Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 11 (1909)
Heft: 1: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: SUR LES TRAVAUX ARITHMÉTIQUES de Lagrange, de Legendre et de Gauss.
Autor: Aurry, A.
DOI: https://doi.org/10.5169/seals-11871

SUR LES TRAVAUX ARITHMÉTIQUES

DE LAGRANGE, DE LEGENDRE ET DE GAUSS.

Le premier travail arithmétique de Lagrange fut la démonstration de la solution connue de l'équation de Pell (*Miscel. Taurin.* 1766-69). Il fait voir que *le calcul de Brouncker aboutit toujours à une solution, laquelle est la plus petite possible*[1]*; que de cette solution on déduit toutes les autres,* par des suites ou des récurrences déjà indiquées par Euler ; que, *dans le cas où elle est possible, la solution de l'équation* $x^2 - ky^2 = -1$ *se ramène à celle de l'équation de Pell ;* il ramène à cette dernière différents cas de l'équation $x^2 - ky^2 = l$.

En 1768 (M. D.), il démontre l'important théorème sur le maximum du nombre des racines des congruences, déjà traité autrement par Euler, et en montre l'importance, avec des corollaires qui le complètent. (E. M. 1907, p. 294).

En 1769 (Id.), il donne la solution de l'équation $ax^2 + b = y^2$; à laquelle se réduit toute équation du second degré.

En 1770 (Id.), même sujet. C'est là qu'il imagine la notation $E\omega$, pour désigner le plus grand entier contenu dans le nombre ω, notation qu'on a remplacée par celle-ci : $E\omega$ (Legendre) et $[\omega]$ (Gauss)[2].

---

[1] Voir par exemple *Mathesis* 1906, p. 233.

[2] L'idée de remplacer les nombres non entiers par leur partie entière s'est présentée aux premiers calculateurs qui ont eu à opérer sur des nombres de ce genre ; mais ce n'était là qu'un procédé abréviatif. La théorie de la division, la recherche du p. g. c. d. de deux nombres, l'extraction de la racine carrée, et plus tard l'analyse indéterminée du premier puis du second degrés utilisaient implicitement la fonction $E\omega$; mais ce n'était encore qu'une application de la méthode instinctive des approximations successives. Lagrange l'emploie explicitement dans sa solution de l'équation de Pell ; puis Legendre, dans une formule arithmétique qu'on signale plus loin. Mais c'est surtout Gauss qui en a compris l'importance ; et depuis, elle est utilisée à chaque instant dans la théorie des nombres.

On en a même déduit l'idée de plusieurs autres *fonctions arithmétiques* dont les suivantes :

G ω, qui désigne l'entier, $E\left(\omega + \frac{1}{2}\right)$, le plus voisin de ω (Kronecker),

La même année (Id.), il donne la preuve de la solubilité de l'équation $x^2 - ay^2 - b \equiv 0$, la généralisation du théorème d'Euler sur le produit de deux sommes de quatre carrés et la première démonstration qu'on ait encore eue du théorème de Bachet.

En 1771 (Id.), deux démonstrations du théorème de Wilson [1].

La grande découverte de Lagrange est celle qui permet de trouver la forme quadratique des diviseurs de l'expression $ax^2 + bxy + cy^2$ (id. 1773-75). (Voir le t. III des *Œuvres complètes* de Lagrange), et dont nous avons donné une idée suffisante (E. M. 1907, p. 289). Rappelons seulement ici que c'est là qu'on voit pour la première fois la considération du déterminant d'une forme et de la réduite de celle-ci.

En 1777 (Id.), usage de la descente infinie pour vérifier cette assertion de Fermat que *le plus petit triangle rectangle dont l'hypoténuse est un carré ainsi que la somme de ses cathètes est celui dont les cathètes sont* 1061652293520 et 4565486027761, solution qu'Euler avait reconnue exacte mais qu'il n'avait pas démontrée être la plus simple.

Enfin, à la suite de sa traduction de l'*Algebra* d'Euler (Lyon, 1794), plusieurs notes importantes relatives à la théorie des fractions continues; à la solution de l'équation de Pell et de l'équation quadratique indéterminée, par des moyens nouveaux, et particulièrement par la considération des minima de la valeur absolue des fonctions $x - \omega y$ [2] et $ax^2 + bxy$

Tω ou Rω, la différence positive ou négative, $\omega - \mathrm{E}\left(\omega + \frac{1}{2}\right)$ de ω et de Gω (Tchebichef),

$$\mathrm{E}'\omega = \mathrm{E}(2\omega) - 2\mathrm{E}\omega, \quad \mathrm{E}''\omega = \frac{1}{2}\mathrm{E}\omega(1 + \mathrm{E}\omega), \quad \mathrm{E}'''\omega = (\mathrm{E}\omega)\left(\mathrm{E}'\frac{\omega}{2}\right), \text{ (Hermite)}.$$

[1] Pour la première il fait voir qu'on a :

$$(x+1)(x+2)\ldots(x+p-1) \equiv x^{p-1} - 1$$

ce qui généralise à la fois les deux théorèmes de Fermat et de Wilson (voir E. M. 1907, p. 299). La seconde s'obtient en faisant $a = p - 1$ dans l'identité de Mercator

$$a! = a^a - \mathrm{C}_{a,1}(a-1)^a + \mathrm{C}_{a,2}(a-2)^a - \ldots \pm a.$$

[2] Bien que cette théorie soit plutôt du ressort de l'analyse indéterminée, il convient d'en donner une idée, à cause de l'importance qu'elle a prise ultérieurement.

Soient α et β les entiers tels que, pour $x < \alpha$, $y < \beta$, on ait : $|\alpha - \omega\beta| < |x - \omega y|$, x et y étant premiers entre eux. Cherchons α' et β' tels que $\alpha\beta' - \alpha'\beta = \pm 1$ et posons

$$(\alpha) \qquad x = \alpha x' + \alpha' y', \qquad y = \beta x' + \beta' y' :$$

x' et y' seront entiers. Les conditions $x < \alpha$ $y < \beta$ font voir que pour $x < \alpha'$ et $y < \beta'$,

$+ cy^2$; à la recherche des expressions dont la forme se reproduit quand on la multiplie par une formule semblable[1].

Legendre fit paraître en 1785, dans les *Mém. de l'Ac. de Sc.*, un mémoire où, entre autres choses de haute importance, il démontrait un remarquable théorème sur la solubilité de l'équation $ax^2 + by^2 = cz^2$;[2] — énonçait sa célèbre *loi de réciprocité*[3] dont il ne donnait qu'une démonstration incomplète ; trouvait incidemment cet important théorème démontré plus tard par Lejeune-Dirichlet : *toute progression arithmétique dont le premier terme est premier avec la raison, renferme une infinité de nombres premiers ;* et posait les bases

---

on a de même

$$|\alpha' - \omega\beta'| < |x - \omega y| .$$

Opérant de même sur α', β', sur les résultats obtenus, et ainsi de suite, on trouve les suites représentées par les relations générales

$$\alpha^{(n)}\beta^{(n+1)} - \alpha^{(n+1)}\beta^{(n)} = \pm 1 , \qquad |\alpha^{(n)} - \omega\beta^{(n)}| < |x - \omega y|$$

$$x < \alpha^{(n)} , \qquad y < \beta^{(n)}$$

$$\mu^{(n-1)} = \frac{\alpha^{(n-1)} - \alpha^{(n+1)}}{\alpha^{(n)}} = \frac{\beta^{(n-1)} - \beta^{(n+1)}}{\beta^{(n)}} = \mathrm{E}\,\frac{\omega\beta^{(n+1)} - \alpha^{(n+1)}}{\alpha^{(n)} - \omega\beta^{(n)}} .$$

La série des α est décroissante et se termine par les termes $\mathrm{E}(\omega - 1)$, 1 ou 1, 0 suivant que $\omega \gtrless 1$; celle des β est également décroissante et se termine par les termes 1, 0 ou $\mathrm{E}\left(\frac{1}{\omega} - 1\right)$, 1 dans les mêmes cas. Les nombres μ représentent les quotients du développement de ω en fraction continue.

