

Cambridge University Press
978-1-108-00173-1 - Essai Sur La Theorie Des Nombres
Adrien-Marie Legendre
Frontmatter
[More information](#)

CAMBRIDGE LIBRARY COLLECTION

Books of enduring scholarly value

Mathematical Sciences

From its pre-historic roots in simple counting to the algorithms powering modern desktop computers, from the genius of Archimedes to the genius of Einstein, advances in mathematical understanding and numerical techniques have been directly responsible for creating the modern world as we know it. This series will provide a library of the most influential publications and writers on mathematics in its broadest sense. As such, it will show not only the deep roots from which modern science and technology have grown, but also the astonishing breadth of application of mathematical techniques in the humanities and social sciences, and in everyday life.

Essai sur la théorie des nombres

Adrien-Marie Legendre (1752–1833), one of the great French mathematicians active in the Revolutionary period, made important contributions to number theory, statistics, mathematical analysis and algebra. He taught at the École Militaire, where he was a colleague of Laplace, and made his name with a paper on the trajectory of projectiles which won a prize of the Berlin Academy in 1782, and brought him to the attention of Lagrange. In 1794 he published *Eléments de géométrie*, which remained a textbook for over 100 years. The first edition of his *Essai sur la théorie des nombres* was published in 1798, and the much improved second edition, which is offered here, in 1808. In it Legendre had taken account of criticism by Gauss of the mathematical proofs in the first edition, though he was bitter at the manner in which his younger rival had claimed credit for some of his solutions.

Cambridge University Press
978-1-108-00173-1 - Essai Sur La Theorie Des Nombres
Adrien-Marie Legendre
Frontmatter
[More information](#)

Cambridge University Press has long been a pioneer in the reissuing of out-of-print titles from its own backlist, producing digital reprints of books that are still sought after by scholars and students but could not be reprinted economically using traditional technology. The Cambridge Library Collection extends this activity to a wider range of books which are still of importance to researchers and professionals, either for the source material they contain, or as landmarks in the history of their academic discipline.

Drawing from the world-renowned collections in the Cambridge University Library, and guided by the advice of experts in each subject area, Cambridge University Press is using state-of-the-art scanning machines in its own Printing House to capture the content of each book selected for inclusion. The files are processed to give a consistently clear, crisp image, and the books finished to the high quality standard for which the Press is recognised around the world. The latest print-on-demand technology ensures that the books will remain available indefinitely, and that orders for single or multiple copies can quickly be supplied.

The Cambridge Library Collection will bring back to life books of enduring scholarly value across a wide range of disciplines in the humanities and social sciences and in science and technology.

Cambridge University Press
978-1-108-00173-1 - Essai Sur La Theorie Des Nombres
Adrien-Marie Legendre
Frontmatter
[More information](#)

Essai sur la théorie des nombres

ADRIEN-MARIE LEGENDRE



CAMBRIDGE
UNIVERSITY PRESS

Cambridge University Press
978-1-108-00173-1 - Essai Sur La Theorie Des Nombres
Adrien-Marie Legendre
Frontmatter
[More information](#)

CAMBRIDGE UNIVERSITY PRESS

Cambridge New York Melbourne Madrid Cape Town Singapore São Paulo Delhi

Published in the United States of America by Cambridge University Press, New York

www.cambridge.org

Information on this title: www.cambridge.org/9781108001731

© in this compilation Cambridge University Press 2009

This edition first published 1808

This digitally printed version 2009

ISBN 978-1-108-00173-1

This book reproduces the text of the original edition. The content and language reflect the beliefs, practices and terminology of their time, and have not been updated.

ESSAI
SUR LA THÉORIE
DES NOMBRES;

PAR A. M. LEGENDRE,

Membre de l'Institut et de la Légion d'Honneur, Conseiller
titulaire de l'Université Impériale.

SECONDE ÉDITION.

PARIS,

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

1808.

AVERTISSEMENT.

ON a tâché de faire disparaître dans cette seconde Édition la plus grande partie des imperfections ou même des erreurs qui étaient restées dans la première, malgré les soins qu'on y avait apportés. Les changemens sont tels, qu'une moitié environ du volume est devenue un ouvrage nouveau.

L'Introduction a été refondue presque en entier, et corrigée d'une erreur qui s'était glissée dans les derniers articles.

La première partie a été augmentée de quelques Théorèmes sur les équations indéterminées, et d'une Méthode nouvelle pour l'approximation des racines imaginaires.

Dans la deuxième partie la démonstration de la loi de réciprocité, entre deux nombres premiers, a été perfectionnée à quelques égards.

La théorie contenue dans la troisième partie a été présentée d'une manière nouvelle et entièrement rigoureuse.

La quatrième partie a été augmentée de plusieurs paragraphes sur différens sujets. Dans l'un d'eux on démontre que toute progression arithmétique (excepté celles dont tous les termes ont un commun diviseur) contient une infinité de nombres premiers.

vj

AVERTISSEMENT.

Enfin il a été ajouté une cinquième partie où l'on expose avec tout le détail nécessaire, la belle théorie de la résolution de l'équation $x^n - 1 = 0$, donnée par M. Gauss, dans ses *Disquisitiones arithmetice*.

Cet ouvrage qui parut à Léipsick en 1801, et qui plaça tout d'un coup son auteur au rang des Analystes les plus célèbres, contient beaucoup de choses analogues à celles qui sont traitées dans l'Essai sur la Théorie des Nombres, publié en 1798. Il contient particulièrement une démonstration directe et fort ingénieuse de la loi de réciprocité déjà citée; démonstration qu'on se proposait d'insérer avec des développemens plus étendus, dans cette seconde Edition. Mais l'Auteur étant parvenu depuis à en trouver une beaucoup plus simple et plus élégante, on a exposé de préférence cette dernière dans le § VII de la quatrième partie.

