$

$$=\frac{\gamma(a-e)p}{b}-\alpha p=\frac{1}{c}(\gamma a-\alpha e-\gamma e)p=-\frac{(\gamma-\gamma')pe}{c};$$

On trouverait de même

$$q'h=\frac{(\beta-\beta')me}{b},\qquad q'h=\frac{(\delta-\delta')pe}{c}.$$

Si r est le plus grand commun diviseur des nombres a, b, c, et partant des nombres b, c, e, comme il est aisé de le prouver par l'équation $a^2+bc=e^2$, un des nombres $\frac{b}{r}$, $\frac{c}{r}$ sera premier avec $\frac{e}{r}$. Supposons que ce soit $\frac{b}{r}$; comme on a

$$p'h=\frac{(\alpha-\alpha')m\frac{e}{r}}{\frac{b}{r}}\quad\text{et}\quad q'h=\frac{(\beta-\beta')m\frac{e}{r}}{\frac{b}{r}},$$

il s'ensuit que $(\alpha-\alpha')m$ est divisible par $\frac{b}{r}$, ainsi que $(\beta-\beta')m$, puisque $p'h$ et $q'h$ sont essentiellement entiers. Donc en prenant $h=\frac{e}{r}$, p' et q' seront entiers.

D'ailleurs des valeurs précédentes de $p'h$, on tire $\alpha-\alpha'=\frac{b}{me}p'h$, $\gamma-\gamma'=-\frac{c}{pe}p'h$, et comme $\gamma' m-\alpha' p=-p'h$, la première des équations (4) devient $\frac{b}{me}q+\frac{c}{pe}=-k$, ou, puisque $q=\mu h=\mu\frac{e}{r}$, $n=\pi h=\pi\frac{e}{r}$, $\frac{b}{mr}\mu+\frac{c}{pr}\pi=-k$. Mais on a $\frac{m}{p}=-\frac{d+e}{c}=-\frac{b}{a+e}=-\frac{\frac{d}{r}+\frac{e}{r}}{\frac{c}{r}}=-\frac{\frac{b}{r}}{\frac{a}{r}+\frac{e}{r}}$, et partant $\frac{c}{r}$ est divisible par p, et $\frac{b}{r}$ par m, ou bien $\frac{c}{pr}$ et $\frac{b}{mr}$ sont entiers. Donc cette équation donne une valeur entière pour k, qui varie suivant les valeurs que l'on attribue à μ et π.

TABLE

TABLE PREMIERE. (nos 58, 91).

		2. 3. 5. 7. 11	13. 17. 19. 23. 29	31. 37. 41. 43. 47
3	2	1		
5	2	1. 3		
7	3	2. 1. 5		
9	2	1. *. 5. 4		
11	2	1. 8. 4. 7		
13	6	5. 8. 9. 7. 11		
16	5	*. 3. 1. 2. 1	3	
17	10	10. 11. 7. 9. 13	12	
19	10	17. 5. 2. 12. 6	13. 8	
23	10	8. 20. 15. 21. 3	12. 17. 5	
25	2	1. 7. *. 5. 16	19. 13. 18. 11	
27	2	1. *. 5. 16. 13	8. 15. 12. 11	
29	10	11. 27. 18. 20. 23	2. 7. 15. 24	
31	17	12. 13. 20. 4. 29	23. 1. 22. 21. 27	
32	5	*. 3, 1. 2. 5	7. 4. 7. 6. 3	0
37	5	11. 34. 1. 28. 6	13. 5. 25. 21. 15	27
41	6	26. 15. 22. 39. 3	31. 33. 9. 36. 7	28. 32
43	28	39. 17. 5. 7. 6	40. 16. 29. 20. 35	32. 35. 18
47	10	30. 18. 17. 38. 27	3. 42. 29. 39. 43	5. 24. 25. 37
49	10	2. 13. 41. *. 16	9. 31. 35. 32. 24	7. 38. 27. 36. 23
53	26	25. 9. 31. 38. 46	28. 42. 41. 39. 6	45. 22. 33. 30. 8

SUITE DE LA TABLE PREMIÈRE.

		2. 3. 5. 7.11 53.59.61.67.71	13.17.19.23.29 73.79.83.89	31.37.41.43.47
59	10	25.32.34.44.45 28	23.14.22.27. 4	7.41. 2.13.53
61	10	47.42.14.23.45 51.17	20.49.22.39.25	13.33.18.41.40
64	5	*. 3. 1.10. 5 5. 1. 3	15.12. 7.14.11	8. 9.14.13.12
67	12	29. 9.39. 7.61 3.54. 5	23. 8.26.20.22	43.44.19.63.64
71	62	58.18.14.33.43 59.29.37.11	27. 7.38. 5. 4	13.30.55.44.17
73	5	8. 6. 1.33.55 53. 5.58.50.44	59.21.62.46.35	11.64. 4.51.31
79	29	50.71.34.19.70 7.17.75.54.33	74. 9.10.52. 1 4	76.23.21.47.55
81	11	25. *.35.22. 1 45.53. 4.20.33	38.15.12. 5. 7 48.52	14.24.29.10.13
83	50	3.52.81.24.72 13.20.34.53.17	67. 4.59.16.36 43.47	32.60.38.49.69
89	30	72.87.18. 7. 4 10.45.19.32.26	65.82.53.31.29 68.46.27	57.77.67.59.34
97	10	86. 2.11.53.82 14.65.32.51.25	83.19.27.79.47 20.42.91.18	26.41.71.44.60

TABLE II. (n° 99).