La série des $\alpha - \omega\beta$ est croissante et les signes des termes alternent.

Legendre a commencé l'étude des substitutions (α) ; mais c'est Gauss qui a le premier reconnu l'importance de cette théorie : il a fait voir qu'il y a grand avantage à distinguer les deux cas $\alpha\beta' - \alpha'\beta = 1$ et $\alpha\beta' - \alpha'\beta = -1$.

[1] Ainsi la formule $x^2 + axy + by^2$. (Voir *Mathesis*, 1907, p. 259.)

[2] Il faut et il suffit qu'on puisse trouver trois nombres λ, μ, ν, tels que $a\lambda^2 + b$, $c\mu^2 - b$, $\nu^2 - a$ soient respectivement des multiples de c, a, b.

[3] Cette loi, qui se note ainsi d'après Legendre :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

le symbole $\left(\frac{a}{p}\right)$ désignant le reste de la division de $a^{\frac{p-1}{2}}$ par p, publiée deux ans après les *Op. Anal.* d'Euler, qui en donne l'équivalent (voir la citation que nous avons faite à propos de cet ouvrage), — a fait accuser Legendre de plagiat. Cette accusation ne nous paraît pas fondée : il était plus facile de conclure par induction la loi de Legendre des cas particuliers qu'en avaient découverts Fermat et Euler, que de la déduire de la proposition des *Op. Anal.* D'ailleurs, sous cette forme, cette proposition était peu apte à faire découvrir les importantes conséquences que Legendre a tirées de sa formule.

d'une théorie des *nombres trinaires* ou décomposables en trois carrés.

Ce fut l'occasion de son *Essai sur la théorie des nombres* (Paris, 1798), où il étudie les propriétés élémentaires des nombres; remplace la formule (24) d'Euler par la suivante

$$\varphi(n) = n\left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right) \dots , \tag{32}$$

et en tire le moyen de déterminer combien il y a de nombres premiers dans une progression arithmétique donnée; remarque qu'on a sensiblement

$$\varphi(10^a) = \frac{1}{2a} \tag{33}$$

d'où il déduit la formule approchée

$$\varphi(a) = \frac{a}{2 \log a}\,^{1} \tag{34}$$

et conjecture que la formule exacte doit être de la forme $\frac{a}{A \log a + B}$; étudie ensuite les fractions continues; enseigne la solution des équations linéaires indéterminées; reproduit en l'améliorant la solution de Lagrange des équations indéterminées du second degré; donne différents théorèmes sur la possibilité de certaines équations de la forme $ax^2 - by^2 = c^2$, la démonstration des théorèmes de Fermat, d'Euler,

---

[1] C'est là le premier exemple de valeur moyenne dans la théorie des nombres. Gauss a également envisagé ce genre d'approximation à propos d'une certaine classification des déterminants. Libri a découvert une formule donnant en moyenne le nombre des solutions entières et positives de la congruence générale $F(x, y, z, \dots) = 0$. Lejeune-Dirichlet a posé les fondements de cette importante théorie, dont il a indiqué de très intéressantes applications. Voir : Berger, *Sur qq. appl. de la fonction gamma* (Upsal, 1880); Cesàro, *Sur div. quest. arith.* (Bruxelles, 1883); Cesàro, *Excursions arith. à l'infini* (Paris, 1885); Berger, *Rech. sur les valeurs moyennes* (Upsal, 1887).

Citons seulement ceci : on a en moyenne

$$\frac{\sum_1^n \int x}{n^2} = \frac{\pi^2}{12} \text{ (Lejeune-Dirichlet)}, \qquad \frac{\sum_1^{E(ne)} \theta(x)}{\sum(ne)} = \theta(n) \text{ (Berger)},$$

$$\frac{\sum_1^n \varphi(x)}{n^2} = \frac{3}{\pi^2} \text{ (Perott)},$$

Il y a en moyenne 61 contre 39 à parier que deux nombres quelconques sont premiers entre eux. (Cesàro.)

[2] Lejeune-Dirichlet a étendu ces théorèmes.

de Wilson, de Bachet, de Lagrange; développe les conséquences de la loi de réciprocité [1]; donne dans sa théorie des nombres trinaires, d'importants théorèmes, dont l'un concernant la relation existant entre le nombre de décompositions de n en trois carrés et les classes de formes de déterminant $-n$, théorème démontré rigoureusement par Gauss et étendu par Jacobi, Lejeune-Dirichlet, Liouville, Kronecker et Hermite.

Rappelons aussi le *symbole* $\left(\frac{a}{p}\right)$, qui porte le nom de Legendre, et qu'on énonce *caractère quadratique* de a : il désigne le reste de la division de $a^{\frac{p-1}{2}}$ par p, reste qui est toujours, comme on le sait, 1 ou -1 [2]. Citons encore d'importantes tables de formes des diviseus, tant linéaires que quadratiques, et celle des solutions de l'équation de Pell jusqu'à $k = 1000$.

Ajoutons qu'on voit pour la première fois, dans cet ouvrage, l'idée et le nom des *formes linéaires* et *quadratiques*, qu'il appelle aussi *formules*. Legendre y montre que la transformation la plus générale d'une forme quadratique en une autre s'obtient à l'aide des substitutions linéaires représentées aujourd'hui par la notation $\left(\begin{smallmatrix}\alpha & \gamma \\ \beta & \delta\end{smallmatrix}\right)$; que les nouvelles indéterminées sont des nombres entiers, quelles que soient les indéterminées primitives si on a $\alpha\delta - \beta\gamma = \pm 1$, et qu'en général on a entre les deux expressions D, D′ appelées depuis déterminants, par Gauss, la relation

$$D' = D(\alpha\delta - \beta\gamma)^2 .$$

Ces remarques en généralisent d'autres données par Lagrange, dans son mémoire de 1775.

---

[1] Ce sera le sujet de notre prochain article, ce qui nous dispense d'en dire davantage ici. On trouvera de nombreux renseignements sur cette belle loi, dans le t. II des *Werke* de Gauss; la *Note sur les rés. quad.* de Genocchi (Bull. de l'Ac. de Belgique, 1852); la brochure de Baumgart. *Ueber das quadratische Reciprocitätgesetz* (Leipzig, 1885) et la *Niedere Zahlentheorie,* de Bachmann (Leipzig, 1902). Pour un aperçu de la question, on pourra consulter le fascicule 1 du vol. III de l'*Encycl. des sc. math.* (Paris, 1906).

[2] Gauss indique que r est résidu et ρ non résidu de p au moyen des notations $r\mathrm{R}p$, $\rho\mathrm{N}p$, qui n'ont guère été employées que par lui. Jacobi a étendu l'emploi du symbole de Legendre à une valeur quelconque de p; il a mis $\left(\left(\frac{a}{p}\right)\right)$ pour désigner le *caractère biquadratique* de a, et Eisenstein $\left[\frac{a}{p}\right]$, pour le *caractère cubique* du même nombre.

