Cyclotomie et formes quadratiques dans l'œuvre arithmétique d'Augustin-Louis Cauchy (1829–1840)

Jenny Boucard

Arch. Hist. Exact Sci. (2013) 67:349–414
DOI 10.1007/s00407-013-0115-3

Cyclotomie et formes quadratiques dans l'œuvre arithmétique d'Augustin-Louis Cauchy (1829–1840)

Jenny Boucard

Received: 28 December 2012 / Published online: 16 April 2013

Résumé Augustin-Louis Cauchy publie une majorité de ses recherches arithmétiques entre 1829 et 1840. Celles-ci ne sont pourtant qu'évoquées dans certaines histoires de la théorie des nombres centrées sur les lois de réciprocité ou sur la théorie des nombres algébriques. Elles y sont décrites comme contenant quelques résultats similaires à ceux de Gauss, Jacobi ou Dirichlet mais de manière incomplète et désordonnée. L'objectif de cet article est de présenter une analyse des textes arithmétiques de Cauchy publiés entre 1829 et 1840 pour montrer qu'ils contiennent au contraire un ensemble cohérent de résultats en lien avec les formes quadratiques $4p^{\mu} = x^2 + ny^2$, où p est un nombre premier et n un diviseur de $p - 1$. Nous discuterons également la forme particulière de ce corpus et la stratégie utilisée pour retrouver les lignes directrices du travail de Cauchy.

Abstract Augustin-Louis Cauchy published most of his arithmetical research between 1829 and 1840. These are however only mentioned in some number theory history centered on reciprocity laws or on theory of algebraic numbers. They are described as containing some results similar to those of Gauss, Jacobi and Dirichlet but in a incomplete and disorganized way. The objective of this paper is to present an analysis of Cauchy's arithmetical texts published between 1829 and 1840 to show that they contain a rather consistent set of results related to quadratic forms $4p^{\mu} = x^2 + ny^2$,

Communicated by: U. Bottazzini.

J. Boucard (✉)
Institut de mathématiques de Jussieu, Case 247, 4 place Jussieu,
75252 Paris Cedex, France
e-mail: jenny.boucard@gmail.com

J. Boucard
Centre François Viète, UFR Sciences et Techniques, 2 rue de la Houssinière,
44322 Nantes Cedex 3, France

where p is a prime and n a divisor of $p-1$. We will also discuss the particular form of this body of texts and the strategy we used to find the guidelines of the work of Cauchy.

1 Introduction

Augustin-Louis Cauchy (1789–1857)[1] est bien sûr connu pour ses travaux en analyse, en particulier sur les nombres et fonctions complexes (Dahan Dalmedico 1979, 1997; Flament 2003; Gilain 1989; Peiffer 1978) et pour ses mémoires sur la théorie des substitutions (Dahan Dalmedico 1980; Wussing 1984). En revanche, ses écrits de théorie des nombres, dont l'ensemble représente un corpus d'un millier de pages, restent peu étudiés. Si son nom revient systématiquement dans les histoires sur le dernier théorème de Fermat (Edwards 1977, pp. 77–79), c'est à propos de tentatives décrites comme infructueuses pour démontrer l'unicité de la décomposition en facteurs premiers des entiers cyclotomiques.[2] Quant à ses résultats publiés jusqu'en 1840, ils sont au mieux présentés comme similaires, mais obtenus de manière dispersée et incomplète, à ceux contenus dans les travaux de Carl Friedrich Gauss, Johann Peter Gustav Lejeune-Dirichlet ou Carl Gustav Jacob Jacobi. Par exemple, Franz Lemmermeyer commente le travail de Cauchy sur les sommes de Gauss:[3] «Cauchy also studied these sums, but his lack of understanding higher reciprocity kept him from going as far as Jacobi did» (Lemmermeyer 2009, p. 171). Il remarque également que: "Cauchy's work is somewhat hard to read [...]. His main work on cyclotomy[4] has about as many pages as this book. This basic relations for Gauss sums are all there, but scattered throughout this treatise" (Lemmermeyer 2000, p. 391).

Notre objectif est ici de montrer qu'au contraire, les différents résultats donnés par Cauchy dans ses travaux arithmétiques entre 1829 et 1840 ne sont pas disparates: ils obéissent à une perspective cohérente, mais différente de celle des autres savants évoqués ci-dessus. Pour cela, nous nous appuyons sur une étude détaillée de ses articles de théorie des nombres publiés entre 1829 et 1840.

Pendant cette période, Cauchy publie ses travaux arithmétiques sur deux intervalles de temps très courts:[5] entre 1829 et 1831, puis entre 1839 et 1840, sous la forme d'une quinzaine de mémoires et de notes. Les différents moyens de publication utilisés par Cauchy pour communiquer ses recherches induisent des textes de formes variées. Ils présentent des difficultés de compréhension et d'interprétation particulières, dûes notamment à leur forme et à l'absence de commentaires de la part de Cauchy sur les principes généraux de ses recherches et sur les liens existant entre les différents

[1] Nous ne donnons pas de détails sur la vie de Cauchy: se reporter à (Belhoste 1985) pour une biographie détaillée de Cauchy. Voir également (Dhombres et Gilain 1992) pour une liste de travaux concernant Cauchy.

[2] Les entiers cyclotomiques sont les combinaisons linéaires à coefficients entiers des puissances d'une racine primitive de l'unité.

[3] Nous revenons dans le premier paragraphe sur cette notion.

[4] Franz Lemmermeyer se réfère ici à (Cauchy 1840a).

[5] Suite à la Révolution de juillet et à l'abdication de Charles X en 1830, Cauchy s'exile volontairement jusqu'en 1839 (Belhoste 1985, pp. 113–143). Entre 1832 et 1839, Cauchy ne produit que très peu de textes et aucun ne concerne la théorie des nombres.

résultats. Nous préciserons donc les modalités grâce auxquelles nous avons pu faire sens de cet ensemble de textes.

Expliciter notre travail de reconstruction permet de comprendre ce que semblent être les finalités de Cauchy dans ses recherches arithmétiques. Notre analyse montre en effet que la ligne directrice des recherches de Cauchy en théorie des nombres est l'étude des formes quadratiques[6] $4p^{\mu} = x^2+ny^2$, où p est un nombre premier et n un diviseur de $p-1$. Il n'est bien entendu pas question ici de détailler tous les raisonnements mathématiques développés par Cauchy; nous insisterons donc particulièrement sur les parties en lien direct avec les formes quadratiques et sur les différentes méthodes utilisées. Pour mieux comprendre le contexte des recherches de Cauchy sur les formes quadratiques, nous revenons dans un premier temps sur certaines parties des *Disquisitiones Arithmeticae* de Gauss: Gauss est en effet cité presque systématiquement par Cauchy dans ses différents textes, et les travaux du premier sont au moins en partie le point de départ des recherches arithmétiques du second.[7] Nous évoquerons également en passant quelques liens entre les résultats obtenus par Cauchy et les travaux mieux connus d'autres auteurs en lien avec la théorie des nombres.

2 Préliminaires: cyclotomie et formes quadratiques dans les *Disquisitiones Arithmeticae* de Gauss

2.1 La théorie des nombres au début du XIX^{e} siècle

Le début du XIX^{e} siècle est marqué par la parution de deux traités de théorie des nombres: l'*Essai sur la théorie des nombres* de Legendre en 1798 et les *Disquisitiones Arithmeticae* de Gauss en 1801. Legendre identifie théorie des nombres et analyse indéterminée comme des domaines semblables et consacre la majeure partie de son travail aux équations indéterminées et aux formes quadratiques. Il introduit également ce que l'on appelle aujourd'hui le symbole de Legendre,[8] énonce la loi de réciprocité quadratique et expose une démonstration incomplète de ce résultat. Gauss définit ses recherches comme appartenant à "cette partie des Mathématiques où l'on considère particulièrement les nombres entiers, quelques fois les fractions, mais où l'on exclut

[6] On retrouve déjà chez Pierre de Fermat des résultats sur les nombres premiers que l'on peut mettre sous la forme x^2+ny^2. Leonhard Euler, Joseph-Louis Lagrange, Adrien-Marie Legendre et Gauss développent des méthodes pour démontrer les conjectures formulées par Fermat, puis par Euler. Ainsi, à l'occasion de recherches sur ce thème, Euler développe sa théorie des résidus quadratiques, Lagrange travaille sur les formes quadratiques, étudiées ensuite par Legendre et Gauss. Ce dernier va également considérer les résidus cubiques et biquadratiques dans les cas où la théorie des formes quadratiques est insuffisante. Voir (Cox 1989).

[7] Nous avons choisi ici de lier les travaux de Cauchy aux travaux du mathématicien auquel il se réfère explicitement à de nombreuses reprises; des savants comme Lagrange, Legendre et Euler ne sont cités que très ponctuellement (voir l'Annexe B). Néanmoins, replacer les recherches de Cauchy dans le contexte des travaux arithmétiques de Lagrange et Legendre permettrait certainement de faire émerger d'autres aspects de ses travaux.

[8] Soit p un nombre premier, et a un nombre entier non divisible par p. Alors le symbole de Legendre $(\frac{a}{p})$ a pour valeur le reste de la division de $a^{\frac{p-1}{2}}$ par p, c'est-à-dire 1 ou -1 selon que a est un carré ou n'est pas un carré modulo p.

toujours les nombres irrationnels" (Gauss 1801, Préface).[9] Ce travail de Gauss est souvent décrit comme un ouvrage clé pour la théorie des nombres au XIX^{e} siècle.[10] Ces deux traités, et particulièrement celui de Gauss, seront des références pour presque tous les auteurs publiant de la théorie des nombres, au moins dans la première moitié du XIX^{e} siècle.