On aurait désiré enrichir cet Essai d'un plus grand nombre des excellens matériaux qui composent l'ouvrage de M. Gauss: mais les méthodes de cet auteur lui sont tellement particulières qu'on n'aurait pu, sans des circuits très-étendus, et sans s'assujétir au simple rôle de traducteur, profiter de ses autres découvertes.

PRÉFACE

DE LA PREMIÈRE ÉDITION.

A EN juger par différens fragmens qui nous restent, et dont quelques-uns sont consignés dans Euclide, il paraît que les anciens Philosophes avaient fait des recherches assez étendues sur les propriétés des nombres. Mais il leur manquait deux instrumens pour approfondir cette science ; l'art de la numération qui sert à exprimer les nombres avec beaucoup de facilité, et l'Algèbre qui généralise les résultats et qui peut opérer également sur les connues et les inconnues. L'invention de l'un et l'autre de ces arts dut donc influer beaucoup sur les progrès de la science des nombres. Aussi voit-on que l'ouvrage de Diophante d'Alexandrie, le plus ancien auteur d'Algèbre qu'on connaisse, est entièrement consacré aux nombres, et renferme des questions difficiles résolues avec beaucoup d'adresse et de sagacité.

Depuis Diophante jusqu'au temps de Viète et de Bachet, les Mathématiciens continuèrent de s'occuper des nombres, mais sans beaucoup de succès, et sans faire avancer sensiblement la science.

Viète, en ajoutant de nouveaux degrés de perfection à l'Algèbre, résolut plusieurs problèmes difficiles sur les nombres. Bachet, dans son ouvrage intitulé *Problèmes plaisans et délec-*

viii

PRÉFACE.

tables, résolut l'équation indéterminée du premier degré par une méthode générale et fort ingénieuse. On doit à ce même savant un excellent commentaire sur Diophante, qui fut depuis enrichi des notes marginales de Fermat.

Fermat, l'un des Géomètres dont les travaux contribuèrent le plus à accélérer la découverte des nouveaux calculs, cultiva avec un grand succès la science des nombres, et s'y fraya des routes nouvelles. On a de lui un grand nombre de Théorèmes intéressans, mais il les a laissés presque tous sans démonstration. C'était l'esprit du temps de se proposer des problèmes les uns aux autres. On cachait le plus souvent sa méthode, afin de se réserver des triomphes nouveaux tant pour soi que pour sa nation; car il y avait surtout rivalité entre les Géomètres français et les anglais. De là il est arrivé que la plupart des démonstrations de Fermat ont été perdues, et le peu qui nous en reste, nous fait regretter d'autant plus celles qui nous manquent.

Depuis Fermat jusqu'à Euler, les Géomètres, livrés entièrement à la découverte ou à l'application des nouveaux calculs, ne s'occupèrent point de la Théorie des Nombres. Euler, le premier, s'attacha à cette partie; les nombreux Mémoires qu'il a publiés sur cette matière dans les Commentaires de Pétersbourg, et dans d'autres ouvrages, prouvent combien il avait à cœur de faire faire à la science des Nombres les mêmes progrès dont la plupart des autres parties des Mathématiques lui étaient redevables. Il est à croire aussi qu'Euler avait un goût particulier pour ce genre de recherches, et qu'il s'y livrait avec une sorte de passion, comme il arrive à presque tous ceux qui s'en occupent. Quoi qu'il en soit, ses savantes recherches

PRÉFACE.

ix

le conduisirent à démontrer deux des principaux Théorèmes de Fermat, savoir, 1°. que si a est un nombre premier, et x un nombre quelconque non divisible par a , la formule $x^{a-1} - 1$ est toujours divisible par a ; 2°. que tout nombre premier de forme $4n + 1$, est la somme de deux quarrés.

Une multitude d'autres découvertes importantes se font remarquer dans les Mémoires d'Euler. On y trouve la théorie des diviseurs de la quantité $a^n \pm b^n$, le traité de *partitione numerorum*, qui est inséré aussi dans son *Introd. in Anal. infinit.*, l'usage des facteurs imaginaires ou irrationnels dans la résolution des équations indéterminées, la résolution générale des équations indéterminées du second degré, en supposant qu'on en connaisse une solution particulière; la démonstration de beaucoup de Théorèmes sur les puissances des nombres, et particulièrement de ces propositions négatives avancées par Fermat; que la somme ou la différence de deux cubes ne peut être un cube, et que la somme ou la différence de deux bi-quarrés ne peut être un quarré. Enfin on trouve dans ces mêmes écrits un grand nombre de questions indéterminées résolues par des artifices analytiques très-ingénieux.

Euler a été pendant long-temps presque le seul Géomètre qui se soit occupé de la Théorie des Nombres. Enfin Lagrange est entré aussi dans la même carrière, et ses premiers pas ont été signalés par des succès égaux à ceux qu'il avait déjà obtenus dans des recherches d'un genre plus sublime. Une méthode générale pour résoudre les équations indéterminées du second degré, et, ce qui était plus difficile, une méthode pour les résoudre en nombres entiers, fut le coup d'essai de ce savant illustre; bientôt après il appliqua les fractions continues à cette

b

x

PRÉFACE.

branche d'analyse; il démontra le premier que la fraction continue égale à la racine d'une équation rationnelle du second degré, devait être périodique, et il en conclut que le problème de Fermat, concernant l'équation $x^2 - Ay^2 = 1$, est toujours résoluble; proposition qui n'avait pas encore été établie d'une manière rigoureuse, quoique plusieurs Géomètres eussent donné des méthodes pour la résolution de cette équation.

Le même savant, par des recherches ultérieures qui sont consignées dans les Mémoires de Berlin, a démontré le premier que tout nombre entier est la somme de quatre carrés; on lui doit également plusieurs autres démonstrations importantes, mais la plus remarquable de ses découvertes est une méthode générale de laquelle découlent comme corollaires une infinité de Théorèmes sur les nombres premiers.