	−1	+2	+3	+5	+7	+11	+13	+17	+19	+23	+29	+31	+37
3			—		—		—		—			—	—
5	—			—		—			—		—	—	
7		—			—	—				—	—		—
11			—	—		—				—		—	—
13	—		—				—	—		—	—		
17	—	—					—	—	—				
19				—	—	—		—	—	—			
23		—	—				—			—	—	—	
29	—			—	—		—			—	—		
31		—		—	—				—			—	
37	—		—		—	—							—
41	—	—		—						—		—	—
43						—	—	—		—		—	
47		—	—		—			—					—
53	—				—	—	—	—			—		—
59			—	—	—			—	—		—		
61	—		—	—			—		—				
67								—	—	—	—		—
71		—	—	—					—		—		—
73	—	—	—						—	—			—
79		—		—		—	—		—	—		—	
83			—		—	—		—		—	—	—	—
89	—	—		—		—		—					
97	—	—	—			—						—	

SUITE DE LA TABLE II.

	+41	+43	+47	+53	+59	+61	+67	+71	+73	+79	+83	+89	+97
3		—				—	—		—	—			—
5	—				—	—		—		—		—	
7		—		—			—	—		—			
11			—	—	—		—	—				—	—
13		—		—		—				—			
17		—	—	—	—		—				—	—	
19		—	—			—			—		—		
23	—		—		—			—	—				
29				—	—		—	—			—		
31	—		—		—		—	—					—
37	—		—	—			—	—	—		—		
41	—	—			—	—			—		—		
43	—	—	—	—	—		—			—	—		—
47			—	—	—	—		—		—	—	—	—
53		—	—	—	—							—	—
59	—			—	—			—		—			
61	—		—			—			—		—		—
67			—		—		—	—	—		—	—	
71		—						—	—	—	—	—	
73	—					—	—	—	—	—		—	—
79							—		—	—	—	—	—
83	—				—	—					—		
89			—	—			—	—	—	—		—	—
97		—	—	—		—			—	—		—	—

TABLE III. (n° 316).

3	(0).....3; (1)...6
7	(0).....142857
9	(0).....1; (1)...2; (2)..4; (3)..8; (4)..7; (5)..5
11	(0).....09; (1)..18; (2)..36; (3)..72; (4)..45
13	(0).....076923; (1)..461538
17	(0).....0588235294 117647
19	(0).....052631578947368421
23	(0).....0434782608 6956521739 13
27	(0).....037; (1)...074; (2)...148; (3)...296; (4)...592; (5)...185
29	(0).....0344827586 20689655517 24137931
31	(0).....0322580645 16129 (1).....5483870967 74193
37	(0).....027; (1)...135; (2)...675; (3)...378; (4)..891; (4)..459; (6)..297; (7)..486; (8)..432; (9)..162; (10)..810; (11)..054
41	(0).....02439; (1)..14634; (2)..87804; (3)..26829; (4)...60975; (5)...65853; (6)...95121; (7)...70731
43	(0).....0232558139 5348837209 3 (1).....6511627906 9767441860 4
47	(0).....0212765957 4468085106 3829787234 0425531914 893617
49	(0).....0204081632 6530612244 8979591836 7346938775 51
53	(0).....0188679245 283; (1)..4905660377 358; (2).....7547169811 320; (3)..6226415094 339
59	(0).....0169491525 4237288135 5932203389 8305084745 7627118644 06779661
61	(0).....0163934426 2295081967 2131147540 9836065573 7704918032 7868852459

SUITE DE LA TABLE III.

67	(0).....01492537315 97	343283582 0	8955223880
	(1).....17910447761 64	1194029850	7462686567
71	(0).....01408450702 8169	4225352112	6760563380
	(1).....87323943664 6478	1971830985	9154929577
73	(0).....01369863; (1)..06849315; (2)..34246575; (3).....7123287 6; (4)..56164383; (5)..80821917; (6).....04109589; (7)..20547945; (8)..02739726		
79	(0).....0126582278 481; (1)..3670886075 949; (2).....6455696202 531; (3)..7215189873 417; (4).....9240506329 113; (5)..7974683544 303		
81	(0).....01234567 9; (1).....135802469; (2).....493827160; (3).....432098765; (4).....753086419; (5).....283950617		
83	(0).....0120481927 4457831325 3	7108433734	9397590361
	(1).....6024096385 2891566265	5421686746 0	9879518072
89	(0).....0112359550 4943820224	5617977528 7191	0898876404
	(1).....3370786516 8314606741	8539325842 5730	6966292134
97	(0).....0103092783 8762886597 4845360824 185567.	5051546391 9381443298 7422680412	7525773195 9690721649 3711340206

FIN.