Dans le premier quart du XIX^{e} siècle, et à la suite de la parution de ces deux livres, ce sont principalement Gauss et Louis Poinsot qui développent des recherches en lien avec les thèmes étudiés dans les *Disquisitiones Arithmeticae*: le premier propose quatre nouvelles démonstrations de la loi de réciprocité quadratique basées sur différentes méthodes et développe des résultats déjà présents dans son traité de 1801 (Gauss 1808, 1811, 1818). Il justifie ces nouvelles démonstrations par la recherche de méthodes pouvant être étendues aux résidus cubiques et biquadratiques. Il présente également des recherches en lien avec les résidus biquadratiques dans lesquelles il introduit et étudie ce que nous appelons aujourd'hui les entiers de Gauss (Gauss 1828).[11] Le second publie deux mémoires de théorie des nombres (Poinsot 1818, 1820), dans lesquels il met en avant une notion fondamentale pour l'algèbre et la théorie des nombres: la *théorie de l'ordre* (Boucard 2011a). À partir de 1826, le nombre de publications de théorie des nombres augmente rapidement, notamment avec la création du *Journal de Crelle* et du *Bulletin de Férussac*. Celles-ci s'appuient principalement sur des thèmes traités précédemment par Gauss. Des mémoires ou comptes rendus de travaux de Jacobi, Dirichlet, Cauchy, Victor-Amédée Lebesgue, Évariste Galois, Poinsot, Guglielmo Libri paraissent dans ces périodiques.

2.2 Quelques remarques sur les *Disquisitiones Arithmeticae*

Dans ses travaux, Cauchy reprend des *Disquisitiones Arithmeticae* la notion de congruence, qu'il renomme *équivalence*, ainsi que certaines de leurs propriétés et utilise la réindexation des racines de l'unité proposée par Gauss. Comme indiqué dans la citation précédente de Franz Lemmermeyer, Cauchy travaille également beaucoup sur des expressions appelées sommes de Gauss. C'est pourquoi nous nous arrêtons rapidement sur l'ouvrage de Gauss.

Gauss introduit dès la première section la notion de congruence;[12] Gauss joint à cette définition un nouveau symbole, puis démontre des propriétés fondamentales des congruences dans les deux premières sections. Les congruences sont ensuite utilisées dans les sections suivantes: Gauss consacre notamment les sections III et IV à l'étude des résidus de puissances et des résidus quadratiques; il propose d'ailleurs une première démonstration de la loi de réciprocité quadratique. Dans la section V, il élabore une théorie des formes quadratiques, en étudiant notamment deux problèmes: déterminer

[9] Toutes nos citations des *Disquisitiones Arithmeticae* sont empruntées à la traduction française de Antoine C. Poullet-Delisle publiée en 1807.

[10] Nous renvoyons à (Goldstein et Schappacher 2007) pour un commentaire plus détaillé sur cet ouvrage et sa réception dans la première moitié du XIX^{e} siècle.

[11] Les entiers de Gauss sont les nombres complexes de la forme $a + bi$, où a et b sont des nombres entiers.

[12] Deux nombres a et b sont dits congrus modulo un nombre premier p lorsque p divise la différence $a - b$.

les nombres qui sont représentés par une forme quadratique donnée (il introduit à cette occasion la notion de déterminant d'une forme quadratique et montre qu'il est résidu quadratique de tout nombre représenté par la forme quadratique associée) et classer les formes quadratiques en fonction de leur déterminant. Il utilise les résultats de cette théorie pour donner une deuxième démonstration de la loi de réciprocité quadratique.

Dans la section VII, il expose la théorie de la cyclotomie: il obtient les conditions de constructibilité du polygone régulier à n côtés à la règle et au compas et donne une méthode générale pour la résolution par radicaux des équations binômes. Cette méthode, qui sera notamment diffusée en France très rapidement,[13] est basée sur les propriétés des racines des équations binômes et sur l'utilisation d'un outil de théorie des nombres: les racines primitives d'un nombre premier.[14] En effet, si n est un nombre premier et r, une racine primitive de l'équation $x^n = 1$, l'ensemble des racines de cette équation est constitué des nombres $1, r, r^2, \ldots, r^{n-1}$. La méthode exposée par Gauss est fondée sur une réindexation des racines de l'équation binôme différentes de l'unité à l'aide d'une racine primitive g du nombre n: r^g, r^{g^2}, ..., $r^{g^{n-2}}$ et la considération de sommes particulières de ces racines, que Gauss nomme *périodes*, qui sont de la forme[15] $(f, \lambda) = \sum_{i=0}^{f-1} r^{\lambda g^{i\frac{n-1}{f}}}$, où f est un diviseur de $n-1$ et λ un nombre entier non divisible par n.

Les sommes de Gauss[16] que nous venons d'évoquer sont en fait des combinaisons linéaires de périodes de Gauss dont les coefficients sont des racines $(n-1)^{\text{e}}$ de l'unité. Gauss travaille d'ailleurs avec des cas particuliers de ces sommes dans la suite de la section VII. Dans l'article 356, il considère les périodes de $\frac{n-1}{2}$ termes et démontre l'égalité:

$$(r - r^g + r^{g^2} - r^{g^3} + \cdots - r^{g^{n-2}})^2 = (-1)^{\frac{n-1}{2}} n,$$

[13] Sylvestre-François Lacroix la résume dans (Lacroix 1804) et Lagrange en propose une simplification dans (Lagrange 1808). Legendre intègre également cette méthode de Gauss dans la deuxième édition de son *Essai sur la théorie des nombres* (Legendre 1808).

[14] Une racine primitive d'un nombre premier p est un nombre tel que les résidus de ses puissances successives donnent tous les nombres entiers compris entre 1 et $p-1$: c'est ce que nous appelons aujourd'hui un générateur du groupe cyclique $\mathbb{F}_p^*$. D'une manière générale, une racine primitive d'une équation ou d'une congruence engendre toutes les autres racines de l'équation ou de la congruence considérée. Les racines primitives de nombres premiers ont tout d'abord été définies et étudiées par Euler dans (Euler 1774) notamment.

[15] Nous reprenons ici les notations utilisées par Gauss. Pour une analyse plus détaillée des principes utilisés par Gauss dans sa méthode de résolution des équations binômes: voir (Boucard 2011a, pp. 55–59).

[16] Nous n'avons retrouvé l'expression "somme de Gauss", ou autre appellation uniformisée pour désigner ces expressions, dans aucune publication de théorie des nombres dans la première moitié du XIX$^{\text{e}}$ siècle; nous nous autoriserons néanmoins à user de cette dénomination dans la suite par souci de clarté. Remarquons par ailleurs que les sommes dépendant de racines primitives de l'unité avec des coefficients ont déjà été utilisées par Lagrange dans le cadre de ses recherches sur la théorie algébrique des équations (Lagrange 1772–1773): c'est ce qu'il appelle les *résolvantes* ou les *réduites*.

qui sera très importante dans les travaux de Cauchy.[17] La valeur du carré de cette somme alternée, souvent qualifiée de somme quadratique de Gauss, est en effet au cœur de la méthode développée par Cauchy pour certaines formes quadratiques. Dans l'article 358, Gauss examine les périodes de $\frac{n-1}{3}$ termes et montre par exemple que tout nombre de la forme $3m + 1$ peut se mettre sous la forme $x^2 + 27y^2$ en utilisant certains cas particuliers de périodes introduites dans la section VII. Il observe d'ailleurs:

> Il suit de là que le nombre $4n$, c'est-à-dire le quadruple de tout nombre premier de la forme $3m + 1$, peut être représenté par la forme $x^2 + 27y^2$; et quoique ce résultat puisse se tirer sans difficulté de la théorie générale des formes binaires, il n'en est pas moins étonnant qu'une telle décomposition soit liée si intimement avec les nombres $a, b, c, \ldots$ (Gauss 1801, art. 358).[18]

Ainsi, Gauss met en avant un lien existant entre ces résultats sur les formes quadratiques et les résultats qu'il obtient dans la section VII. Ce rapprochement entre théorie des formes quadratiques et cyclotomie sera central dans les travaux arithmétiques de Cauchy.[19]

3 Les premiers mémoires de Cauchy autour des lois de réciprocité et des formes quadratiques (1829–1831)

3.1 Les activités arithmétiques de Cauchy jusqu'en 1831

Les premiers mémoires de Cauchy que nous nous proposons d'étudier paraissent entre 1829 et 1831. Ce ne sont pas les premiers écrits arithmétiques de Cauchy: au début de sa carrière, il publie effectivement quelques articles de théorie des nombres sur des thèmes qu'il ne reprendra pas par la suite. En 1813, il introduit ce qu'il appelle les *nombres de même forme*. Cela lui permet par exemple d'obtenir une démonstration plus simple d'un résultat sur les formes quadratiques prouvé par Lagrange[20] en 1770.

[17] Dans les *Disquisitiones Arithmeticae*, Gauss conjecture également la valeur de la somme alternée $r - r^g + r^{g^2} - r^{g^3} + \cdots - r^{g^{n-2}}$, dont il propose une démonstration dans (Gauss 1811). Elle lui permettra d'obtenir une quatrième preuve de la loi de réciprocité quadratique. D'autres démonstrations de cette égalité seront ensuite proposées par Dirichlet, Cauchy et Kronecker notamment.

[18] Les nombres a, b et c dépendent de la répartition des résidus cubiques de n.

[19] Remarquons que c'est également le cas pour certaines recherches de Jacobi: voir par exemple (Jacobi 1837, pp. 345–346).