Cette méthode, singulièrement féconde, est fondée sur la considération des formes tant quadratiques que linéaires qui conviennent aux diviseurs de la formule $t^2 + au^2$, où t et u sont deux indéterminées, et a un nombre donné. Il restait cependant à établir, d'une manière générale, la relation qui doit exister entre les formes linéaires et les formes quadratiques appliquées aux nombres premiers; car au défaut du principe qui contient cette relation (1), la Théorie de Lagrange, qui donne une infinité de Théorèmes pour les nombres premiers $4n + 3$, n'en fournit qu'un très-petit nombre relatifs aux nombres premiers $4n + 1$.

Un Mémoire que j'ai publié dans le volume de l'Académie

(1) Voyez sur cet objet les Mémoires de l'Académie des Sciences de Berlin, année 1775, pag. 350 et 352.

PRÉFACE.

xj

des Sciences pour l'année 1785, offre les moyens de démontrer le principe dont il s'agit, et renferme d'ailleurs des propositions qui paraissent avancer la science des nombres. J'y ai donné 1°. la démonstration d'un Théorème pour juger de la possibilité ou de l'impossibilité de toute équation indéterminée du second degré, ramenée à la forme $ax^2 + by^2 = cz^2$; 2°. la démonstration d'une loi générale qui existe entre deux nombres premiers quelconques, et qu'on peut appeler *loi de réciprocité*; 3°. l'application de cette loi à diverses propositions, et son usage, tant pour perfectionner la Théorie de Lagrange, que pour vaincre d'autres difficultés du même genre.

Le même Mémoire contient en outre l'ébauche d'une théorie entièrement nouvelle sur les nombres considérés en tant qu'ils sont décomposables en trois quarrés; théorie à laquelle appartient le fameux Théorème de Fermat, qu'un nombre quelconque est la somme de trois triangulaires, et cet autre Théorème du même auteur, que tout nombre premier $8n + 7$ est de la forme $p^2 + q^2 + 2r^2$.

Depuis l'époque de la publication de ce Mémoire, je me suis occupé à diverses reprises de développer les vues qu'il contient, et d'apporter quelques perfectionnemens à différens points de la Théorie des Nombres ou de l'Analyse indéterminée (1). Mes recherches à cet égard ayant été suivies de

(1) Je ne sépare point la Théorie des Nombres de l'Analyse indéterminée, et je regarde ces deux parties comme ne faisant qu'une seule et même branche de l'Analyse algébrique. En effet, il n'est pas de Théorème sur les nombres qui ne soit relatif à la résolution d'une ou de plusieurs équations indéterminées. Ainsi quand on assure, d'après Fermat, que tout nombre premier $4n + 1$ est la somme de deux quarrés, c'est comme

xij

PRÉFACE.

quelques succès, je me proposais d'abord d'en publier le résultat dans un Mémoire particulier ; j'ai cru ensuite devoir profiter de cette occasion pour traiter la Théorie des Nombres avec plus d'étendue qu'on ne l'a fait jusqu'à présent, et en y comprenant le résultat des principales recherches d'Euler et de Lagrange sur la même matière.

C'est ainsi que je me suis déterminé à composer l'ouvrage que j'offre en ce moment au Public ; je le donne non comme un traité complet, mais simplement comme un essai qui fera connaître à-peu-près l'état actuel de la science, et qui contribuera peut-être à en accélérer les progrès.

si on disait que l'équation $A = y^2 + z^2$ est toujours résoluble tant que A est un nombre premier de la forme $4n + 1$. On peut ajouter que dans ce même cas l'équation $A = y^2 + z^2$ n'aura jamais qu'une solution, ce qui est un second Théorème contenant une propriété caractéristique des nombres premiers $4n + 1$.

TABLE DES MATIÈRES.

INTRODUCTION,

Contenant des notions générales sur les Nombres.

| | |
|--|--------|
| O _N considère les nombres en tant qu'ils résultent de la multiplication de plusieurs facteurs, | pag. 1 |
| Des différens diviseurs d'un nombre donné, et de leur somme, | 4 |
| On détermine combien il y a de nombres plus petits que N et premiers à N , | 5 |
| On cherche combien de fois un même nombre premier θ peut être facteur dans le produit $1.2.3\dots N$, | 8 |
| Propriétés générales des nombres premiers: leur répartition en diverses progressions arithmétiques dont la raison est constante, | 10 |

PREMIÈRE PARTIE.

EXPOSITION DE DIVERSES MÉTHODES ET PROPOSITIONS RELATIVES A L'ANALYSE INDÉTERMINÉE.

| | |
|---|----|
| § I. <i>Des fractions continues,</i> | 14 |
| Définition des quotiens-complets et des fractions convergentes, | 15 |
| Propriétés générales des fractions convergentes, | 16 |
| Condition pour qu'une fraction donnée soit comprise parmi les fractions convergentes, | 20 |
| Application à l'équation $p^2 - Aq^2 = \pm D$, | 21 |
| Des fractions continues symétriques, | 22 |
| § II. <i>Résolution des équations indéterminées du premier degré,</i> | 24 |
| § III. <i>Méthode pour résoudre en nombres rationnels les équations indéterminées du second degré,</i> | 27 |
| Réduction de l'équation générale à la forme $x^2 - By^2 = Az^2$, | 28 |
| Résolution de l'équation $x^2 - y^2 = Az^2$, | 29 |
| On donne, d'après Lagrange, les moyens de diminuer successivement les coefficients A et B , jusqu'à ce que l'un des deux soit égal à l'unité, | 30 |
| § IV. <i>Théorème pour juger de la possibilité ou de l'impossibilité de toute équation indéterminée du second degré,</i> | 35 |
| Une telle équation étant réduite à la forme $ax^2 + by^2 = cz^2$, dans laquelle a, b, c sont positifs et dégagés de tout facteur carré; elle sera possible, s'il y a trois | |

TABLE DES MATIÈRES.

entiers λ, μ, ν , tels que les trois quantités $\frac{a\lambda^2 + b}{c}, \frac{c\mu^2 - b}{a}, \frac{c^2 - a}{b}$, soient des entiers; autrement elle sera impossible, pag. 41

§ V. Développement de la racine d'un nombre non-quarré en fraction continue, 42

Loi générale du développement, 43

On prouve que la fraction continue est périodique, 45

On en conclut que l'équation $x^2 - Ay^2 = 1$ admet toujours une infinité de solutions, 47

§ VI. Résolution en nombres entiers de l'équation indéterminée.....