Dans la deuxième édition de son *Essai* (Paris, 1808), Legendre ajoute plusieurs remarques très intéressantes : la formule

$$\text{(35)} \qquad \mathrm{E}\frac{n}{p} + \mathrm{E}\frac{n}{p^2} + \mathrm{E}\frac{n}{p^3} + \dots$$

indiquant combien de fois le nombre premier p est facteur dans le produit $n!$; la recherche du nombre des termes d'une progression arithmétique, divisibles par des nombres premiers donnés, d'où les formules suivantes :

$$\text{(36)} \qquad n - \Sigma\frac{n}{p} + \Sigma\mathrm{E}\frac{n}{pq} - \Sigma\mathrm{E}\frac{n}{pqr} + \dots$$

$$\text{(37)} \qquad n - \Sigma\mathrm{E}\frac{2n+p-1}{2p} + \Sigma\mathrm{E}\frac{2n+pq-1}{2pq} - \dots$$

donnant respectivement le nombre des termes des deux suites $1, 2, 3, \dots n$ et $1, 3, 5, \dots 2n-1$, non divisibles par les nombres premiers différents $p, q, r, \dots$; cette formule empirique

$$\text{(38)} \qquad \frac{a}{\mathrm{L}a - 1{,}08366}$$ [1]

fournissant approximativement le nombre $\mathrm{N}(a)$ des entiers plus petits que a, $\mathrm{L}a$ désignant un logarithme népérien. Il en déduit l'évaluation des expressions suivantes [2]

$$\sum_3^p \frac{1}{p}, \qquad \prod_3^p \left(1 - \frac{1}{p}\right)$$

---

[1] Cette formule est remarquablement exacte dans la limite des tables actuelles de nombres premiers. Tchebichef a étudié les expressions de cette forme et a démontré que la *formule moyenne* ou *asymptotique* $\frac{a}{\mathrm{L}a - 1}$ représente $\mathrm{N}(a)$ en général, avec une approximation poussée aux termes de l'ordre $\frac{a}{(\mathrm{L}a)^2}$, et a en outre proposé cette autre $\int_2^a \frac{dx}{\mathrm{L}x}$, que, dès 1793, Gauss avait également trouvée sous la forme $\int_e^a \frac{dx}{\mathrm{L}x}$, ainsi que Lejeune-Dirichlet, qui la notait ainsi $\Sigma\frac{1}{\mathrm{L}a}$.

Riemann, dans un mémoire célèbre, a montré la haute importance de la formule de Gauss au point de vue de la théorie des nombres premiers.

Voir à ce sujet la savante et très intéressante monographie de Torelli : *Sulla totalità dei numeri primi fino ad un limite assegnato* (Naples, 1901).

[2] Euler avait évalué les séries de ces expressions continuées à l'infini.

ainsi que ce théorème, insuffisamment démontré : *de* a *à* $a + 2\sqrt{a}$, *il y a au moins un nombre premier* [1].

Signalons aussi les notations M (a) pour désigner un certain multiple de a [2], et T $\left(\frac{a}{p}\right)$ pour désigner le nombre des termes de la progression 1, 3, 5, ... $2n$ — T non divisibles par les nombres premiers 3, 5, 7, 11, ... p [3].

Legendre a en outre donné en 1816 et en 1825, deux suppléments à son *Essai;* dans le premier, il démontre, d'après Cauchy, le théorème de Fermat sur les nombres polygones ; dans le second, il fait voir que l'équation $x^n + y^n = z^n$ ne peut avoir lieu pour $n > 2$ que pour des nombres d'une grandeur excessive [4]. Il cite Sophie Germain comme lui ayant fourni quelques-uns des théorèmes utilisés par lui ; donne, en même temps que Lejeune-Dirichlet la démonstration de l'impossibilité de cette égalité pour $n = 5$ et étudie l'équation $x^3 + y^3 = az^3$, qui, dit-il, est impossible pour $a = 1$, 2, 3, 4, 5, 6, 8, 16, ... [5].

Enfin il a donné en 1830 une édition définitive de son ouvrage, réédité en allemand en 1885 et reproduit textuellement en 1900.

En résumé, malgré son titre, l'ouvrage de Legendre n'est

---

[1] J. Bertrand a énoncé ce théorème, démontré par Tchebichef : *entre* a *et* 2a — 2, *il y a nécessairement un nombre premier.*

[2] Leibniz indiquait un multiple d'une quantité par un point placé au-dessus de cette quantité ; cette notation, qui s'applique mal à des expressions compliquées et cause des embarras typographiques, a été peu employée. Celle de Legendre, qu'il a remplacée par celle-ci $\mathfrak{M}(a)$, s'emploie encore aujourd'hui ainsi : $\mathfrak{M}(a)$, dans les traités élémentaires. Gauss se sert de la notation $\equiv 0 \pmod{a}$, encore plus encombrante. On aurait, ce nous semble, une notation très expressive en indiquant les multiples par des caractères gras.

Le plus souvent, on a avantage a employer la forme linéaire $ax + b$.

[3] On a imaginé depuis un grand nombre de fonctions de ce genre, qui ont surtout pour but de simplifier les énoncés et faciliter la découverte de nouvelles propriétés des nombres. Telles sont les suivantes, prises parmi les plus simples :

$\varphi(n)$, nombre des entiers premiers avec n et non supérieurs à n (Gauss).

$\theta(n)$, nombre des entiers premiers jusqu'à n (Voir Cesàro, op. cit.).

$\lambda(n)$, fonction dont la valeur est ± 1 selon que le nombre des facteurs égaux ou inégaux de n est pair ou impair (id.).

$\omega(n)$, nombre de manières dont l'entier n peut se décomposer en deux facteurs (Mertens).

$\mu(n)$, fonction dont la valeur est ± 1 selon que le nombre des facteurs premiers inégaux de n est pair ou impair (id.).

$\sigma(n) = \mu(1) + \mu(2) + \ldots + \mu(n)$ (id.). Mertens a construit une table de cette fonction allant jusqu'à $\sigma(10000) = -23$. (*Sitzb. d. math.-naturw. Cl.* 1897)

$t(n)$, nombre des diviseurs carrés de n (Cesàro).

Voir pour d'autres notations : Cesàro et Torelli, op. cit.

[4] Landry a continué ces recherches de Legendre.

[5] Cependant, comme l'a remarqué le P. Pépin, on a : $17^3 + 37^3 = 6.21^3$.

pas un véritable traité, mais plutôt un recueil de théorèmes non reliés entre eux par une conception ou un but communs. Seule, la loi de réciprocité y est l'objet d'une théorie bien complète. D'ailleurs, même à l'époque de sa troisième édition, il n'était déjà plus au niveau des progrès de la science. Remarquons aussi que, bien à tort selon nous, Legendre commence par une longue et fastidieuse exposition de la théorie des fractions continues, et qu'il considère la théorie des nombres comme une division de l'analyse indéterminée. Néanmoins il est encore souvent consulté aujourd'hui, surtout à cause de ses tables, et il faut reconnaître combien il a été utile pour la vulgarisation de la haute arithmétique.

Si Legendre n'a pas toujours été aussi heureux dans ses démonstrations que dans ses découvertes, la clarté de ses écrits, sa loi de réciprocité et les applications qu'il en a faites, ses études sur les formes trinaires et sur la progression arithmétique, ses formules semi-empiriques sur les nombres premiers lui assurent une place parmi les fondateurs de l'arithmétique moderne.