[20] Voici le résultat en question: si p est un nombre premier et B, C sont des entiers non divisibles par p alors il existe des nombres entiers t et u tels que $t^2 + Bu^2 + C$ soit divisible par p. Il démontre des résultats préliminaires en s'appuyant sur les nombres de même forme qu'il définit ainsi: «Pour simplifier les énoncés de ces théorèmes, j'appellerai *nombres de même forme*, relativement à un diviseur donné, des nombres entiers qui, étant divisés par ce diviseur, donnent des restes entiers et positifs égaux» (Cauchy 1813, p. 40). Remarquons d'ailleurs qu'ici, Cauchy ne cite pas Gauss et la notion de congruence que ce dernier a introduit en 1801 dans les *Disquisitiones Arithmeticae*. Cauchy ne reprendra pas cette notion de *nombre de même forme* dans ses travaux ultérieurs et discute ici à plusieurs reprises le nombre de valeurs prises par certaines expressions, problématique que l'on retrouve dans ses travaux sur les substitutions: voir (Cauchy 1815a) et (Cauchy 1815b).

Il présente ensuite une démonstration du théorème de Fermat sur les nombres polygones le 13 novembre 1815 à l'Académie des sciences.[21] On ne retrouve dans ces premiers travaux aucune référence à l'ouvrage de Gauss, traduit et publié en français depuis 1807.

À l'exception d'un mémoire sur les équations indéterminées[22] en 1826, Cauchy publie à nouveau des textes de théorie des nombres à partir de 1829. En 1829, deux articles paraissent dans les *Exercices de Mathématiques* et contiennent des résultats sur les congruences (Cauchy 1829b,c). Dans ces deux mémoires, Cauchy démontre des résultats sur les congruences en général, sur les congruences binômes et celles de degré 2, 3 et 4. Ses différents raisonnements sont construits autour d'une analogie entre les équations et les congruences. Par exemple, Cauchy énonce en suivant les théorèmes analogues sur le nombre de racines primitives pour les équations et congruences binômes et s'appuie sur des démonstrations similaires: «pour établir le théorème VII, il suffit de remplacer, dans la démonstration que nous avons donnée du théorème VI, le signe $=$ par le signe $\equiv$, en prenant le nombre p pour module» (Cauchy 1829b, p. 272).[23]

Deux autres articles paraissent dans le *Bulletin de Férussac* en 1829 et 1831 et sont ceux que nous allons analyser ci-après. On retrouve également huit entrées en lien avec Cauchy et ses recherches de théorie des nombres dans les *Procès Verbaux* des séances de l'Académie des Sciences sur cette période:[24] par exemple, Cauchy présente quatre mémoires sur la détermination des racines primitives[25] en 1829 et 1830 qui ne sont pas publiés. Deux *Mémoires sur la théorie des nombres* sont également listés dans les *Procès Verbaux*, pour les séances du 9 novembre 1829 et du 31 mai 1830. Enfin, Cauchy propose lors de la séance du 14 septembre 1829 à l'Académie un texte intitulé *Théorie générale des puissances qui comprend comme cas particuliers tout ce que l'on sait sur la théorie des résidus quadratiques et biquadratiques, etc.*, qui semble correspondre au mémoire *Sur la théorie des nombres* publié dans le douzième tome du *Bulletin de Férussac*[26] en 1829.

Arrêtons-nous maintenant sur les deux publications de Cauchy parues dans le *Bulletin de Férussac*.

[21] Cette démonstration est complètement publiée dans (Cauchy 1818).

[22] Cauchy insère en 1826 un mémoire *Sur la résolution de quelques équations indéterminées en nombres entiers* dans le premier volume de ses *Exercices de mathématiques*, qui paraissent régulièrement de 1826 à 1830 et dont Cauchy est l'unique rédacteur: voir (Belhoste 1985, p. 93). Dans ce mémoire sur les équations indéterminées, Cauchy n'utilise pas les notions et objets exposés par Gauss dans son traité, et ne fait aucune référence.

[23] Ce type de raisonnements, fondés sur un rapprochement équation-congruence, est très courant dans les travaux des mathématiciens français (au moins) dans la première moitié du XIX^{e} siècle: voir à ce sujet (Boucard 2011b).

[24] Ces huit entrées sont consignées dans l'Annexe B.

[25] Séances des 14 septembre 1829 et 25 janvier, 31 mai et 5 juillet 1830.

[26] En effet, dans la pochette de séance du 14 septembre 1829, il est indiqué que ce travail contient des résultats sur les lois de réciprocité, ainsi que sur des équations indéterminées de la forme $p = x^2 + y^2$, $p = x^2 + 2y^2$, $p = x^2 + 3y^2$, ..., ce qui correspond aux thèmes abordés par Cauchy dans (Cauchy 1829a).

3.2 Lois de réciprocité et formes quadratiques chez Cauchy en 1829: un premier *Mémoire sur la théorie des nombres*

Le *Mémoire sur la théorie des nombres* publié en 1829 dans le *Bulletin de Férussac* est divisé en trois parties: des *Considérations générales*, des *Principes fondamentaux* et des *Nouvelles formules déduites du second paragraphe*. Cauchy commence par annoncer les objectifs généraux de son travail:

> Dans la science des nombres, l'une des propriétés les plus importantes et les plus fécondes en conséquences dignes de remarque, est le théorème connu sous le nom de *loi de réciprocité* entre deux nombres premiers. On sait en particulier que cette proposition sert de base à la théorie des résidus quadratiques. Or, des recherches relatives à la résolution des équations binômes, après m'avoir fourni une démonstration nouvelle de la loi de réciprocité dont il s'agit, m'ont conduit à reconnaître qu'il existe une infinité de lois du même genre, mais d'un ordre plus élevé, et j'ai vu découler de ces lois des théories nouvelles, savoir: la théorie des résidus cubiques et généralement des résidus fournis par des puissances d'un degré quelconque. D'ailleurs l'analyse par laquelle je suis parvenu à découvrir ces mêmes lois, m'a offert le moyen de résoudre algébriquement une foule d'équations indéterminées et d'établir des théorèmes dignes de l'attention des géomètres (Cauchy 1829a, p. 88).

Cet extrait contient les seuls commentaires que Cauchy donne dans ce texte sur ses objectifs en termes de résultats sur des thèmes arithmétiques. Cauchy semble se focaliser sur deux sujets de la théorie des nombres: les résidus de puissances et les lois de réciprocité d'une part, ce qui paraît bien s'insérer dans la suite des travaux de Gauss, et sur certaines équations indéterminées d'autre part.

À partir de quelques extraits, nous allons maintenant voir dans quelle mesure ces deux thématiques sont traitées par Cauchy: ce mémoire ne contient en fait que deux exemples de résolution d'équations indéterminées, déjà traités dans les *Disquisitiones Arithmeticae*. Cauchy ne propose pas non plus des formules ou des théorèmes pour une loi de réciprocité d'ordre supérieur, comme on peut en retrouver chez Jacobi pour le cas cubique en 1827 par exemple (Jacobi 1827).

3.2.1 Les notations utilisées par Cauchy

Cauchy consacre le début de son deuxième paragraphe à introduire les notations qu'il utilisera dans ce mémoire, mais également dans la plupart de ses travaux ultérieurs. Tout d'abord, il introduit ce qu'il appelle des nombres *équivalents*: «les nombres entiers positifs ou négatifs u et v sont *équivalents* suivant le module n, lorsque la différence $u - v$ ou $v - u$ sera divisible par n». Il remarque que ce qu'il appelle équivalence correspond en fait aux congruences de Gauss et utilise les mêmes symboles que ce dernier.[27] Il introduit ensuite parallèlement la notion de racine primitive d'équation et

[27] Nous utiliserons dans ce texte le vocabulaire de Cauchy.

de congruence en se référant cette fois-ci à Poinsot:[28] il appelle ρ (respectivement r) une racine primitive de l'équation $x^n = 1$ (respectivement de l'équivalence $x^n \equiv 1 \pmod{p}$, où p est un nombre premier) lorsque ρ^n (respectivement r^n) est la plus petite puissance égale à 1 (respectivement équivalente à 1 modulo p). De même, il nomme θ une racine primitive de l'équation $x^p = 1$ et t une racine primitive de l'équation $x^{p-1} \equiv 1 \pmod{p}$.

Il considère le cas où $p - 1$ est divisible par n (c'est-à-dire lorsque l'équivalence $x^n \equiv 1 \pmod{p}$ admet des racines primitives) et pose $p - 1 = n\varpi$: le nombre p est donc de la forme $p = n\varpi + 1$. Il définit ensuite une expression dépendant des différentes racines primitives ρ, θ et t: $\Theta_h = \theta + \rho^h\theta^t + \rho^{2h}\theta^{t^2} + \cdots + \rho^{(p-2)h}\theta^{t^{p-2}}$. Cauchy ne donne à ces expressions aucun nom particulier, et ne commente pas leur origine, mais elles correspondent aux sommes de Gauss évoquées plus haut.