$x^2 - Ay^2 = \pm D$, D étant $< \sqrt{A}$, 48

Condition pour que l'équation soit possible, 51

Formules générales qui contiennent une infinité de solutions de l'équation proposée, 52

§ VII. Théorèmes sur la possibilité des équations de la forme.....

$Mx^2 - Ny^2 = \pm 1$, ou ± 2 , 54

A étant un nombre premier $4n + 1$, l'équation $x^2 - Ay^2 = -1$ est toujours possible, 55

A étant un nombre premier $8n + 3$, l'équation $x^2 - Ay^2 = -2$ est toujours possible, *ibid.*

A étant un nombre premier $8n + 7$, l'équation $x^2 - Ay^2 = 2$ est toujours possible, *ibid.*

M et N étant deux nombres premiers $4n + 3$, l'équation $Mx^2 - Ny^2 = +1$, ou l'équation $Mx^2 - Ny^2 = -1$, sera toujours possible, 56

Les mêmes théorèmes se déduisent de la considération du quotient-moyen dans le développement de \sqrt{A} en fraction continue, 57

Moyen direct de mettre A sous la forme $D^2 + I^2$, lorsque A est un nombre premier $4n + 1$, ou lorsqu'en général A rend possible l'équation $x^2 - Ay^2 = -1$, 60

§ VIII. Réduction de la formule $Ly^2 + Myz + Nz^2$ à l'expression la plus simple, 61

Cette réduction se fait par la méthode de Lagrange (Mém. de Berlin, an. 1775). On démontre ensuite, par une méthode particulière, que deux formules $py^2 + 2qyz + rz^2, p'y^2 + 2q'yz + r'z^2$, dans lesquelles $pr - q^2$ et $p'r' - q'^2$ sont égales à un même nombre positif A , sont différentes l'une de l'autre, si elles satisfont à la condition que le coefficient-moyen ne surpasse aucun des extrêmes, 66

§ IX. Développement de la racine d'une équation du second degré en fraction continue, 68

Loi générale du développement, la même que pour les simples racines quarrées, 70

On prouve que la fraction continue est périodique, 71

On détermine l'expression générale des diverses fractions convergentes qui répondent à un même quotient dans les périodes successives, 73

TABLE DES MATIÈRES.

xv

- Considérations diverses sur la résolution de l'équation $fy^2 + gyz + hz^2 = \pm D$, pag. 76
- § X. *Comparaison des fractions continues résultantes du développement des deux racines d'une même équation du second degré*, 80
- On prouve que la période comprise dans le développement d'une racine est l'inverse de la période comprise dans le développement de l'autre racine, *ibid.*
- § XI. *Résolution en nombres entiers de l'équation $Ly^2 + Myz + Nz^2 = \pm H$* , 88
- Il ne peut y avoir une infinité de solutions que lorsque $M^2 - 4LN$ est un nombre positif non-quarré : on résout alors l'équation en la ramenant au cas où le second membre $= \pm 1$, 92
- On confirme par divers exemples la remarque déjà faite, que les formules obtenues par le développement d'une racine contiennent implicitement le résultat du développement des deux racines, 100
- § XII. *Démonstration d'une proposition supposée dans les paragraphes précédens*, 102
- Etant proposée l'équation $fy^2 + gyz + hz^2 = \pm H$, dans laquelle on a $H < \frac{1}{2}\sqrt{g^2 - 4fh}$; si cette équation est résoluble, la fraction $\frac{y}{z}$ se trouvera parmi les fractions convergentes vers une racine de l'équation $fx^2 + gx + h = 0$, 105
- Les cas qui semblent faire exception sont néanmoins compris dans les formules générales, 109
- § XIII. *Réduction ultérieure des formules $Ly^2 + Myz + Nz^2$, lorsque $M^2 - 4LN$ est égal à un nombre positif*, 111
- On donne pour cet objet une méthode directe fondée sur le développement en fraction continue d'une racine de l'équation $Lx^2 + Mx + N = 0$, 113
- Les Tables I et II, construites d'après cette théorie, offrent les réductions toutes faites pour un grand nombre de formules. Voyez le Recueil des Tables.
- § XIV. *Développement en fraction continue de la racine d'une équation d'un degré quelconque*, 121
- Méthode générale due à Lagrange. — Perfectionnement de cette méthode par le même auteur, 123
- Observation sur le nombre des quotiens nouveaux qu'on peut déduire des quotiens déjà trouvés, 126
- Exemples de développemens qui offrent des rapports remarquables entre les racines, 130
- Observations sur la solution de quelques équations indéterminées d'un degré élevé, 133
- Rapport remarquable entre les racines des transformées successives et les racines de la proposée, 139
- Développement en fraction continue d'une racine réelle de toute équation proposée, 143
- Méthode pour obtenir la première approximation dans les équations algébriques, 145
- Nouvelle méthode pour l'approximation des racines imaginaires, 151

xvj

TABLE DES MATIÈRES.

Cette méthode prouve directement que la valeur de l'inconnue peut toujours être représentée par $a + \ell\sqrt{-1}$, a et ℓ étant réels, pag. 153

§ XV. *Résolution en nombres entiers de l'équation indéterminée....*
 $Ly^n + My^{n-1}z + Ny^{n-2}z^2 \dots + Vz^n = \pm H$, 154

On ramène cette équation au cas où le second membre $= \pm 1$, *ibid.*

Recherches sur les moyens de déterminer y et z , pour que la fonction homogène $at^n + bt^{n-1}u + ct^{n-2}u^2 \dots + ku^n$ soit un *minimum*, 155

On prouve que dans le cas du *minimum* la fraction $\frac{t}{u}$ doit être l'une des fractions convergentes vers une racine réelle de l'équation $ax^n + bx^{n-1} + cx^{n-2} \dots + k = 0$, ou vers la partie réelle d'une racine imaginaire de la même équation, 159

SECONDE PARTIE.