Il nous reste à donner un aperçu des travaux arithmétiques de l'illustre Gauss. A l'encontre de Legendre, le livre qu'il a modestement intitulé *Disquisitiones arithmeticæ* contient un ensemble de théories complètes, qui sont d'ailleurs aussi remarquables par l'importance, la nouveauté, la variété et la généralité des résultats que par la profondeur, l'élégance et la concision des méthodes. Gauss à la vérité paraît avoir eu pour but le perfectionnement, non de l'arithmétique, mais celui de l'algèbre, dans ce célèbre ouvrage, qui a ouvert un champ immense surtout aux investigations des algébristes et sera encore longtemps l'objet de leur étude ; mais, bien qu'elle n'y soit qu'accessoirement traitée, c'est là que l'arithmétique a reçu sa constitution définitive et le programme des travaux qu'elle devait aborder. Ecrit vers 1796, il ne fut imprimé qu'en 1801, à Leipzig ; et encore il ne contient que la moitié de ce que Gauss pensait y mettre : dans le but d'abréger, il a supprimé l'analyse des questions traitées ainsi que toute la huitième et dernière section ; depuis,

de multiples et importantes occupations, l'ont toujours empêché de publier le complément de son travail, ainsi que ses découvertes postérieures, dont on n'a que quelques fragments[1].

Les *Disq. ar.* ont paru, traduites en français, en 1807; elles ont été réimprimées dans les deux éditions des *Werke* de Gauss (Göttingue, 1863 et 1870), dont elles forment le premier volume ; et ont été en outre publiées, dans le texte primitif allemand (Berlin, 1889). Nous allons donner une courte analyse de son contenu.

Sect. I. Définition, notation et théorie de la *congruence*, dont Gauss fait la base de toute l'arithmétique[2]. Lemme fondamental de Bachet (E. M. 1907, p. 288).

Sect. II. Application de la notion de la congruence à la démonstration des théorèmes arithmétiques. *Congruences*[3]. Congruences linéaires. C'est là qu'on voit la remarquable formule

$$\varphi(a) + \varphi(b) + \ldots = n \tag{39}$$

a, b, ... désignant tous les facteurs premiers de n, y compris n lui-même[4].

---

[1] Il semble qu'une certaine fatalité s'attache aux écrits de vulgarisation arithmétique. Bien que les documents qui nous restent sur la science mathématique et astronomique des Egyptiens, des Chaldéens et des Babyloniens montrent que l'étude des nombres a chez eux progressé bien plus rapidement que celle des figures, on a bien plus de renseignements sur l'histoire de celle-ci ; ce qui tient à ce que les Grecs prisaient beaucoup plus l'exactitude des résultats de la géométrie que les opérations numériques, se terminant le plus souvent en approximation. Passant aux temps historiques, on peut citer d'importants travaux d'Apollonius sur la numération, qui ont été perdus, ainsi que la seconde partie de l'ouvrage de Diophante et son commentaire par Hypathia. D'insignifiantes difficultés ont empêché Fermat de publier ses méthodes ; Gauss n'a pu divulguer toutes les siennes ; Eisenstein, Riemann, Stieltjès sont morts jeunes ; Liouville n'a pas eu le temps de faire connaître ses méthodes et de compléter ses découvertes arithmétiques ; Lejeune-Dirichlet est mort avant d'avoir produit le commentaire de Gauss qu'il pensait écrire ; Lebesgue n'a pas trouvé de souscripteurs pour le *Traité* qu'il se proposait de publier ; Ed. Lucas est mort, le premier volume de sa *Th. des n.* à peine publié ; Cesàro a dû abandonner ses études arithmétiques auxquelles il avait dû ses premiers succès. Parlerons-nous de l'obstination avec laquelle cette science, — si éminemment propre à former l'esprit mathématique, — est bannie de l'enseignement ; bien que, sans charger davantage les programmes, il soit facile de lui trouver place en élaguant çà et là de ceux-ci divers articles bien moins utiles. Le nom même de l'arithmétique a été détourné de son sens primitif, *science des nombres,* pour en faire la désignation de la *science du calcul.*

[2] Cette notion était connue des Anciens, mais ne commença guère à être utilisée que lors de l'invention de la preuve des opérations numériques. Euler et Lagrange y font souvent appel ; mais c'est Legendre qui le premier a compris la nécessité de la considérer systématiquement. Toutefois il la traite et la note comme une équation ordinaire, en ajoutant le plus souvent : *à un multiple près de* p, et « sans qu'il soit besoin des égalités ni des dénominations nouvelles assez *incongrues* dont quelques géomètres font usage ».

[3] Il s'agit des équations de la forme $F(x) = Ay$. Libri a tenté l'étude des équations $F(x, y) = 0$, mais la trop grande généralité de ses résultats a rendu son travail à peu près inutilisable.

[4] Cette formule semble avoir donné le signal de la découverte d'une foule de relations

Divisibilité par p du nombre de permutations de p choses avec répétitions. Théorème sur le nombre possible des racines des congruences [1].

Sect. III. Théorème de Fermat. Etude approfondie des racines primitives. Théorème de Wilson et sa généralisation. Divers théorèmes sur la somme et le produit des racines primitives. Diverses extensions du théorème de Fermat.

Sect. IV. Théorie des résidus. Critérium d'Euler. Théorèmes quadratiques de Fermat; démonstration de quelques-

---

arithmétiques qu'il y aurait grand intérêt à réunir et à rapprocher. En voici quelques-unes élémentaires et assez caractéristiques :

$\Sigma\omega(a) = \theta(n^2)$ (Liouville)

$\Sigma\lambda(a)\,\omega(a) = \lambda(n)$ »

$\Sigma\theta(a^2) = \theta^2(n)$ »

$\Sigma\varphi(a)\,\theta\left(\frac{n}{a}\right) = \int n$ »

$\Sigma\varphi(a)\int\frac{n}{a} = n\theta(n)$ »

$\Sigma\omega\left(\frac{n}{A}\right) = \theta(n)$ (Lejeune-Dirichlet)

$\Sigma\lambda(a)\,\theta\left(\frac{n}{a}\right) = \iota(n)$ (Cesàro)

$\Sigma\mu(a)\,\lambda\left(\frac{n}{a}\right) = \lambda(n)\,\omega(n)$ »

$\Sigma\lambda(a)\,\omega\left(\frac{n}{a}\right) = 1$ »

$\Sigma\omega(a)\,\theta\left(\frac{n}{a}\right) = \theta^2(n)$ (Cesàro)

$\dfrac{\Sigma\dfrac{a}{\varphi(a)}}{\Sigma\dfrac{\varphi(a)}{a}} = \Sigma\dfrac{1}{\varphi(a)}$ »

$\Sigma\theta\left(\frac{n}{A}\right) = \Sigma\iota(a)$ »

$\Sigma\lambda(a)\,\theta(a) = \lambda(n)\,\iota(n)$ »

$\Sigma\mu(a) = 0$ »

$\Sigma a\mu\left(\frac{n}{a}\right) = \varphi(n)$ »

$\Sigma\mu(a)\,\theta\left(\frac{n}{a}\right) = 1$ »

$\Sigma\mu(a)\int\frac{n}{a} = n$ »

$\Sigma a\mu(a)\int\frac{n}{a} = 1$ »

A, B, ... représentent les diviseurs carrés de n. Les fonctions indiquées ont été définies plus haut.

[1] Gauss avance que les personnes doctes verront aisément que les deux démonstrations de ce théorème, données par Euler et Lagrange (voir *E. M.*, 1907, p. 295), ne diffèrent pas essentiellement, et revient plusieurs fois sur des remarques analogues.