Cauchy expose ensuite sans démonstration certaines propriétés des sommes de Gauss:

- Si h n'est pas divisible par $p - 1$: $\Theta_h\Theta_{-h} = (-1)^{\varpi h}p$.
- Dans le cas où $h + k$ n'est pas divisible par $p - 1$, Cauchy démontre que

$$\Theta_h\Theta_k = (a_0 + a_1\rho + a_2\rho^2 + \cdots + a_{n-1}\rho^{n-1})\Theta_{h+k},$$

  où les a_i sont des nombres entiers inférieurs à p tels que leur somme vaut $p - 2$.
- Cauchy introduit également les produits $P_m = \dfrac{((2n - i - j)\varpi)!}{((n - i)\varpi)!((n - j)\varpi)!}$, où m est un nombre quelconque entier compris entre 0 et $n - 1$, $mh \equiv i \pmod{n}$ et $mk \equiv j \pmod{n}$. Ces produits lui permettent d'obtenir des équivalents modulo p des nombres a_i grâce à la congruence:

$$a_m \equiv \left(2 + P_{n-1}r^m + P_{n-2}r^{2m} + \cdots + P_{n-1}r^{(n-1)m}\right)\varpi \pmod{p}.$$

Remarquons que c'est la racine primitive r, qui est l'analogue de ρ en termes d'équivalence, qui intervient dans la formule ci-dessus. Le transfert d'égalités dépendant de ρ vers des équivalences contenant des expressions en fonction de r sera très régulièrement utilisé par Cauchy.[29]

3.2.2 Une application: des exemples d'équations indéterminées

Cauchy applique enfin les formules obtenues sur deux exemples: lorsque p est de la forme $3k+1$, il montre qu'il existe des entiers x et y tels que $p = x^2+3y^2$ et donne les formules permettant de déterminer x et y; il en déduit également les expressions des racines de l'équivalence $z^2 \equiv -3 \pmod{p}$. Il considère ensuite le cas où p est de la forme $4k+1$: il résout alors l'équation $p = x^2+y^2$. La présentation de chaque exemple

[28] Poinsot définit les racines primitives de congruences et d'équations et établit une analogie entre ces nombres dans (Poinsot 1820).

[29] Jacobi observera d'ailleurs que cette correspondance est fondamentale dans (Jacobi 1837).

se fait sur deux ou trois pages et Cauchy ne commente pas les principes généraux de la méthode utilisée. Les exemples qu'il donne sont d'ailleurs déjà connus, et semblent lui permettre de justifier l'intérêt des recherches présentées ici.[30] Rappelons que, dans sa préface, Cauchy indique que son travail lui permet de résoudre algébriquement une foule d'équations indéterminées (Cauchy 1829a, p. 206), commentaire qui annonce vraisemblablement une méthode générale.

3.2.3 Une seconde application: résidus et lois de réciprocité

Dans la troisième partie du mémoire, *Nouvelles formules déduites des principes exposés dans le second paragraphe*, Cauchy commence par introduire ce que l'on appelle aujourd'hui les sommes de Jacobi:[31] il pose $\Theta_h\Theta_k = R_{h,k}\Theta_{h+k}$. L'expression $R_{h,k}$ est donc égale à $-(-1)^{\varpi h}\,p$ si $h+k$ est divisible par n et à $a_0+a_1\rho+a_2\rho^2+\cdots+a_{n-1}\rho^{n-1}$ si $h+k$ n'est pas divisible par n. Il donne différentes propriétés liant les expressions $R_{h,k}$ et Θ_h et propose en particulier une méthode permettant de calculer $R_{h,k}$ en fonction des $R_{1,i}, i = 1,\ldots,n-1$. La fin du mémoire est consacrée aux lois de réciprocité et contient notamment les étapes d'une démonstration de la loi de réciprocité quadratique, basée également sur les sommes de Gauss.[32]

Cauchy introduit pour cela la notation $\left[\frac{k}{p}\right]$ qui est une expression équivalente à 0 ou 1 ou ρ ou ρ^2 ou ρ^3 ou ...ou ρ^{n-1} suivant que l'on aura $k^{\varpi} \equiv 0$ ou 1 ou ρ ou ρ^2 ou ρ^3 ou ...ou ρ^{n-1} (mod p) (Cauchy 1829a, p. 104).

Comme $\varpi = \frac{p-1}{n}$, cette définition est une version généralisée dans le cadre des résidus d'ordre supérieur à 2 du symbole de Legendre. Cependant, seuls les nombres entiers naturels sont considérés ici.[33]

---

[30] Ces exemples sont notamment traités par Gauss dans (Gauss 1801) et énoncés par Jacobi dans (Jacobi 1827): le premier développe le cas des nombres premiers de la forme $4n+1$, $3n+1$ et $20n+1$ que l'on peut respectivement représenter par les sommes x^2+y^2, x^2+3y^2 et x^2+5y^2 dans la section V sur la théorie des formes quadratiques (Gauss 1801, Art. 182) tandis que le second énonce, sans dévoiler la méthode utilisée, le cas des nombres premiers de la forme $4n+1$, $3n+1$ et $7n+1$, les derniers pouvant être mis sous la forme x^2+7y^2.

[31] Jacobi travaille également avec ces expressions à la même période, mais ne publie des résultats sur ces sommes qu'à partir de 1837 (Jacobi 1837). Il correspond néanmoins avec Gauss sur ce thème dans une lettre datée du 8 février 1827 (Jacobi 1881–1891).

[32] Cauchy la détaillera dans la note IV du *Mémoire sur la théorie des nombres* de 1840. Cette démonstration est assez proche de la sixième preuve de la loi de réciprocité donnée par Gauss en 1818, et semblable à celle de Jacobi, publié dans la troisième édition de la *Théorie des nombres* de Legendre en 1830.

[33] En effet, aujourd'hui, dans le cas de la théorie des résidus cubiques par exemple, on se place dans l'anneau $\mathbb{Z}[\omega] = \{a+b\omega : a, b \in \mathbb{Z}\}$, où $\omega = e^{2i\pi/3}$ est une racine cubique primitive de l'unité. On munit cet anneau euclidien de la norme $N(\alpha) = \alpha\overline{\alpha}$, où $\overline{\alpha}$ désigne le conjugué de α. On définit alors le caractère cubique d'un nombre α modulo π, que l'on peut noter $(\frac{\alpha}{\pi})_3$, ainsi:

- $(\frac{\alpha}{\pi})_3 = 0$ si π divise α;
- $(\frac{\alpha}{\pi})_3 \equiv \alpha^{\frac{N(\pi)-1}{3}}$ (mod π), où $(\frac{\alpha}{\pi})_3$ est égal à 1, ω, ou ω^2.

Voir par exemple (Ireland 1990, pp. 108–137). La définition de Cauchy coïncide bien avec cette définition lorsque α et π sont des entiers.

Il considère dans un premier temps le cas où $n = 2$ et donne ainsi les étapes de la démonstration de la loi de réciprocité quadratique:

$$\left[\frac{q}{p}\right] = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} p^{\frac{q-1}{2}}.$$

Pour finir, il reprend son raisonnement dans le cas où n est un nombre quelconque et aboutit à l'égalité:

$$p^{\frac{q-\varsigma}{n}}(b_0 + b_1\rho + \cdots + b_{n-1}\rho^{n-1}) = \left[\frac{q}{p}\right]^{n-\varsigma} + qQ,$$

où ς est le reste de la division de q par n, les b_i sont des nombers entiers et Q est un polynôme de la forme $c_0 + c_1\rho + c_2\rho^2 + \cdots + c_{n-1}\rho^{n-1}$, (où les c_i sont des nombres entiers).

Il annonce que ces résultats seront développés dans ses recherches arithmétiques ultérieures. Néanmoins, comme nous le verrons par la suite, c'est la dernière fois que Cauchy aborde les lois de réciprocité d'ordre supérieur dans ses travaux.

3.3 Le *Mémoire sur la théorie des nombres* de 1831: un résultat général sur les formes quadratiques

Le deuxième mémoire *Sur la théorie des nombres* inséré dans le quinzième tome du *Bulletin de Férussac* en 1831 est le dernier texte de théorie des nombres de Cauchy publié avant son exil. Dans les trois pages qui le composent, Cauchy veut «donner une idée [des] propositions» (Cauchy 1831, p. 137) qu'il a exposées dans les différents mémoires présentés à l'Académie depuis 1829. Ces feuilles contiennent un théorème général sur les formes quadratiques traitées dans son mémoire précédent:

> Théorème 1er. Soit p un nombre premier,[34] n un diviseur premier de $p - 1$, ϖ la valeur du rapport $\dfrac{p-1}{n}$
>
> $$\mathscr{A}_1 = \frac{1}{6},\ \mathscr{A}_2 = \frac{1}{30},\ \mathscr{A}_3 = \frac{1}{42},\ etc.$$
>
> les nombres de Bernoulli,[35] et m le plus petit nombre entier équivalent, suivant le module n, à $\pm 2A_{\frac{n+1}{4}}$. Enfin, soit s une racine primitive de l'équivalence

[34] Nous corrigeons ici ce qui semble être une faute de frappe dans le mémoire: n est défini comme un diviseur de p, ce qui est incohérent avec la définition de ϖ.