PROPRIÉTÉS GÉNÉRALES DES NOMBRES.

§ I. *Théorèmes sur les nombres premiers*, 166

Si c est un nombre premier et N un nombre quelconque non-divisible par c , la quantité $N^{c-1} - 1$ sera divisible par c , *ibid.*

Si n est un nombre premier, le produit $1.2.3 \dots (n-1)$, augmenté de l'unité, sera divisible par n , 167

Si un polynome du degré m divise $x^{c-1} - 1$, c étant un nombre premier, il y aura toujours m valeurs de x , comprises entre $-\frac{1}{2}c$ et $+\frac{1}{2}c$, qui rendront ce polynome divisible par c , 169

Le nombre premier c sera diviseur de $x^2 + N$, si la quantité $(-N)^{\frac{c-1}{2}} - 1$ est divisible par c ; dans le cas contraire, il ne pourra diviser $x^2 + N$, 170

Explication du caractère abrégé $\left(\frac{N}{c}\right)$, *ibid.*

§ II. *Recherche de la forme qui convient aux diviseurs de la formule $t^2 + au^2$, t et u étant premiers entre eux*, 172

On prouve que tout diviseur de cette formule peut être représenté par une formule de même degré $py^2 + 2qyz + rz^2$, dans laquelle on a $pr - q^2 = a$, et $2q < p$ et r , 173

§ III. *Application de la théorie précédente à diverses formules $t^2 + u^2$, $t^2 + 2u^2$, $t^2 - 2u^2$, etc.*, 175

On prouve que la somme de deux carrés premiers entre eux, $t^2 + u^2$, ne peut avoir pour diviseur qu'une somme semblable $y^2 + z^2$, *ibid.*

Il en est de même des formules $t^2 + 2u^2$, $t^2 - 2u^2$, chacune n'admettant que des diviseurs qui lui sont semblables, 176

TABLE DES MATIÈRES.

xvii

| | |
|--|--------------|
| Propriétés générales et caractéristiques des nombres premiers $8n + 1$, $8n + 3$, $8n + 5$, $8n + 7$, | pag. 180 |
| Valeur du symbole $\left(\frac{2}{c}\right)$ selon l'espèce du nombre premier c , | 181 |
| § IV, où l'on prouve que tout nombre entier est la somme de quatre ou d'un moindre nombre de carrés, | 182 |
| On démontre que B et C étant deux nombres quelconques donnés, il y a toujours des valeurs de t et u telles que $t^2 - Bu^2 - C$ est divisible par un nombre pre- mier donné A , | <i>ibid.</i> |
| Le produit de la formule $p^2 + q^2 + r^2 + s^2$ par une formule semblable est également la somme de quatre carrés, | 184 |
| Un nombre quelconque est la somme de quatre carrés, | 186 |
| Développement des différens cas du théorème de Fermat sur les nombres polygones, | 188 |
| § V. De la forme linéaire qui convient aux diviseurs de la formule $a^n \pm 1$, a et n étant des nombres donnés, | 191 |
| Tout nombre premier p qui divise la formule $a^n + 1$ est de la forme $2nx + 1$, ou au moins il doit diviser une formule plus simple $a + 1$, dans laquelle ω est le quotient de n divisé par un nombre impair, | 192 |
| Tout nombre premier p qui divise la formule $a^n - 1$ doit être compris dans la forme $nx + 1$, ou au moins doit diviser la formule $a^\omega - 1$, dans laquelle ω est sous-multiple de n , | 195 |
| Applications diverses où l'on détermine des nombres premiers très-grands, | 197 |
| § VI. Théorème contenant une loi de réciprocité qui existe entre deux nombres premiers quelconques, | 198 |
| Si les nombres premiers m et n ne sont pas tous deux de la forme $4x + 3$, on aura généralement $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)$, et s'ils sont tous deux de cette forme, on aura... | |
| $\left(\frac{m}{n}\right) = -\left(\frac{n}{m}\right)$, | <i>ibid.</i> |
| Théorèmes divers, dont plusieurs dépendent de la loi précédente, | 204 |
| Démonstration de deux conclusions générales auxquelles Euler est parvenu par voie d'induction, dans ses <i>Opuscula Analytica</i> , tom. I, | 206 |
| § VII. Usage du théorème précédent pour connaître si un nombre pre- mier c divise la formule $x^2 + a$, | 208 |
| Algorithme très-simple pour cet objet, | <i>ibid.</i> |
| Développement d'un grand nombre de cas où l'on peut déterminer <i>a priori</i> la va- leur de x , | 211 |
| § VIII. De la manière de déterminer x pour que $x^2 + a$ soit divisible par un nombre composé quelconque N , | 214 |