Avant lui, le marquis de l'Hospital avait dit *(Sect. con.)* que rien n'est plus propre à éclairer l'esprit que la comparaison de plusieurs démonstrations d'une même vérité; et après lui, Cesàro *(Mém. d'Ar.)* observe que « si l'on connaît plusieurs moyens pour arriver à un même but, on peut affirmer qu'il existe une méthode générale qui résume tous ces moyens, les coordonne et les explique ». Citons aussi Stouf *(Les Lois de réciprocité)* : « ... les principes qui servent aux définitions... se ramènent souvent les uns aux autres, mais chacun d'eux permet d'envisager la question sous un point de vue spécial et d'en préciser les difficultés. »

Toute démonstration n'est au fond que l'identification de deux définitions. Les sorites qui composent deux démonstrations sont virtuellement formés des mêmes syllogismes se succédant dans des ordres différents, de sorte qu'un être parfaitement intelligent n'y trouverait pas de différence essentielle et verrait clairement toutes les transformations qui conduisent de l'une à l'autre; le puissant cerveau d'un Gauss peut en embrasser plusieurs d'un coup, tandis qu'un esprit ordinaire les saisira avec peine, en les prenant une à une. Nous croyons que ce serait œuvre utile de faire saisir aux commençants, dans quelques cas choisis, les principes des démonstrations, et de leur en faire sentir l'identité. Rappelons à ce propos ce passage de la *Logique de Port-Royal* : « Les géomètres... n'ont pas assez pris garde qu'il ne suffit pas, pour avoir une parfaite science de quelque vérité d'être convaincu que cela est vrai, si de plus on ne pénètre, par des raisons prises de la nature de la chose même, pourquoi cela est vrai. »

uns par la méthode de la descente[1]. Démonstration de ce théorème : *tout nombre premier* $4+1$, *positif ou négatif, est non résidu d'un nombre premier qui lui est inférieur*. Exposition et démonstration du *theorema fundamentale*[2]. Moyen de reconnaître si a est résidu de p. Détermination des formes quadratiques des diviseurs de $x^2 - a$. Extension aux nombres composés des propriétés précédentes démontrées seulement pour des nombres premiers.

Sect. V. Cette section, qui a été l'objet de nombreux et importants travaux, est consacrée à l'étude des propriétés des formes quadratiques[3]. C'est une savante application de l'algèbre à l'analyse quadratique indéterminée, aussi remarquable par la simplicité et le choix des considérations mises en jeu, que par leur multiplicité et leur enchaînement. Celui-ci d'ailleurs, avec la densité et la longueur du texte, la rendent d'une difficulté telle que peu sont capables de la tension intellectuelle nécessaire à son étude, et qu'on a dû la scinder et la particulariser, malgré l'unité et la belle ordonnance qui ont présidé à l'édification de cette théorie. On trouvera une excellente préparation à cette étude dans la *Theory of numbers* de Mathews (Cambridge, 1892). La *Zahlentheorie*, de Lejeune-Dirichlet, la donne plus complètement.

---

[1] *Si* -1 *est un résidu,* p *ne peut être de la forme* $4-1$. Autrement, soit p le plus petit nombre de cette forme donnant le résidu -1, et soit $a^2 = pu - 1$; on peut supposer $a < p$. On a alors

$$u = \frac{a^2+1}{p} < \frac{p^2+1}{p} = p + \frac{1}{p}, \qquad \text{d'où} \qquad u \leq p .$$

Or on ne peut avoir $u = p$ car il viendrait l'égalité impossible $a^2 = p^2 - 1$: on a donc $u < p$. Remarquons que a peut être supposé pair; autrement on le remplacerait par le nombre $b = p - a$, qui donne également $b^2 = pv - 1$. On a ainsi $pu = 4+1$ d'où $u = 4-1$. Ainsi u serait $< p$ et contiendrait des facteurs premiers de la forme $4-1$, lesquels seraient à fortiori $< p$ et auraient -1 comme résidu; p ne serait donc pas le plus petit nombre dans ce cas, ce qui implique contradiction avec l'hypothèse, laquelle est donc fausse.

Gauss fait voir de même que -2 ne peut être résidu de $p = 8-3$ ni de $8-1$; ni 2 résidu de 8 ± 3; ni -3 résidu de $6-1$; ni 3 résidu de 12 ± 5.

Il semble que cette méthode n'a pas été utilisée autant qu'elle aurait pu l'être.

[2] Gauss désigne ainsi la loi de réciprocité, qu'il avait trouvée de son côté en 1796. Cette démonstration, la première qui en ait été donnée était très appréciée de son auteur, parce qu'elle n'emploie d'autre notion que celle des résidus. Lejeune-Dirichlet l'a présentée plus simplement.

[3] Diophante paraît avoir le premier imaginé les substitutions linéaires dans les expressions algébriques, afin de rendre celles-ci plus traitables, et ce procédé a été imité par tous ceux qui se sont occupés de l'analyse indéterminée. Lagrange, à qui on doit la considération des formes, les a appliquées à ces dernières; il en a déduit l'importante théorie de la réduite (voir *E. M.*, 1907, p. 290); il a aussi remarqué la substitution modulaire, comme nous l'avons vu plus haut. Legendre les a également étudiées.

Bachmann lui a consacré un volume de son importante collection (*Arithmetik der quadratischen Formen*, Leipzig, 1898).

Une première partie tout élémentaire [1] aboutit à des solutions directes et générales de problèmes déjà connus : on la trouvera exposée dans le chap. VI de la *Théorie des nombres* de Cahen (Paris, 1900). Les énoncés suivants donneront une idée des sujets traités, mais non de l'ingéniosité des mille considérations auxquelles l'auteur a recours et des remarques dont il les accompagne.

Si l'entier n est représentable par la *forme* (a, b, c), le *déterminant* D de celle-ci pris avec un signe contraire est résidu de n [2].

Si deux formes ont même déterminant et que l'une *contienne* l'autre, celle-ci contient également la première, et elles sont dites *équivalentes*.

Si la forme F contient la forme F′, et celle-ci la forme F″, F contient F″.

Pour D positif, la solution de l'équation $z^2 + Dw^2 = n^2$ se ramène à effectuer deux transformations d'une forme (a, b, c) de déterminant D et telle que n soit le p. g. c. d. des entiers a, b, c.

Définition et détermination de la *forme réduite* à déterminant positif, comme Lagrange.

Reconnaître si deux fonctions réduites de même déterminant sont équivalentes.

Trouver la transformation permettant de passer de la forme (a, b, c) à l'une quelconque de ses *formes contiguës* [3].

$$(a', b', a'') , \quad (a'', b'', a''') , \quad (a''', b''', a'''') , \ldots$$

Trouver les transformations permettant de passer d'une forme à une autre qui lui soit équivalente.

Trouver les représentations d'un nombre donné par une forme également donnée [4].

---

[1] Nous ne voulons pas dire que cette première partie serait à sa place dans un traité élémentaire des nombres : les méthodes de Lagrange conduisent aux solutions des mêmes problèmes, moins élégamment, mais sans nécessiter un aussi grand nombre de théories préliminaires. Il conviendrait de la considérer avec Gauss, non comme un but, mais comme une introduction à la deuxième partie.

[2] Voir, par exemple, *E. M.*, 1907, p. 297.

[3] Deux formes (a, b, c), $(a', b'. c')$ sont contiguës quand $a' = c'$ et que $b + b'$ est un multiple de c.