[35] Les $\mathscr{A}_i$ ainsi définis correspondent aux B_{2i} actuels, si B_i désigne le i^{e} nombre de Bernoulli. Cela semble être habituel à l'époque. Cela vient du fait que $B_k = 0$, pour k impair et différent de 1. Par ailleurs, Cauchy considère ici les valeurs absolues des nombres de Bernoulli actuels. Les nombres de Bernoulli interviennent dans de nombreuses formules mathématiques; citons par exemple celle d'Euler-Mac-Laurin. Pour des résultats sur ces nombres, voir (Nielsen 1923). Cauchy revient sur l'utilisation de ces nombres dans la démonstration du théorème énoncé ici dans son *Mémoire sur la théorie des nombres* de 1840.

$$x^{n-1} \equiv 1 \pmod{n};$$

P_s, le produit des nombres entiers 1, 2, 3, . . s; n' le nombre des racines[36] de l'équivalence $x^{\frac{n-1}{2}} \equiv 1 \pmod{n}$, qui sont inférieures à $\frac{n-1}{2}$, et $n'' = n - n' - 1$, le nombre des racines de l'équivalence $x^{\frac{n-1}{2}} \equiv -1 \pmod{n}$ qui remplissent la même condition. Si n est de la forme $4k + 3$, l'équation

$$x^2 + ny^2 = 4p^m,$$

sera résoluble en nombres entiers, et on la vérifiera en prenant

$$x \equiv P_\varpi P_{s^2\varpi} P_{s^4\varpi} \ldots P_{s^{n-3}\varpi}, \quad \pmod{p}$$

ou bien

$$x \equiv P_{s\varpi} P_{s^3\varpi} P_{s^5\varpi} \ldots P_{s^{n-2}\varpi}, \quad \pmod{p}$$

suivant que l'on aura $n' < n''$ ou $n' > n''$. De plus, on trouvera dans le premier cas

$$m = \frac{n - 1 - 4n'}{2} \text{ ou } m = \frac{n - 1 - 4n'}{6},$$

et dans le second cas

$$m = \frac{4n' - n + 1}{2} \text{ ou } m = \frac{4n' - n + 1}{6}$$

suivant que n est de la forme $8k + 7$ ou $8k + 3$ (Cauchy 1831, pp. 137–138).

Aucune justification n'est donnée. Cauchy illustre son théorème par un exemple, en considérant les nombres premiers p de la forme $7n + 1$. L'équation $4p^m = x^2 + 7y^2$ est donc résoluble en nombres entiers pour $m \equiv \mathscr{A}_2 \pmod{7}$. Or, comme $\mathscr{A}_2 = \frac{1}{30}$, alors $m \equiv \frac{1}{15} \equiv 1 \pmod{7}$ puisque $15 \equiv 1 \pmod{7}$. Finalement, on peut toujours résoudre en nombres entiers l'équation $x^2 + 7y^2 = 4p$, lorsque p est un nombre de la forme $7k + 1$. Remarquons qu'ici, Cauchy ne justifie pas l'existence de l'inverse du nombre 15 modulo 7; il ne commente pas non plus le fait que si le dénominateur du nombre de Bernoulli est un multiple du module considéré, alors cette méthode n'est plus valide.[37]

[36] Ces nombres sont donc les résidus quadratiques de n.

[37] Avec les notations utilisées par Cauchy, on peut cependant démontrer que, si $p - 1$ ne divise pas k, alors le dénominateur de $\mathscr{A}_k$ n'est pas divisible par p : voir (Ireland 1990, Ch. 15). Ce résultat peut notamment être déduit d'un théorème annoncé par Thomas Clausen en 1840 dans les *Astronomische Nachrichten* et démontré la même année par George Karl Christian von Staudt (Staudt 1840).

D'autre part, il introduit ici les nombres de Bernoulli dans son théorème sur les formes quadratiques; ces nombres sont reliés à l'aide d'une congruence aux nombres de résidus et non-résidus quadratiques. Cette première utilisation des nombres de Bernoulli dans le cadre de la théorie des nombres est à noter car elle peut être associée aux résultats développés par Ernst Eduard Kummer sur le dernier théorème de Fermat en 1847 (Kummer 1847), *via* les recherches de Jacobi et Dirichlet notamment.

Notons le caractère général de ce théorème: en effet, les résultats vus précédemment concernaient toujours des cas particuliers où n était fixé et avaient déjà été démontrés par d'autres savants, à partir de méthodes diverses. Ici, Cauchy propose un nouveau théorème valable pour tous les nombres premiers n de la forme $4k + 3$. De plus, Cauchy donne une expression équivalente au nombre x et la valeur de m. Ainsi, même s'il ne démontre pas son théorème - ce texte semble avoir pour simple rôle d'annoncer le résultat obtenu par le mathématicien, peut-être en vue d'éviter de futures querelles de priorité - Cauchy semble déjà posséder les principaux outils que l'on retrouve dans ses textes de 1839–1840. Remarquons également que dans cette note, Cauchy ne fait plus aucune allusion aux lois de réciprocité.

Finalement, les deux mémoires publiés dans le *Bulletin de Férussac* donnent quelques indications sur les thèmes abordés par Cauchy, ainsi qu'un nouveau résultat général sur les formes quadratiques $4p^{\mu} = x^2 + ny^2$. Ce dernier lie la répartition des résidus et non-résidus quadratiques, l'exposant μ et les nombres de Bernoulli. Par contre, les méthodes utilisées ne sont pas précisées et il semble difficile de comprendre les différents raisonnements de Cauchy en ne se basant que sur ces deux textes. Cette stratégie de publication est alors courante. Par exemple, dans le *Bulletin de Férussac*, on retrouve principalement des comptes-rendus d'ouvrages ou d'articles parus dans d'autres journaux, ainsi que cinq articles inédits pour ce qui concerne la théorie des nombres: il y a bien sûr les deux textes de Cauchy, ainsi qu'une courte note de Libri sur les racines primitives (Libri 1830), une de Lebesgue sur les résidus de puissances (Lebesgue 1831) et un mémoire de Galois (Galois 1830). Dans ces cinq textes, les auteurs exposent des résultats de manière très succincte (dans le cas de Lebesgue, Cauchy et Libri), ou donnent des indications sur les méthodes utilisées, et en profitent pour annoncer des compléments à venir.[38]

Il faut alors attendre 1839 pour que Cauchy publie à nouveau des textes de théorie des nombres, sous deux formes: un nouveau *Mémoire sur la théorie des nombres* de plus de quatre cent pages, ainsi qu'une dizaine de notes aux *Comptes Rendus* des séances de l'Académie des Sciences. Ces deux types de publications contiennent des apports de nature différente et c'est l'étude de ces deux ensembles d'écrits qui nous a permis de reconstruire la méthode de Cauchy autour des formes quadratiques. Nous allons d'ailleurs commencer par décrire les difficultés rencontrées à la lecture de ces textes. Nous expliquerons ensuite la stratégie que nous avons mise en place pour faire sens de ces travaux de Cauchy.

[38] De même, Jacobi, dans le *Journal de Crelle*, publie une courte note de théorie des nombres en 1827 dans laquelle il énonce des théorèmes sur les résidus cubiques, et sur les formes quadratiques évoquées précédemment.

4 Le *Mémoire sur la théorie des nombres* de 1840 (1) : Outils et résultats développés par Cauchy permettant d'obtenir le résultat de 1831

4.1 Structure du mémoire et problèmes de reconstruction

4.1.1 Présentation par Cauchy et composition du mémoire de 1840

Voici comment Cauchy présente son troisième *Mémoire de théorie des nombres*, publié en 1840 dans le dix-septième tome des *Mémoires* de l'Académie:

> Le Mémoire qu'on va lire est l'un des deux que j'ai présentés à l'Académie des Sciences le 31 mai 1830. Il renferme le développement des principes que j'avais établis dans les *Exercices de Mathématiques* et surtout dans le *Bulletin des Sciences* de M. de Férussac, pour l'année 1829. Mon absence, qui s'est prolongée pendant 8 années, ayant retardé l'impression de ce Mémoire, je le publie aujourd'hui tel que je le retrouve dans le manuscrit présenté, le 31 mai 1830[...] Toutefois, pour ne pas fatiguer l'attention du lecteur, je supprimerai une grande partie des numéros placés devant les formules et, pour éclaircir quelques passages, je joindrai au texte plusieurs notes placées, les unes au bas des pages, les autres à la suite du dernier paragraphe (Cauchy 1840a, p. 5).

Ce mémoire est donc composé d'une partie principale, composée de 80 pages et partagée en quatre paragraphes. Elle est suivie de quatorze notes de taille variable. La partie principale correspond à un des mémoires présentés à l'Académie en 1830, et les quatorze notes ont été écrites ultérieurement. On retrouve certaines de ces dernières dans les *Comptes rendus* des séances de l'Académie des sciences de 1840, ou même dans le *Journal de Liouville.*[39]

Notons néanmoins que la chronologie de ces publications semble difficile à confirmer. En effet, Cauchy observe dans une note publiée aux *Comptes rendus* le 14 octobre 1839: "Ce théorème, qui a été publié, avec un extrait du Mémoire en question [Cauchy se réfère au mémoire du 31 mai 1830], dans le *Bulletin de M. Férussac* de mars 1831, et d'autres théorèmes analogues se trouvent démontrés dans ce Mémoire, dont l'impression s'achève en ce moment, et à la suite duquel j'ai placé des Notes nouvelles qui me paraissent de nature à intéresser les savants occupés de la théorie des nombres (Cauchy 1839a, p. 473)". Cette citation laisse à penser que l'écriture du mémoire est alors terminée. Néanmoins, en conclusion de la note XII du mémoire, Cauchy remarque que les formules qu'il vient d'obtenir «peuvent être démontrées directement, et d'une manière très simple, comme je l'ai remarqué dans un Mémoire que renferment les *Comptes rendus des séances de l'Académie des Sciences, pour l'année 1840* (I^{er} semestre, page 444)» (Cauchy 1840a, p. 390). Le mémoire en question a été présenté à l'Académie le 16 mars 1840.

Enfin, contrairement à ce que Cauchy annonce, pratiquement chaque paragraphe de la partie principale, ou chaque note, contient plus de 40 formules numérotées, voire dans certains cas autour d'une centaine. À ce sujet, le lecteur pourra se reporter

[39] La note XI de mémoire est par exemple reproduite dans les *Comptes rendus* de la séance du 6 avril 1840 et dans le cinquième volume du *Journal de Liouville*.