| xviii | TABLE DES MATIÈRES. | pag. |
|---|----------------------------|--------------|
| Solution du problème général, | | 214 |
| Du cas particulier où N a pour facteur 2^m , | | 215 |
| Détermination du nombre des solutions, | | 217 |
| § IX. Résolution des équations symboliques $\left(\frac{x}{c}\right) = 1$, $\left(\frac{x}{c}\right) = -1$, | | 220 |
| § X. Recherche des formes linéaires qui conviennent aux diviseurs de la formule $t^2 + cu^2$, | | 223 |
| Théorèmes par lesquels on détermine les formes linéaires des diviseurs de la formule $t^2 + cu^2$, c étant premier ou double d'un premier, | | <i>ibid.</i> |
| On détermine <i>a priori</i> les formes linéaires de ces mêmes diviseurs, lorsque c est le produit de deux ou de plusieurs nombres premiers, | | 231 |
| En général les diviseurs d'une même formule $t^2 \pm cu^2$ se partagent en un nombre déterminé de groupes, composés chacun d'un même nombre de formes linéaires $2cx + a$, ou $4cx + a$, | | <i>ibid.</i> |
| Méthode abrégée pour trouver, par le moyen des diviseurs quadratiques, toutes les formes linéaires des diviseurs, | | 232 |
| § XI. Explication des Tables III, IV, V, VI et VII, | | 244 |
| Ces Tables présentent, pour chaque formule $t^2 + cu^2$ comprise dans leurs limites, le système de ses diviseurs quadratiques et des diviseurs linéaires correspondans. | | |
| § XII. Suite de théorèmes contenus dans les Tables précitées, | | 255 |
| On démontre en général que si $4cx + a$ est l'une des formes linéaires qui conviennent aux diviseurs de la formule $t^2 \pm cu^2$, tout nombre premier compris dans la forme $4cx + a$, sera diviseur de la formule $t^2 \pm cu^2$, et par conséquent sera de l'une des formes quadratiques qui répondent à la forme $4cx + a$. On tire de là autant de théorèmes particuliers qu'il y a de formes linéaires dans les Tables, | | 260 |
| § XIII. Autres théorèmes concernant les formes quadratiques des nombres, | | 263 |
| Tout nombre premier A qui divise la formule $t^2 \pm cu^2$, ne peut appartenir qu'à l'un des diviseurs quadratiques de cette formule, | | <i>ibid.</i> |
| Tout nombre premier A qui est de la forme $y^2 + az^2$, ne peut être qu'une fois de cette forme, | | 265 |
| On détermine le nombre de manières dont un même nombre composé A peut être de la forme $y^2 + az^2$, d'où l'on déduit la solution d'un problème de Fermat, | | 269 |
| Tout nombre A , premier ou double d'un premier, compris dans la formule $py^2 + aqyz + rz^2$, où $pr - q^2$ est un nombre positif, n'y peut être compris que d'une manière, sauf le cas des diviseurs <i>bifides</i> , | | 271 |
| § XIV. Sur les moyens de trouver un nombre premier plus grand qu'un nombre donné, | | 279 |
| Tableau de diverses formules propres à exprimer des nombres premiers, si une condition est remplie, | | 282 |

TABLE DES MATIÈRES.

xix

- Explication de la propriété qu'ont certaines formules de contenir une suite assez étendue de nombres premiers,** pag. 284
- § XV. *Usage des théorèmes précédens pour reconnaître si un nombre donné est premier, ou s'il ne l'est pas,* 286
- On ajoute aux autres moyens déjà indiqués le développement en fraction continue de la racine du nombre donné, ou d'un de ses multiples, 288

TROISIÈME PARTIE.

THÉORIE DES NOMBRES CONSIDÉRÉS COMME DÉCOMPOSABLES
EN TROIS QUARRÉS.

- § I. *Définition de la forme trinaire. Nombres et diviseurs quadratiques auxquels cette forme peut ou ne peut pas convenir,* 293
- § II. *Correspondance entre les formes trinaires du nombre c et les diviseurs trinaires de la formule $t^2 + cu^2$,* 296
- Si un diviseur quadratique de la formule $t^2 + cu^2$ est décomposable en trois carrés, toute manière de faire cette décomposition, c'est-à-dire toute forme trinaire de ce diviseur, donnera une valeur trinaire correspondante de c , *ibid.*
- Réciproquement, étant donnée une forme trinaire du nombre c , on pourra toujours trouver un diviseur quadratique trinaire de la formule $t^2 + cu^2$, correspondante à la valeur donnée, 298
- On démontre généralement 1°. qu'il ne peut y avoir qu'un diviseur quadratique qui répondra à la valeur trinaire donnée de c ; 2°. que ce diviseur ne pourra avoir qu'une seule forme trinaire correspondante à cette même valeur, sauf le cas des diviseurs bifides où il y en a deux, 305
- § III. *Théorèmes concernant les diviseurs quadratiques trinaires,* 306
- Si le nombre c est premier ou double d'un premier, la formule $t^2 + cu^2$ aura autant de diviseurs quadratiques trinaires qu'il y a de formes trinaires du nombre c , et chacun de ces diviseurs ne pourra avoir qu'une seule forme trinaire, 308
- Si le nombre N est compris dans un diviseur trinaire de la formule $t^2 + cu^2$, réciproquement le nombre c sera compris dans un diviseur trinaire de la formule $t^2 + Nu^2$. De plus les valeurs trinaires correspondantes de N et c seront les mêmes dans les deux cas, 309
- Caractères qui distinguent les diviseurs quadratiques *réci-proques*, des diviseurs *non-réci-proques*, 318
- Les diviseurs quadratiques de la formule $t^2 + cu^2$ se distinguent encore en diviseurs de première et diviseurs de deuxième espèce, 319
- Si le nombre c est premier ou double d'un premier, tout diviseur quadratique de première espèce est un diviseur *réci-proque*, 320
- Quel que soit c , pourvu qu'il ne soit ni de la forme $4n$, ni de la forme $8n + 7$,

TABLE DES MATIÈRES.

| | |
|--|--------------|
| les diviseurs quadratiques de la formule $t^2 + cu^2$ en contiendront toujours au moins un qui sera réciproque, | pag. 321 |
| Tout diviseur quadratique réciproque de la formule $t^2 + cu^2$ est un diviseur trinaire, et ce diviseur a autant de formes trinaires qu'il y a d'unités dans 2^{i-1} , i étant le nombre des facteurs premiers, impairs et inégaux qui divisent c , | 322 |
| Corollaires généraux qui offrent toutes les propriétés de la Table VIII, continuée indéfiniment, | 335 |
| Tout nombre impair, excepté seulement ceux de la forme $8n + 7$, est la somme de trois carrés, | 336 |
| Tout nombre entier est la somme de trois triangulaires, | 337 |
| Tout nombre double d'un impair est la somme de trois carrés, | <i>ibid.</i> |
| Tout nombre entier, ou au moins son double, est la somme de trois carrés, | 338 |
| On peut trouver un nombre qui ait tant de formes trinaires qu'on voudra, | <i>ibid.</i> |

QUATRIÈME PARTIE.