[4] Si d'une part, on peut prouver que les diviseurs premiers du nombre $af^2 + bfg + cg^2$ sont

La forme réduite (A, B, C), dans le cas d'un déterminant négatif D, non carré [1], est celle où on a :

$$\sqrt{D} + B > |A| > \sqrt{D} - B , \qquad \sqrt{D} > B > 0 .$$

On peut déterminer une *période* de réduites contiguës (A, B, C), (C, B′, C′), (C′, B″, C″), ... et elle est cyclique.

Ces considérations permettent à Gauss la solution des problèmes analogues à ceux indiqués plus haut pour le cas de D positif. Il traite ensuite le cas d'un déterminant négatif et carré, et termine la première partie par le problème général de reconnaître si une forme est contenue dans une autre forme de déterminant différent, et si cela a lieu, de trouver les transformations qui les lient; — et par là, la solution de l'équation indéterminée du second degré.

La deuxième partie, entièrement neuve mais très abstraite, commence par l'étude de la *composition* des formes [2], c'est-à-dire la transformation de la forme $AX^2 + 2BXY + CY^2$ en le produit des deux formes $ax^2 + 2bxy + cy^2$, $a'x'^2 + \dots$, au moyen de la substitution

$$X = gxx' + g'xy' + g''x'y + g'''yy' , \qquad Y = hxx' + \dots$$

Par exemple voici deux propositions tirées de cette théorie :

Les formes composées avec f et f' sont identiques à celles qui sont composées avec les formes g et g', respectivement équivalentes à f et f'.

Si deux nombres sont représentables par deux formes de

---

de l'une des formes $\alpha x^2 + \beta xy + \gamma y^2$, $\alpha' x^2 + \dots$, etc., et que d'autre part un certain nombre premier p divise un nombre de la forme $ax^2 + bxy + cy^2$, il s'ensuivra que p est de l'une des formes $\alpha x^2 + \dots$, etc.

Fermat et Euler ont trouvé plusieurs cas simples de ce théorème. Lagrange, par son théorème, a montré comment on peut réaliser en général la première condition; et Legendre, par sa loi de réciprocité, a permis de réaliser la seconde.

Gauss arrive directement à représenter un nombre n par une forme de déterminant D, en résolvant l'équation $x^2 + D \equiv 0 \pmod{n}$ et utilisant divers théorèmes qu'il a donnés précédemment.

[1] L'étude de ce cas a grandement été simplifié par Lejeune-Dirichlet.

[2] Euler et Lagrange avaient eu quelque idée de cette théorie dans leurs recherches de fonctions se reproduisant par multiplication; Legendre avait considéré plus généralement la multiplication de formes; mais c'est Gauss qui a attaqué la question dans toute son étendue.

On consultera avec fruit les *Werke* de Lejeune-Dirichlet, où sont expliqués et démontrés beaucoup de beaux problèmes de Gauss, qui ne peuvent guère être exposés ici.

Voir aussi, parmi les auteurs qui se sont occupés de la composition des formes, un mémoire du P. Pépin, paru en 1880, dans les *Atti nuovi lincei,* où la théorie de Gauss est très simplement exposée.

déterminant D, leur produit l'est par la forme composée avec ces deux formes [4].

Entre autres conséquences importantes, Gauss en tire une seconde démonstration de la loi de réciprocité.

Il considère ensuite les *formes ternaires quadratiques.*

$$\begin{pmatrix} a, & b, & c \\ d, & e, & f \end{pmatrix} = ax^2 + 2bxy + cy^2 + 2dxz + 2eyz + fz^2$$

dont l'étude dépend surtout du déterminant

$$D = ad^2 + ba^2 + cf^2 - abc - 2def$$

ainsi que de la *forme adjointe*

$$\begin{pmatrix} d^2 - bc, & e^2 - ac, & f^2 - ab \\ ad - ef, & be - df, & cf - de \end{pmatrix}$$

dont le déterminant est D^2. Il aborde l'étude des problèmes suivants :

Représentation d'un nombre donné par une forme ternaire.

Représentation d'une forme binaire donnée par une forme ternaire de déterminant donné.

Reconnaître si deux formes ternaires sont équivalentes, et dans ce cas, trouver les transformations qui les changent l'une dans l'autre.

Application à la démonstration de théorèmes énoncés par Legendre et de celui-ci d'Euler : *tout nombre entier* 8 + 3 *est la somme de trois carrés,* insuffisamment prouvé par Legendre et qui conduit immédiatement à celui-ci, de Fermat : *tout entier est la somme de trois triangulaires et de quatre carrés.*

Généralisation du théorème de Legendre sur la solubilité de l'équation $ax^2 + by^2 + cz^2 = 0$.

Dans le reste de la section V, Gauss traite un grand nombre de questions relatives à la classification des formes, et sur lesquelles s'est exercée la sagacité de nombreux géomètres.

Sect. VI. Cette section renferme d'intéressantes applications des théories qui précèdent, et dont voici les plus simples :

Résolution de l'équation $\frac{a}{pq} = \frac{x}{p} + \frac{y}{q}$ et sa généralisation.

Utilisation de la théorie des racines primitives dans celle des fractions décimales périodiques.

Emploi des considérations qui précèdent pour la recherche du quotient de deux grands nombres.

Solution de l'équation $x^2 - ky = a$ au moyen d'une méthode d'exclusion basée sur cette remarque que si $r, r', r'', \ldots$ sont les résidus du nombre quelconque E, et $\alpha, \alpha', \ldots$ les racines des équations $a + ky \equiv r$, $a + ky \equiv r'$, ... (mod. E), on peut se dispenser d'essayer les nombres contenus sous les formes $Ex + \alpha$, $Ex + \alpha'$, ... Cette méthode a reçu depuis de notables perfectionnements.

Recherche des diviseurs des nombres, d'abord par une méthode déjà employée par Euler et Legendre, puis à l'aide de la considération des résidus. (Voir E. M. 1907, pp. 292 et 36).

Sect. VII. C'est là surtout qu'éclate le génie de Gauss. La résolution complète de l'équation binôme qu'il donne dans cette section est non seulement neuve mais entièrement inattendue. Elle s'appuie sur un grand nombre de considérations algébraïco-arithmétiques, dont nous mentionnerons les plus importantes.

Soient $\alpha, \beta, \gamma \ldots$ *certaines racines de l'équation* $X = x^{p-1} + x^{p-2} + \ldots + 1 = 0$, lesquelles sont, comme on sait, les puissances de l'une d'elles ; $\varphi(t, u, v, \ldots)$ *une fonction entière et à coefficients entiers, et enfin* n *un entier quelconque ; en posant :*

$$\varphi(\alpha, \beta, \ldots) = A + B\alpha + C\alpha^2 + \ldots + N\alpha^{p-1} ,$$

on aura :

$$\varphi(\alpha^n, \beta^n, \ldots) = A + B\alpha^n + C\alpha^{2n} + \ldots$$

$$\varphi(\alpha, \beta, \ldots) + \varphi(\alpha^2, \beta^2, \ldots) + \ldots + \varphi(\alpha^p, \beta^p, \ldots) \equiv 0 .$$

Le polynôme X ne saurait avoir de diviseur entier à coefficients tous rationnels[1]. *Soit R une racine primitive de* p ; *les*

deux suites

$$\alpha^{R^1}, \alpha^{R^2}, \ldots \alpha^{R^{p-2}} \quad \text{et} \quad \alpha, \alpha^1, \alpha^2, \ldots \alpha^{p-1}$$

sont identiques à l'ordre près.