à l'annexe C, dans laquelle nous avons listé les titres, paginations, et nombres de formules numérotées pour chaque paragraphe et chaque note de (Cauchy 1840a).

4.1.2 Une première tentative de lecture linéaire: difficultés historiographiques

Notre premier contact avec cet ouvrage de Cauchy a été une expérience décourageante: l'expression «hard to read» utilisée par Lemmermeyer (Lemmermeyer 2000, p. 391) nous a alors paru très appropriée. En effet, la forme de la partie principale rappelle celle du mémoire de 1829 publiée dans (Cauchy 1829a): une succession de formules, difficiles à relier les unes aux autres.

Comme en 1829, les démonstrations sont à peine esquissées, voire inexistantes. Il est de plus ardu de distinguer les résultats importants des formules intermédiaires. Le texte est parsemé de commentaires du type «Donc, alors, l'exposant de μ se réduit à $\frac{N}{2}$ dans les formules (84) et (90), aussi bien que dans les formules (38) et (47), (67) et (70)» (Cauchy 1840a, p. 152) ou encore «Il serait au reste facile de déduire directement la formule (66) de l'équation (47), par un calcul semblable à celui qui nous a conduit à la formule (57). Les formules (49), (57), (58), (59), (60), (66) offrent le moyen de simplifier la recherche des quantités équivalentes à $\Pi_{h,k}[\ldots]$» (Cauchy 1840a, p. 264). Ce constant va-et-vient nécessaire entre les nombreuses formules rend la lecture du mémoire d'autant plus pénible.

Cauchy ne donne aucun commentaire sur les résultats obtenus et n'indique pratiquement aucun lien entre les formules contenues dans la partie principale et les compléments insérés dans les notes. Nous avons d'ailleurs indiqué dans l'annexe C les rares fois où Cauchy se réfère dans les notes à la partie principale du mémoire: à part les deux premières notes qui sont explicitement consacrées à détailler certaines démonstrations des deux premiers paragraphes, Cauchy n'indique pas en quoi les notes suivantes complètent (ou non) la partie principale du mémoire.

Cette première lecture nous a seulement permis de repérer quelques résultats familiers, sur les sommes de Gauss par exemple, des cas particuliers d'égalités sur les formes quadratiques $4p^{\mu} = x^2 + ny^2$. Mais elle ne nous a en aucun cas fourni d'informations sur la méthode employée par Cauchy pour déterminer la «foule d'équations indéterminées» annoncée en 1829. Nous allons montrer qu'il est pourtant possible de faire ressortir une méthode générale de ce texte.

Ici, une lecture linéaire n'est donc pas appropriée. Deux questions se posent alors: comment, d'une part, réussir à saisir le mieux possible le sens des recherches de Cauchy ? Comment, d'autre part, transmettre le plus clairement possible à nos propres lecteurs les conclusions de notre travail sans toutefois dissimuler la forme des recherches de Cauchy, cette dernière ayant dû vraisemblablement avoir un impact sur leur réception ? Pour répondre à la première question, nous avons évité autant que possible de calquer nos propres réflexes mathématiques sur les recherches de Cauchy. Nous n'avons pas non plus recherché des traces de thèmes traditionnellement attachés aux recherches arithmétiques de l'époque (comme les lois de réciprocité supérieures ou la théorie des formes quadratiques alors développée par Dirichlet). Nous avons par contre essayé de repérer des références au mémoire de Cauchy dans les articles de théorie des nombres d'autres savants de la même période. Mais aucun savant n'a consacré et publié une partie de ses recherches à la recherche d'égalités de la forme

$4p^{\mu} = x^2+ny^2$ et nous n'avons trouvé que quelques références très ponctuelles au travail de Cauchy. Nous avons donc élaboré un plan d'attaque s'appuyant sur l'ensemble des textes publiés par Cauchy entre 1839 et 1840.

4.1.3 Comprendre et transmettre la méthode sur les formes quadratiques de Cauchy

Cauchy indique au début de son mémoire qu'il a ajouté des notes pour «éclaircir certains passages» (Cauchy 1840a, p. 5). Nous avons donc commencé par étudier globalement les quatorze notes, en relevant les outils développés, les principaux résultats démontrés, sans nous attarder sur les détails des preuves. Nous avons ainsi réussi à dégager les outils fondamentaux intervenant dans le travail de Cauchy: certaines propriétés des sommes de Gauss (note I), les produits de sommes de Gauss (note III), les propriétés des fonctions symétriques et alternées des racines primitives des équations binômes (notes VI à IX). D'autres notes contiennent des résultats qui sont utilisés plus ponctuellement dans un paragraphe de la partie principale. Remarquons que dans les dix premières notes, Cauchy en profite également pour exposer des résultats qui ne servent pas dans la partie principale du mémoire: c'est par exemple le cas de la démonstration de la loi de réciprocité quadratique insérée dans la note IV. Enfin, à partir de la dixième note, Cauchy développe des résultats sur les sommes de Gauss ou des variantes dans la présentation de sa méthode sur les formes quadratiques, qui sont indépendants de la partie principale du mémoire.

Après ce premier travail de repérage, nous avons repris l'étude de notre partie principale en la relisant minutieusement: nous avons ainsi pu comprendre progressivement quels résultats des notes étaient utilisés plus ou moins implicitement pour obtenir chaque formule de la partie principale. Cela nous a permis de reconstruire de manière détaillée la démarche de Cauchy.

Nous avons choisi d'illustrer ce travail à l'aide de deux exemples. Nous avons tout d'abord représenté la structure des deux premiers paragraphes de la partie principale dans le schéma ci-dessous (Fig. 1). Nous avons indiqué dans les cartouches centrales les différentes parties du premier paragraphe. Les notes inscrites à gauche sont celles contenant des compléments ponctuels: par exemple, dans la note IV, Cauchy donne une démonstration détaillée du lien existant entre nombres de Bernoulli et résidus quadratiques. Dans la note II, il complète certaines preuves du deuxième paragraphe. Nous avons placé à droite du schéma les notes renfermant des résultats utilisés à plusieurs reprises dans la partie principale du mémoire. Nous pouvons d'ailleurs remarquer que Cauchy utilise également (et toujours implicitement) des résultats des notes VI et VII dans certains passages de la note III.

Notre deuxième exemple, qui constitue l'annexe A, se situe à une échelle plus locale: nous y avons recopié un extrait du premier paragraphe de la partie principale en indiquant systématiquement comment interviennent les résultats des différentes notes. Cela montre encore qu'une note donnée n'est pas utilisée à un seul endroit de la partie principale, mais de manière diffuse. Ainsi, pour obtenir la formule (26) du premier paragraphe, Cauchy s'appuie sur une égalité de la note III, elle-même démontrée à partir de propriétés de sommes de Jacobi déduites des notes VI et VII. Dans la suite de l'extrait, Cauchy obtient également d'autres formules à partir de cette

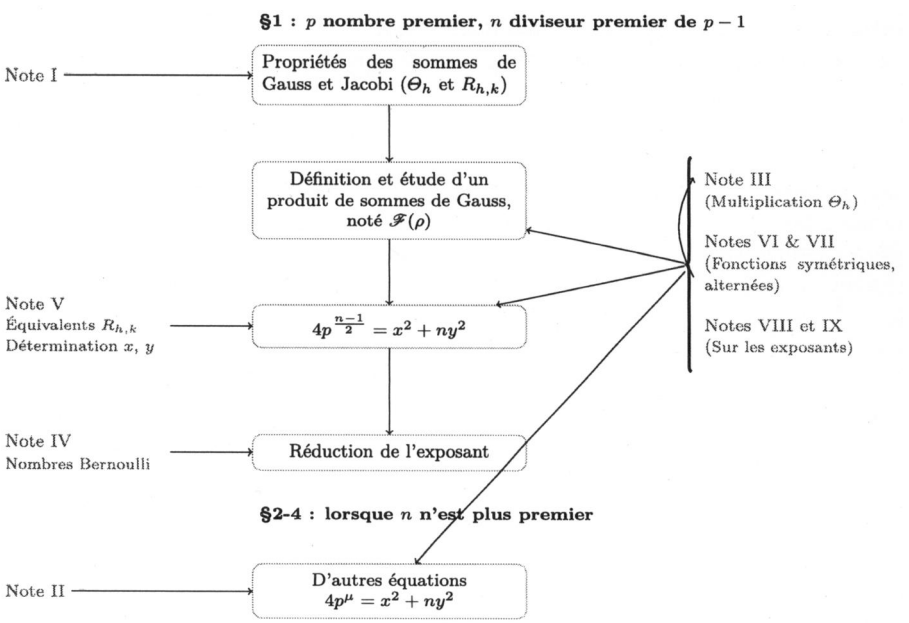

Fig. 1 Quelques liens entre la partie principale et les notes de (Cauchy 1840a)

note III. Dans le deuxième paragraphe de la partie principale, Cauchy utilise à nouveau la note III dans le cas où le nombre n est composé.

À côté de cette reconstruction méthodique du travail de Cauchy, nous avons également étudié les articles parus dans les *Comptes rendus* des séances de l'Académie des sciences entre 1839 et 1840. Dans ceux-ci, Cauchy détaille beaucoup moins ses raisonnements mais donne explicitement le grand principe général de sa méthode: celui-ci consiste à multiplier dans un certain ordre des sommes de Gauss pour obtenir une expression de la forme $4p^{\mu} = x^2 + ny^2$. C'est donc grâce à l'étude conjointe du mémoire et de ces courts articles que nous avons saisi les grandes lignes et les détails du travail de Cauchy.