ACHEVÉ D'IMPRIMER
EN JUIN 1989
PAR L'IMPRIMERIE
DE LA MANUTENTION
A MAYENNE
N° 212-89

Dépôt légal : Juin 1989



ÉDITIONS JACQUES GABAY

RÉIMPRESSIONS

Paul APPELL
- *Traité de Mécanique rationnelle (5 tomes)*

Ludwig BOLTZMANN
- *Leçons sur la théorie des gaz*

Emile BOREL
- *Leçons sur les séries divergentes*

Léon BRILLOUIN
- *Les tenseurs en mécanique et en élasticité*
- *La science et la théorie de l'information*

Louis de BROGLIE
- *Ondes et mouvements*

Elie CARTAN
- *Leçons sur la géométrie des espaces de Riemann*
- *Leçons sur la géométrie projective complexe*
- *Leçons sur la théorie des espaces à connexion projective*
- *La théorie des groupes finis et continus et la géométrie différentielle, traitées par la méthode du repère mobile*

Augustin-Louis CAUCHY
- *Cours d'Analyse de l'École Royale Polytechnique*
Analyse algébrique

Michel CHASLES
- *Aperçu historique sur l'origine et le développement des méthodes en géométrie*

R. DELTHEIL & D. CAIRE
- *Géométrie*
Transformations - Coniques
- *Compléments de géométrie*
Géométrie métrique - Géométrie projective
Géométrie anallagmatique

Joseph FOURIER
- *Théorie analytique de la chaleur*

Évariste GALOIS
- *Œuvres mathématiques*
publiées en 1846 dans le *Journal de Liouville*
suivies d'une étude par
Sophus LIE
Influence de Galois sur le développement des mathématiques

Carl Friedrich GAUSS
- *Disquisitiones Arithmeticae* (traduction française)

Jacques HADAMARD
- *Leçons de géométrie élémentaire (2 vol.)*

Camille JORDAN
- *Cours d'Analyse de l'École Polytechnique (3 vol.)*
- *Traité des substitutions et des équations algébriques*

JOURNAL DE L'ÉCOLE POLYTECHNIQUE
- *Textes d'Ampère, Cauchy, Lagrange, Laplace, Legendre, Monge, Poisson...*

Stephen C. KLEENE
- *Logique mathématique*

Joseph-Louis LAGRANGE
Méchanique analitique
Edition originale de la *Mécanique analytique* parue en 1788

Trajan LALESCO
- *La géométrie du triangle*

Henri LEBESGUE
- *Leçons sur les constructions géométriques*
- *Les Coniques*

A. LIAPOUNOFF
- *Problème général de la stabilité du mouvement*

André LICHNEROWICZ
- *Éléments de calcul tensoriel*

Ernst MACH
- *La Mécanique*
Exposé historique et critique de son développement

James Clerk MAXWELL
- *Traité d'Électricité et de Magnétisme (2 vol.)*

John von NEUMANN
- *Les fondements mathématiques de la Mécanique quantique*

Julius PETERSEN
- *Méthodes et théories pour la résolution des problèmes de géométrie*

Henri POINCARÉ
- *Calcul des probabilités*
- *La Mécanique nouvelle*
Conférence (1909), Mémoire (1905) et Note (1905) sur la Théorie de la Relativité
- *Théorie du potentiel newtonien*
- *Théorie des tourbillons*
- *Théorie mathématique de la lumière*
Tome I,
Tome II, Nouvelles études sur la diffraction
Théorie de la dispersion de Helmholtz
- *Figures d'équilibre d'une masse fluide*
- *Électricité et Optique*

George POLYA
- *Comment poser et résoudre un problème*

Erwin SCHRÖDINGER
- *Mémoires sur la Mécanique ondulatoire*

Paul TANNERY
- *Pour l'histoire de la science hellène*
- *La géométrie grecque*

François TISSERAND
- *Traité de Mécanique céleste*
Tome I, Perturbation des planètes d'après la méthode de la variation des constantes arbitraires
Tome II, Théorie de la figure des corps célestes et de leur mouvement de rotation
Tome III, Exposé d'ensemble des théories relatives au mouvement de la Lune
Tome IV, Théorie des satellites de Jupiter et de Saturne Perturbations des petites planètes
- *Leçons sur la détermination des orbites,*
avec une préface de H. Poincaré

Diffusion-Distribution : JACQUES GABAY
151 bis, rue Saint-Jacques 75005 PARIS
Téléphone : (1) 43 54 64 64 - Télex : 203 521 F

ISBN 2-87647-054-3