Soient $p - 1 = ef$. $R^e = h$; *si on pose :*

$$(f, \lambda) = \alpha^{\lambda} + \alpha^{\lambda h} + \alpha^{\lambda h^2} + \ldots + \alpha^{\lambda h^{f-1}},$$

le second membre est indépendant de la racine primitive choisie : on l'appelle la *période* de *f* et de λ.

On a, pour deux périodes semblables (f, λ), (f, μ) :

$$(f, \lambda)(f, \mu) = (f, \lambda + \mu) + (f, \lambda h + \mu) + (f, \lambda h^2 + \mu) + \ldots$$

Posons $(f, \lambda) = g$; *la période semblable* (f, μ) *peut se mettre sous la forme d'un polynôme entier en* g *et du degré* $e - 1$.

Si $\varphi(t, u, v, \ldots)$ *est une fonction symétrique entière des* f *racines de la période* (f, λ), *qu'on ramènera à la forme* $A + B\alpha^1 + C\alpha^2 + \ldots$, *les racines de cette expression appartenant à une même période auront des coefficients égaux.*

Soit $p - 1 = abc$; *si la période* (bc, λ) *est composée de* b *périodes* (c, λ), $c, \lambda')$, ... *de* c *termes chacune, la substitution des sommes de ces périodes dans l'expression symétrique* $\varphi(t, u, \ldots)$ *en donnera une autre de la forme*

$$A + B(c, 1) + C(c, R) + \ldots + N(c, R^{ab-1})$$

telle que les périodes appartenant à une même période de bc *termes auront les mêmes coefficients.*

Gauss applique cette belle théorie à la solution de l'équation binôme, pour les cas de $p = 17$ et $p = 19$, et à la division du cercle en $2^n + 1$ parties égales, ce nombre étant premier[2].

Viennent ensuite ces très remarquables propositions

$$(40) \qquad \Sigma\alpha^r - \Sigma\alpha^\rho = \pm\sqrt{p} \quad \text{ou} \quad \pm i\sqrt{p}\ [3]$$

$$(41) \qquad \Sigma \cos\frac{2ar\pi}{p} - \Sigma \cos\frac{2a\rho\pi}{p} = \pm\sqrt{p} \quad \text{ou} \quad = 0\ .$$

$$(42) \qquad \Sigma \sin\frac{2ar\pi}{p} - \Sigma \sin\frac{2a\rho\pi}{p} = 0 \quad \text{ou} \quad = \pm\sqrt{p}\ .$$

[1] Autrement dit, *le polynome X est irréductible.* Cette importante proposition a été démontrée de bien des façons.

[2] Richelot et Cayley ont traité le cas de $p = 257$, et Hermes, celui de $p = 65537$.

[3] Le signe du radical reste indéterminé et il y a grande difficulté à le définir. Gauss plus

Dans ces deux dernières relations, le signe Σ s'étend à tous les résidus r ou à tous les non résidus ρ ; on a d'ailleurs le signe $+$ ou le signe $-$ selon que a est résidu ou non résidu. De plus, on a le premier ou le second résultat selon que $p = 4 \pm 1$.

Faisant $p = 2m + 1$ et appelant $z = x^m - ax^{m-1} + bx^{m-2} - \ldots = 0$ l'équation donnant la période $(m, 1)$, on pourra écrire :

$$z = \mathrm{F} + \mathrm{G}(m, 1) + \mathrm{H}(m, \mathrm{R}),$$

$$4\mathrm{X} = (2\mathrm{F} - \mathrm{G} - \mathrm{H})^2 \mp p(\mathrm{H} - \mathrm{G})^2, \qquad (p = 4 \pm 1) \tag{43}$$

Le premier membre peut donc se mettre sous la forme $\mathrm{Y}^2 \mp p\mathrm{Z}^2$, comme nous l'avions annoncé. (Voir *E. M.*, 1907, p. 443.)[1]

Gauss termine par diverses considérations tendant à l'extension de ces propositions au cas des résidus cubiques.

L'ouvrage se termine par des tables de racines primitives, de résidus quadratiques et de périodes décimales.

Non moins profonds et non moins élégants sont les autres écrits arithmétiques de Gauss. Ce sont des mémoires détachés, parus dans les *Commentationes societatis Gottingensis*. Nous en rappellerons le sujet en quelques mots.

1808. Troisième démonstration du théorème fondamental, la plus simple de toutes celles qui en ont été données.

1811. *Summatio serierum quarumdam singularium*. Il s'agit des suites[2]

$$1 - \frac{1 - a^n}{1 - a} + \frac{1 - a^n}{1 - a}\frac{1 - a^{n-1}}{1 - a^2} + \ldots, \qquad \Sigma a^{x(x-1)}, \qquad \Sigma a^{x^2},$$

---

tard, Eisenstein, Lejeune-Dirichlet, Cauchy, Lebesgue, Kronecker, Mertens et d'autres encore ont fait voir que ce signe est le signe $+$.

Ajoutons que c'est dans cette même section que le symbole i a été introduit dans l'analyse, pour remplacer l'imaginaire $\sqrt{-1}$.

[1] Gauss donne les expressions des polynômes Y et Z pour $p = 3, 5, 7, 11, 13, 17, 19$ et 23. Legendre a donné celui correspondant à $p = 29$. En général on les calculera à l'aide des formules suivantes de Lejeune-Dirichlet

$$\mathrm{Y} - \mathrm{Z}\sqrt{p} = 2\Pi\left(x - e^{\frac{2r\pi i}{p}}\right), \qquad \mathrm{Y} + \mathrm{Z}\sqrt{p} = 2\Pi\left(x - e^{\frac{2\rho\pi i}{p}}\right).$$

Ce dernier, ainsi que Jacobi, en ont tiré la solution de l'équation de Pell.

[2] Jacobi en a donné de plus générales, déduites de la théorie des fonctions elliptiques, dont

d'où Gauss tire de nombreuses conséquences, dont la valeur des sommes

$$\sum_{1}^{p-1} \cos \frac{2x^2\pi}{p}, \qquad \sum_{1}^{p-1} \sin \frac{2x^2\pi}{p}, \quad [1]$$

et une nouvelle démonstration du théorème fondamental.

Ce mémoire passe pour une des plus belles productions du génie de Gauss.

1818. Cinquième et sixième démonstrations du théorème fondamental.

1828. *Theoria residuorum biquadraticorum. Commentatio prima.* Posons $p = 4\mu + 1$ et $f^2 \equiv -1$; les entiers inférieurs à p se partagent en quatre classes également nombreuses

$$r, r', \ldots ; \rho_1, \rho_1', \ldots ; \rho_2, \rho_2', \ldots ; \rho_3, \rho_3', \ldots$$

des racines des congruences

$$x^{\mu} \equiv 1, f, -1, -f.$$

Gauss examine le nombre des solutions des congruences telles que $r + r' + 1 \equiv 0$, les relations de ces nombres entre eux, et en tire la décomposition de p en une somme de deux carrés[2] ainsi que le caractère biquadratique du nombre 2 [3].

1832. *Id. Commentatio secunda.* Il étend aux nombres imaginaires les éléments de la théorie des nombres, contenus dans les quatre premières sections des *Disq. Ar.* Il en déduit le caractère biquadratique des nombres $i \pm 1$ [4], et

---

les formules sont d'ailleurs la traduction de celles de l'arithmétique quadratique, cubique et biquadratique. Voir la démonstration de Lebesgue (*Journal de Liouville*, 1840).