MÉTHODES ET RECHERCHES DIVERSES.

| | |
|---|--------------|
| § I. <i>Théorèmes sur les puissances des nombres,</i> | 340 |
| L'aire d'un triangle rectangle en nombres entiers ne saurait être égale à un carré, | <i>ibid.</i> |
| La somme de deux bicarrés ne peut être un carré, | 343 |
| La formule $x^4 + 2y^4$ ne peut être un carré, | 344 |
| Aucun nombre triangulaire, excepté 1, n'est égal à un bicarré, | 345 |
| La somme ou la différence de deux cubes ne peut être un cube, | <i>ibid.</i> |
| Elle ne peut non plus être double d'un cube, | 347 |
| Aucun nombre triangulaire, excepté 1, n'est égal à un cube, | 348 |
| § II. <i>Théorèmes concernant la résolution en nombres entiers de l'équation</i> $x^n - b = ay$, | 349 |
| Condition de possibilité et réduction de l'équation lorsque a est un nombre premier, | <i>ibid.</i> |
| Résolution de l'équation $x^n - 1 = ay$, lorsque a est un nombre premier, et n un diviseur de $a - 1$, | 350 |
| Résolution de l'équation $x^{2n} + 1 = ay$, dans les mêmes cas, | 353 |
| Résolution de l'équation $x^n - b = ay$, dans les mêmes cas, | 355 |
| Résolution générale de la même équation, | 357 |
| § III. <i>Résolution de l'équation</i> $x^2 + a = 2^m y$, | 358 |
| § IV. <i>Méthode pour trouver le diviseur quadratique qui renferme le produit de plusieurs diviseurs quadratiques donnés,</i> | 361 |
| Formule pour avoir le produit de deux diviseurs quadratiques donnés, | 362 |
| Formule pour avoir le produit de deux diviseurs quadratiques semblables, | 365 |
| Diverses formes dont est susceptible le produit de plusieurs diviseurs quadratiques | |

TABLE DES MATIÈRES.

x x j

| | |
|--|--------------|
| donnés, | pag. 367 |
| Formule pour avoir la puissance n d'un diviseur quadratique donné, | 369 |
| § V. <i>Résolution en nombres entiers de l'équation $Ly^2 + Myz + Nz^2 = b\Pi$, Π étant le produit de plusieurs indéterminées ou de leurs puissances,</i> | 374 |
| Après avoir dégagé le second membre du facteur constant b , on fait voir comment la résolution de cette équation se déduit des développemens donnés dans le § précédent, | 375 |
| Exemples divers, | 375 — 379 |
| § VI. <i>Démonstration d'une propriété relative aux diviseurs quadratiques de la formule $t^2 + au^2$, a étant un nombre premier $8n + 1$,</i> | 380 |
| Après quelques propositions subsidiaires, on prouve que l'équation $U^2 = PY^2 + 2QYZ + RZ^2$, dans laquelle $PR - Q^2 = a$, n'est susceptible que de deux solutions, lesquelles se réduisent à une seule, lorsque l'équation proposée est de la forme $U^2 = 2y^2 + 2yz + \frac{1}{2}(a + 1)z^2$, | 383 |
| De là on conclut que le nombre des diviseurs quadratiques $4n + 1$ de la formule $t^2 + au^2$, surpasse toujours d'une unité le nombre des diviseurs quadratiques $4n + 3$ de la même formule, | 385 |
| § VII. <i>Démonstration du théorème contenant la loi de réciprocité qui existe entre deux nombres premiers quelconques,</i> | 386 |
| § VIII. <i>D'une loi très-remarquable observée dans l'énumération des nombres premiers,</i> | 394 |
| Comparaison de la formule avec les Tables, | <i>ibid.</i> |
| Valeur moyenne et probable de la différence entre deux nombres premiers consécutifs, | 395 |
| Sommation de quelques suites qui dépendent de la loi des nombres premiers, | 396 |
| Essai sur la démonstration de la formule trouvée par induction, | 398 |
| § IX. <i>Démonstration de divers théorèmes sur les progressions arithmétiques,</i> | 399 |
| Si on désigne par π le terme de rang $(k - 1)$ dans la suite des nombres premiers 3, 5, 7, 11, etc., je dis que sur π termes consécutifs d'une progression arithmétique quelconque, il y en aura toujours au moins un qui ne sera divisible par aucun terme pris dans une suite de k nombres premiers quelconques, | 404 |
| Il en résulte que toute progression arithmétique, dont le premier terme et la raison sont premiers entre eux, contient une infinité de nombres premiers, | <i>ibid.</i> |
| § X, où l'on prouve que tout diviseur quadratique de la formule $t^2 + Nu^2$, contient au moins un nombre premier à N et plus petit que N , | 407 |
| § XI. <i>Méthodes pour trouver combien, dans une progression arithmétique quelconque, il y a de termes qui ne sont divisibles par aucun des nombres premiers compris dans une suite donnée,</i> | 412 |

xxij

TABLE DES MATIÈRES.