Nous avons choisi de partager la présentation des recherches arithmétiques de Cauchy en trois parties, afin de respecter la chronologie de lecture que nous venons d'expliciter. Dans un premier temps, nous détaillons les notes du mémoire qui sont fondamentales pour suivre précisément la partie principale du mémoire de Cauchy. Nous avons choisi de conserver systématiquement les numérotations utilisées par Cauchy afin de faciliter la comparaison avec les textes originaux. L'aspect très technique de cette partie est nécessaire pour s'approprier la méthode et les résultats développés par Cauchy en détails. Il est néanmoins possible de ne pas s'y attarder: nous revenons d'ailleurs à la fin de chaque sous-section sur les formules qui sont fondamentales pour la compréhension de la méthode de Cauchy. Dans un second temps, nous présentons les commentaires éclairants et certains résultats que Cauchy donne dans les *Comptes rendus* des séances de l'Académie. Nous revenons enfin sur le mémoire de 1840 et les deux premiers paragraphes de la partie principale pour montrer qu'à la lumière du travail de reconstruction ainsi effectué, nous pouvons conclure que Cauchy expose une

méthode cohérente autour des formes quadratiques $4p^{\mu} = x^2 + ny^2$ qu'il applique dans différents cas, selon que le nombre n est premier ou composé.

4.2 Des relations sur les sommes de Gauss et de Jacobi (Note I)

Les notations et les propriétés fondamentales des sommes de Gauss et de Jacobi utilisées dans tout le mémoire sont listées sur trois pages au début de la partie principale, pratiquement sans aucune justification. Cauchy donne également une définition généralisée du symbole de Legendre, présentée différemment par rapport à son texte de 1829, bien qu'elle soit équivalente.[40] Il rappelle d'abord la définition d'indice, sans se référer à Gauss : Soit k un nombre entier. Alors on note $m = I(k)$ lorsque $k \equiv t^m \pmod{p}$. Cependant, Cauchy ne précise pas que m doit être la plus petite puissance i telle que $k \equiv t^i \pmod{p}$.

Ainsi: $k^{\varpi} \equiv t^{m\varpi} \equiv r^m \equiv r^{I(k)}$. Il peut ensuite donner sa définition de $(\frac{k}{p})$: $(\frac{k}{p}) = \tau^{m\varpi} = \rho^{I(k)}$.

Il détermine alors la valeur de $(\frac{-1}{p})$ en remarquant que $I(-1) = \frac{n\varpi}{2}$, puisque t est une racine primitive de $x^{p-1} \equiv 1 \pmod{p}$, et donc:[41] $(\frac{-1}{p}) = \rho^{I(-1)} = \rho^{\frac{n\varpi}{2}} = \tau^{\frac{n\varpi}{2}\varpi} = (-1)^{\varpi}$ car $\tau^{\frac{n\varpi}{2}} = -1$.

Finalement: $(\frac{-1}{p}) = (-1)^{\frac{p-1}{n}}$. Il ajoute également que $(\frac{h}{p})(\frac{k}{p}) = (\frac{hk}{p})$.

Pour illustrer la nature des démonstrations de Cauchy sur les sommes de Gauss et de Jacobi, nous présentons la note I. Dans celle-ci, Cauchy développe le cas particulier où $n = p - 1$ et donc $\varpi = 1$. À la fin de la note, il explique rapidement comment obtenir les formules pour le cas général où $p - 1 = n\varpi$.

Dans un premier temps, Cauchy rappelle des définitions et propriétés connues, dans le cas où p est un nombre premier et n un nombre entier quelconque. En particulier, si ρ est une racine primitive de $x^n = 1$, alors les différentes racines de cette équation peuvent être exprimées sous la forme $1, \rho, \rho^2, \ldots, \rho^{n-1}$. De plus, l'équivalence $x^n \equiv 1 \pmod{p}$ admet n racines distinctes si n est un diviseur de $p - 1$. Il revient ensuite sur une propriété de la somme des puissances ρ^{im}, où m est un nombre entier et où i est compris entre 0 et $n - 1$:

$$1 + \rho^m + \rho^{2m} + \cdots + \rho^{(n-1)m} = \frac{\rho^{nm} - 1}{\rho^m - 1} = \begin{cases} n \text{ si } m \text{ est divisible par } n; \\ 0 \text{ si } m \text{ n'est pas divisible par } n. \end{cases}$$

Puis il donne la propriété équivalente pour la somme des puissances r^{im}, où r est une racine de l'équivalence $x^n \equiv 1 \pmod{p}$:

$$1 + r^m + r^{2m} + \cdots + r^{(n-1)m} = \frac{r^{nm} - 1}{r^m - 1} \equiv \begin{cases} n \pmod{p} \text{ si } m \text{ est divisible par } n; \\ 0 \pmod{p} \text{ si } m \text{ n'est pas divisible par } n. \end{cases}$$

Enfin, il rappelle que, si n est pair, on a $\rho^{\frac{n}{2}} = -1$ et $r^{\frac{n}{2}} \equiv -1 \pmod{p}$.

[40] Comme en 1829, Cauchy ne cite pas Legendre dans la partie principale du mémoire.

[41] Dans le mémoire, il est indiqué que $\rho^{\frac{n\varpi}{2}} = \tau^{\frac{\varpi}{2}\varpi}$ ce qui me semble être une erreur d'impression.

Ici, comme dans ses premiers mémoires, Cauchy donne parallèlement des propriétés liées à des égalités, puis les propriétés pour les équivalences correspondantes, en remplaçant la racine primitive ρ par la racine primitive r. Même s'il ne fait aucune remarque explicite à ce sujet, Cauchy s'appuie donc sur une correspondance entre racines primitives d'équation et d'équivalence pour obtenir ces résultats.

Cauchy introduit de nouvelles notations, semblables à celles du premier paragraphe de la partie principale et du mémoire de 1829, dans le cas où $n = p - 1$:

- p est un nombre premier impair.
- θ est une racine primitive de l'équation $x^p = 1$.
- τ est une racine primitive de l'équation $x^{p-1} = 1$.
- t est une racine primitive de l'équivalence $x^{p-1} \equiv 1 \pmod{p}$.

Les racines de $x^{p-1} \equiv 1 \pmod{p}$ peuvent être représentées par les termes de la progression arithmétique $1, 2, \ldots, p-1$ ou par les termes de la progression géométrique $1, t, t^2, \ldots, t^{p-2}$, donc:

$$1 + \theta + \theta^2 + \cdots + \theta^{p-1} = 0$$

et

$$1 + \theta^t + \theta^{t^2} + \cdots + \theta^{t^{p-2}} = 0. \tag{1}$$

Il applique également les résultats précédents à la racine primitive τ : $\tau^{\frac{p-1}{2}} = -1$ et

$$1+\tau^m+\tau^{2m}+\cdots+\tau^{(p-2)m} = \begin{cases} p-1 \pmod{p} & \text{si } m \text{ est divisible par } p-1; \\ 0 \pmod{p} & \text{si } m \text{ n'est pas divisible par } p-1. \end{cases}$$

Il introduit alors les sommes Θ_h:

$$\Theta_h = \theta + \tau^h\theta^t + \tau^{2h}\theta^{t^2} + \cdots + \tau^{(p-2)h}\theta^{t^{p-2}}$$

et donne trois propriétés[42] de la somme Θ_h : $\Theta_h = \Theta_k$ si $h \equiv k \pmod{p-1}$; $\Theta_0 = -1$; et

[42] Voici comment Cauchy note la troisième égalité dans son mémoire:

$$\Theta_h\Theta_k = S(\tau^{ih+jk}\theta^{t^i+t^j})$$

le signe S s'étendant à toutes les valeurs de i et j comprises dans la suite

$$0, 1, 2, 3, \ldots p-2$$

(Cauchy 1840a, p. 87).

$$\Theta_h\Theta_k = \sum_{i,j=0}^{p-2} \tau^{ih+jk}\theta^{t^i+t^j} \tag{2}$$

En effet, seuls les exposants de τ dépendent de h et $\tau^{h+(p-1)k} = \tau^h \times \tau^{(p-1)k} = \tau^h$ puisque τ est une racine primitive de l'équation $x^{p-1}=1$. D'autre part, $\Theta_0 = \theta + \theta^t + \theta^{t^2} + \cdots + \theta^{t^{p-2}} = -1$ d'après l'égalité (1). La dernière égalité est une application directe de la définition de Θ_h.

À partir de l'égalité (2), Cauchy détermine les valeurs de i et j rendant l'exposant de θ équivalent à des valeurs données modulo p. L'objectif est de démontrer l'égalité liant les sommes de Gauss avec les sommes de Jacobi: $\Theta_h\Theta_k = R_{h,k}\Theta_{h+k}$.

Cauchy commence par considérer les valeurs de i et j telle que $\theta^{t^i+t^j} \equiv 1 \pmod p$: ce sont les valeurs de i et j telles que $t^i + t^j \equiv 0 \pmod p$, soit $t^{i-j} \equiv -1 \pmod p$ ou $t^{j-i} \equiv -1 \pmod p$.