La théorie des nombres n'est au fond que l'étude des identités, les unes simplement algébriques, les autres concernant des suites de termes en nombre indéterminé mais fini, comme celles de Gauss, ou bien des séries élémentaires, ou des séries transcendantes, ou des intégrales définies. C'est Jacobi qui paraît avoir le premier soupçonné ces mystérieux liens qui unissent l'analyse des quantités continues à la théorie des nombres.

[1] Ces sommes ont été calculées autrement par Lejeune-Dirichlet.

[2] Soit $p = x^2 + 4y^2$, on a :

$$x \equiv \pm \frac{2\mu(2\mu - 1) \ldots (\mu + 1)}{2\mu!}.$$

[3] Gauss avait fait la découverte de ce caractère en 1805 et l'avait fait connaître en 1807 dans une lettre à Sophie Germain.

[4] Lire sur ce sujet l'intéressante *Contribution à l'étude des rés. biquadr. et cub.* de Stieljès, parue dans les *Archives néerlandaises*, 1883, et reproduite dans les *Ann. de la Fac. de Toulouse.*

Lejeune-Dirichlet a démontré la loi de réciprocité généralisée de la même manière, et a étendu ses recherches aux formes quadratiques à coefficients et indéterminées imaginaires. La théorie des nombres a reçu de la notion des imaginaires une nouvelle impulsion, grâce surtout aux travaux de Galois, de Kummer et de Dedekind.

énonce la loi générale de réciprocité biquadratique, démontrée par Eisenstein.

1831. Premières applications de la géométrie à la théorie des nombres.

Considérons deux systèmes de parallèles équidistantes se coupant sous un angle θ dont le cosinus est égal à $\frac{b}{\sqrt{ac}}$; appelons $\sqrt{a}$ les longueurs des divisions d'un des systèmes de parallèles et $\sqrt{b}$ celles de l'autre. Prenons l'une des intersections, θ, ainsi déterminées comme origine. Le carré de la distance d'une autre intersection, M, à l'origine est $ax^2 + 2bxy + cy^2$, x et y désignant les nombres de parallèles rencontrées par OM dans chacun des deux systèmes. La surface d'un des petits parallélogrammes ainsi construits représente la racine carrée du déterminant $b^2 - ac = D$.

Si on remarque que par tous ces points passent une infinité de systèmes de parallèles, il s'ensuivra que l'ensemble de ces mêmes points représentent, non seulement la forme $ax^2 + 2bxy + cy^2$, mais toutes celles qui s'en déduisent au moyen de substitutions linéaires telles que $\begin{pmatrix} \alpha\beta \\ \gamma\delta \end{pmatrix}$. Dans le cas où $\alpha\gamma - \beta\delta = -1$, le nouveau déterminant est égal au premier ; les parallélogrammes élémentaires sont égaux et il y a simple translation. Si $\alpha\gamma - \beta = -1$, le nouveau déterminant est égal à $-D$ et il y a retournement.

Les formes ternaires font l'objet d'une semblable symbolisation dans l'espace [1].

Le reste des travaux arithmétiques de Gauss se trouve dans sa correspondance et dans ses œuvres posthumes. Nous en extrayons seulement ces théorèmes (*Werke*, b. II) :

(n) désignant le nombre des fonctions entières du degré n suivant le module p et a, b, c, ... les facteurs premiers de

[1] Depuis Gauss, les plus éminents géomètres ont utilisé de même la géométrie pour la représentation des théorèmes arithmétiques et découvrir de nouvelles propriétés des nombres. Il suffira de citer les noms d'Eisenstein, Lejeune-Dirichlet, Smith, Ed. Lucas, Poincaré, Cesàro, Hurwitz, Klein, Minkowski. Gauss paraît être arrivé ainsi à ses théorèmes de la composition des formes. (Voir Klein, *Conf. sur les Math.* 1898).

n, on a :

$$p^n = n(n) + (1) + a(a) + b(b) + \cdots \tag{44}$$

$$n(n) = p^n - \Sigma p^{\frac{n}{a}} + \Sigma p^{\frac{n}{ab}} - \cdots \text{ [1]} \tag{45}$$

Le nombre des points dont les coordonnées à l'intérieur d'un cercle de rayon $\sqrt{n}$ sont des nombres entiers est [2]

$$1 + 4\left(\mathrm{E}\frac{n}{1} - \mathrm{E}\frac{n}{3} + \mathrm{E}\frac{n}{5} - \cdots\right).$$

Les sujets traités sont d'ailleurs : l'analyse des résidus, des développements sur la section VII des *Disq. Ar.*, les congruences en général, le classement des formes, la représentation géométrique des formes ternaires et des résidus biquadratiques, enfin une théorie des nombres complexes des troisième, cinquième et septième degrés.

Avec Gauss se termine la deuxième période de l'histoire de l'arithmétique. D'auxiliaire de l'algèbre qu'elle était chez ce profond analyste, — surtout dans ses *Disq. Ar.*, — elle va reprendre son autonomie et appeler à son aide l'intuition géométrique, la théorie des séries, celle des fonctions, l'analyse infinitésimale et plus tard la théorie des ensembles, qui permettront d'entrevoir et même de formuler certains des principes qui la relient à l'analyse générale ; de sorte qu'il ne sera plus chimérique d'espérer soumettre les fonctions arithmétiques aux méthodes habituelles d'étude des fonctions, après transformation de la discontinuité variable des éléments qu'elle considère en discontinuité infinitésimale. D'abord la théorie des moyennes, créée par Legendre et Gauss, mise dans tout son jour par Lejeune-Dirichlet, ne sera plus qu'une première approximation, que Tchebichef et Riemann apprendront à perfectionner par de géniales conceptions. Liouville, par sa découverte des nombres transcendants, créera une branche nouvelle et inattendue de l'arithmétique et dont

[1] Ces deux formules ont été trouvées par plusieurs auteurs avant la publication des œuvres posthumes de Gauss.

[2] Eisenstein a publié la même chose en 1844 (*Journal de Crelle*).

l'étude produira d'importants résultats en même temps qu'il ouvrira un domaine immense aux recherches des savants. Les lois numériques, — particulièrement celles des nombres premiers, — plus savamment attaquées, livreront de plus en plus leurs secrets, et l'idée de nombre entier paraîtra si primordiale qu'on pensera à en faire la base de toute l'analyse mathématique.

Quoique la littérature arithmétique nous soit assez connue, le caractère élémentaire que nous avons tenu à laisser à la présente notice, et surtout la défiance que nous avons de nos modestes lumières, ne nous permettent pas d'en dire davantage sur cet important sujet, dont nous avons voulu seulement essayer d'expliquer les origines.

A. Aubry (Dijon).

LE THÉORÈME DE PYTHAGORE EN MÉTAGÉOMÉTRIE

Dans un article publié au 42e volume du *Journal de Crelle* (année 1851, page 280), et paru la veille de sa mort, Gudermann donnait pour le triangle rectangle sphérique de côtés a, b, c l'énoncé et la démonstration d'un théorème analogue à celui de Pythagore pour le triangle rectangle plan. Si S, S′ et S″ sont les aires des carrés ayant pour côtés respectifs a, b et c, le théorème de Gudermann peut s'exprimer par la relation

$$\mathrm{L}\left(\frac{1}{4}\,\mathrm{S}\right) = \mathrm{L}\left(\frac{1}{4}\,\mathrm{S}'\right) + \mathrm{L}\left(\frac{1}{4}\,\mathrm{S}''\right),$$

en posant pour abréger,

$$\mathrm{L}(x) = \log \sqrt{\frac{1+\sin x}{1-\sin x}} = \mathrm{Arg.}\, th\,(\sin x)\ .$$