| | |
|---|----------|
| Formule générale qui satisfait dans tous les cas, | pag. 414 |
| Algorithme pour simplifier le calcul de la formule générale, | 418 |
| Formules pour la comparaison des diverses progressions, | 420 |
| Une progression quelconque et la simple progression des nombres impairs peuvent être disposées terme à terme, de manière que les termes correspondans soient tous deux premiers, ou tous deux non-premiers à un même produit Ω , | 422 |
| § XII. Méthodes pour compléter la résolution en nombres entiers des équations indéterminées du second degré, | |
| On ramène généralement l'équation $ay^2 + byz + cz^2 + dy + fz + g = 0$ à la forme $ay'^2 + by'z' + cz'^2 = H$: on donne ensuite une méthode générale et exempte de tâtonnement pour déduire des valeurs de y' et z' celles de y et z en nombres entiers, | 426 |
| Le succès de la méthode précédente étant fondé sur ce que les fractions à faire disparaître ont pour dénominateur $bb - 4ac$, on se propose plus généralement de déterminer l'exposant n , tel qu'en faisant $(\varphi + \sqrt{A})^n = F + G\sqrt{A}$, la quantité $\lambda F + \mu G + \nu$ soit divisible par un nombre premier quelconque ω , | 427 |
| On détermine ensuite directement la valeur du même exposant, telle que $\lambda F + \mu G + \nu$ soit divisible par une puissance donnée du nombre premier ω , | 428 |
| § XIII. Méthode de Fermat pour la résolution de l'équation $y^2 = a + bx + cx^2 + dx^3 + ex^4$ en nombres rationnels, | |
| Si l'équation proposée est telle que a ou e soit un carré positif, ou si on en connaît une solution, on donne la méthode d'avoir successivement d'autres solutions, <i>ibid.</i> | 431 |
| Application à deux problèmes particuliers, | 433 |

CINQUIÈME PARTIE.

Usage de l'analyse indéterminée dans la résolution de l'équation $x^n - 1 = 0$, n étant un nombre premier,

435

Ayant fait $X = \frac{x^n - 1}{x - 1}$, le polynome X ne peut être décomposé en facteurs rationnels,

439

Connexion entre la résolution de l'équation $X = 0$ et celle de l'équation indéterminée $x^{n-1} - 1 = ny$,

443

Formation des périodes dans lesquelles se distribuent les racines de l'équation $X = 0$; équations subsidiaires qui servent à trouver la somme des racines comprises dans chaque période,

443 - 459

Développement de la solution lorsque $n = 19$,

460

Développement du cas où $n = 17$,

462

En général il résulte de cette théorie que si l'on décompose $n - 1$ en ses facteurs premiers $a^{\alpha} b^{\beta} c^{\gamma}$, etc., la résolution de l'équation $X = 0$ se réduira à celle de α équations du degré a , β du degré b , etc.

465

On peut toujours trouver deux polynomes Y et Z , tels que $4X = Y^2 \pm nZ^2$,

468

TABLE DES MATIÈRES.

xxiiij

- Théorèmes relatifs à la résolution de l'équation $X = 0$, dans le cas de $n = 3m + 1$, et dans celui de $n = 4m + 1$,** pag. 472
- La résolution des équations auxiliaires se réduit toujours à celle des équations à deux termes de même degré. On en donne un exemple dans la résolution de l'équation $x^{11} - 1 = 0$, ce qui conduit au même résultat qu'a donné Vandermonde dans les Mémoires de l'Académie, année 1771,** 473

TABLES.

- Table I.* Expressions les plus simples des formules $Ly^2 + 2Myz + Nz^2$, pour toutes les valeurs du nombre non-quarré $A = M^2 - LN$, depuis $A = 2$ jusqu'à $A = 136$.
- Table II.* Expressions les plus simples des formules $Ly^2 + Myz + Nz^2$, pour toutes les valeurs de $B = M^2 - 4LN$, depuis $B = 5$ jusqu'à $B = 305$.
- Table III.* Diviseurs quadratiques et linéaires impairs de la formule $t^2 - au^2$, pour tout nombre a non-quarré, ni divisible par un carré, depuis $a = 2$ jusqu'à $a = 79$.
- Table IV.* Diviseurs quadratiques et linéaires impairs de la formule $t^2 + au^2$, pour tout nombre a de forme $4n + 1$, non-quarré ni divisible par un carré, depuis $a = 1$ jusqu'à $a = 105$.
- Table V.* Diviseurs quadratiques et linéaires impairs de la formule $t^2 + au^2$, pour tout nombre a de forme $4n + 3$, non-divisible par un carré, depuis $a = 3$ jusqu'à $a = 103$.
- Table VI.* Diviseurs quadratiques et linéaires impairs de la formule $t^2 + 2au^2$, pour tout nombre a de forme $4n + 1$, non-divisible par un carré, depuis $a = 1$ jusqu'à $a = 53$.
- Table VII.* Diviseurs quadratiques et linéaires impairs de la formule $t^2 + au^2$, pour tout nombre a de forme $4n + 3$, non-divisible par un carré, depuis $a = 3$ jusqu'à $a = 51$.
- Table VIII,* contenant les diviseurs quadratiques trinaires de la formule $t^2 + cu^2$, avec les valeurs trinaires correspondantes de c , pour tout nombre c qui n'est ni de la forme $4n$, ni de la forme $8n + 7$, depuis $c = 1$ jusqu'à $c = 214$.
- Table IX.* Valeurs du produit $\frac{2}{3} \cdot \frac{4}{5} \cdot \frac{6}{7} \cdot \frac{10}{11} \dots \frac{\omega - 1}{\omega}$, formé avec les nombres premiers successifs, depuis $\omega = 3$ jusqu'à $\omega = 1229$.
- Table X,* contenant les fractions les plus simples $\frac{m}{n}$ qui satisfont à l'équation $m^2 - an^2 = \pm 1$, pour tout nombre non-quarré a , depuis $a = 2$ jusqu'à $a = 135$.

FIN DE LA TABLE DES MATIÈRES.

ERRATA.

| | | | |
|-----------|---------------|------------------|---------------------------|
| Pag. 228, | lign. 21..... | $t^2c + cu^2$, | <i>lisez</i> $t^2 + cu^2$ |
| 232, | 2 et 6... | a aura | <i>a</i> aura |
| 265, | 34..... | $\mu m^2 + vn^2$ | $m\mu^2 + nv^2$ |
| 384, | 23..... | pusique | puisque |
| 456, | avant-dern. | pouvant | peuvent |