Or, comme t est une racine primitive de $x^{p-1} \equiv 1 \pmod p$, $t^{\pm\frac{p-1}{2}} \equiv -1 \pmod p$. On en déduit donc que $j - i = \pm\frac{p-1}{2}$, soit $j = i \pm \frac{p-1}{2}$. Le $\pm$ dépend de la valeur de i (si elle est supérieure ou inférieure à $\frac{p-1}{2}$). Donc

$$\sum_{\substack{0\le i,j\le p-2 \\ t^i+t^j\equiv 0 \pmod p}} \tau^{ih+jk}\theta^{t^i+t^j} = \sum_{i=0}^{p-2} \tau^{i(h+k)}\tau^{\pm\frac{p-1}{2}k}.$$

Finalement, on a $(p-1)$ couples (i, j) qui vérifient cette condition. En utilisant l'égalité (A), la somme des termes en θ^0 sera donc égale à:

$$\sum_{i=0}^{p-2} \tau^{i(h+k)}\tau^{\pm\frac{p-1}{2}k} = (-1)^k \sum_{i=0}^{p-2} \tau^{i(h+k)} = \begin{cases} (-1)^k(p-1) & \text{si } h+k \text{ est divisible par } p-1; \\ 0 & \text{si } h+k \text{ n'est pas divisible par } p-1. \end{cases}$$

Il considère[43] ensuite les valeurs de i et j telle que $\theta^{t^i+t^j} \equiv \theta \pmod p$ sont les valeurs de i et j telles que $t^i + t^j \equiv 1 \pmod p$, soit $t^j \equiv 1 - t^i \pmod p$. Or, puisque i est compris entre 0 et $p-2$, seule la valeur $i = 0$ implique $1 - t^i \equiv 0 \pmod p$ donc il existe $(p-2)$ couples (i, j) tels que $t^j \equiv 1 - t^i \pmod p$, avec $1 - t^i \not\equiv 0 \pmod p$.

Cauchy suppose pour commencer que $p-1$ ne divise pas $h+k$. Soit $R_{h,k}$ la somme des termes en θ^1 dans (2). Alors

$$R_{h,k} = \sum_{\substack{t^i+t^j\equiv 1 \pmod p \\ 0\le i,j\le p-2}} \tau^{ih+jk}.$$

[43] Ici, Cauchy écrit: "Ces systèmes seront ceux pour lesquels l'équivalence $t^i + t^j \equiv 1 \pmod p$ se trouvera vérifiée. Or, cette équivalence, présentée sous la forme $t^j = 1 - t^i$ fournira une seule valeur de j, comprise dans la suite 0, 1, 2, 3, ..., $p-2$, pour toute valeur de i, qui étant comprise dans cette même suite, ne rendra pas nulle la différence $1 - t^i$[...]" (Cauchy 1840a, p. 88). On remarque donc qu'il transpose sans commentaire une équivalence en équation.

Cette somme se compose de $p-2$ termes, égaux à une des puissances τ^l, $0 \leq l \leq p-2$ donc

$$R_{h,k} = a_0 + a_1\tau + a_2\tau^2 + \cdots + a_{p-2}\tau^{p-2}, \tag{5}$$

où les a_i sont des coefficients entiers tels que

$$a_0 + a_1 + a_2 + \cdots + a_{p-2} = p - 2. \tag{6}$$

Enfin, Cauchy traite le cas général, toujours dans le cas particulier où $p-1$ ne divise pas $h+k$: les valeurs de i et j telle que $\theta^{t^i+t^j} \equiv \theta^{t^m} \pmod p$, où $1 \leq m \leq p-2$ sont les valeurs de i et j telles que $t^i + t^j \equiv t^m \pmod p$. La somme des termes en θ^{t^m} est

$$\theta^{t^m} \sum_{\substack{t^i+t^j \equiv t^m \pmod p \\ 0 \leq i,j \leq p-2}} \tau^{ih+jk}.$$

et $t^i + t^j \equiv t^m \pmod p$ équivaut à $t^{i-m} + t^{j-m} \equiv 1 \pmod p$.

Donc, «en faisant usage de la notation ci-dessus adoptée» (Cauchy 1840a, p. 90):

$$R_{h,k} = \sum_{\substack{t^{i-m}+t^{j-m} \equiv 1 \pmod p \\ 0 \leq i,j \leq p-2}} \tau^{(i-m)h+(j-m)k} = \tau^{-m(h+k)} \sum_{\substack{t^{i-m}+t^{j-m} \equiv 1 \pmod p \\ 0 \leq i,j \leq p-2}} \tau^{ih+jk},$$

soit

$$\sum_{\substack{t^{i-m}+t^{j-m} \equiv 1 \pmod p \\ 0 \leq i,j \leq p-2}} \tau^{ih+jk} = R_{h,k}\tau^{m(h+k)}$$

Finalement, la somme des termes en θ^{t^m} est égale à $R_{h,k}\tau^{m(h+k)}\theta^{t^m}$ et la somme des termes en puissances positives de θ est

$$R_{h,k} = \underbrace{\sum_{m=0}^{p-2} \tau^{m(h+k)}\theta^{t^m}}_{\Theta_{h+k}}.$$

Donc, si $h+k$ n'est pas divisible par $p-1$:

$$\Theta_h\Theta_k = R_{h,k}\Theta_{h+k}, \tag{7}$$

où $R_{h,k} = \sum_{\substack{t^i+t^j\equiv 1 \pmod p \\ 0\le i,j\le p-2}} \tau^{ih+jk}$. On a donc:

$$\Theta_h\Theta_k = \Theta_{h+k} \sum_{\substack{t^i+t^j\equiv 1 \pmod p \\ 0\le i,j\le p-2}} \tau^{ih+jk}. \tag{8}$$

Cauchy revient ensuite sur le cas où $p-1$ divise $h+k$. On part de l'égalité précédente sachant que $h+k \equiv 0 \pmod{p-1}$, donc $h \equiv -k \pmod{p-1}$. Cauchy indique ici comment on trouve les valeurs de $R_{h,k}$:

> Donc, si l'on suppose la formule (7) étendue au cas où la somme $h+k$ est divisible par $p-1$, c'est-à-dire si, en choisissant $R_{h,k}$ de manière à vérifier dans tous les cas cette formule, on pose

$$\Theta_{h,-h} = R_{h,-h}\Theta_0 \tag{9}$$

(Cauchy 1840a, p. 91).

On aura, puisque $h+k$ est divisible par $p-1$, et d'après la valeur calculée plus haut pour la somme des termes en θ^0:

$$R_{h,-h} = \sum_{\substack{t^i+t^j\equiv 1 \pmod p \\ 0\le i,j\le p-2}} \tau^{(i-j)h} - (-1)^h(p-1).$$

$t^i + t^j \equiv 1 \pmod p$ entraîne $t^{i-j} \equiv t^{-j} - 1 \pmod{p-1}$. Comme t est une racine primitive de $x^{p-1} \equiv 1 \pmod p$, $t^{\frac{p-1}{2}} \equiv -1 \pmod p$ donc les valeurs de $i-j$ considérées dans la somme précédente sont telles que $i-j \neq \frac{p-1}{2}$. Or, la somme $S\tau^{(i-j)h}$ est nulle si elle contient toutes les valeurs de $i-j$ comprises entre 0 et $p-2$. Donc, si l'on considère cette même somme en éliminant la valeur correspondant à $i-j = \frac{p-1}{2}$, on obtient $-\tau^{\frac{p-1}{2}h} = -(-1)^h$. Donc:

$$R_{h,-h} = \sum_{\substack{t^i+t^j\equiv 1 \pmod p \\ 0\le i,j\le p-2}} \tau^{(i-j)h} - (-1)^h(p-1) = -(-1)^h - (-1)^h(p-1) = -(-1)^h p. \tag{10}$$

Finalement: si $p-1$ ne divise pas h, et puisque $\Theta_h\Theta_{-h} = R_{h,-h}\Theta_0$:

$$\Theta_h\Theta_{-h} = (-1)^h p \tag{11}$$

Comme nous l'avons vu précédemment, cette égalité est fondamentale pour ce qui va suivre sur les formes quadratiques; Cauchy ne fait ici aucune remarque mais il

insistera particulièrement sur l'importance de cette formule dans les notes qu'il publie en 1840 dans les *Comptes rendus* de l'Académie des sciences en 1840.

Si $p-1$ divise h, alors h est pair, et $(-1)^h = 1$ et $\tau^h = 1$ donc:[44]

$$R_{h,-h} = \sum_{\substack{t^i+t^j\equiv 1 \pmod p \\ 0\le i,j\le p-2}} \tau^{(i-j)h} - (-1)^h(p-1) = (p-2) - (p-1) = -1.$$

Enfin, Cauchy donne d'autres propriétés de $R_{h,k}$:

> Au reste, on peut conclure immédiatement de la formule (7): 1° que la valeur de $R_{h,k}$ ne varie pas lorsqu'on fait croître ou décroître h ou k d'un multiple de $p-1$; 2° que $R_{h,k}$ se réduit à -1 dès que l'une des quantités h, k est divisible par $p-1$ (Cauchy 1840a, p. 92).

Toujours d'après la formule (7), on a $\Theta_h\Theta_k = R_{h,k}\Theta_{h+k}$ et $\Theta_{-h}\Theta_{-k} = R_{-h,-k}\Theta_{-h-k}$. En multipliant ces deux égalités, on obtient:

$$\Theta_h\Theta_{-h}\Theta_k\Theta_{-k} = R_{h,k}\Theta_{h+k}R_{-h,-k}\Theta_{-h-k}.$$

Donc, d'après (11):

$$(-1)^h p(-1)^k p = R_{h,k}R_{-h,-k}(-1)^{h+k}p$$

soit, lorsque h, k et $h+k$ ne sont pas divisibles par $p-1$:

$$R_{h,k}R_{-h,-k} = p. \tag{13}$$

Comme l'égalité (11), cette formule donne une décomposition du nombre premier p en deux nombres complexes, mais Cauchy ne fait aucune remarque à ce sujet.

Pour finir, Cauchy indique que pour obtenir les formules du premier paragraphe de son mémoire, il suffit de remplacer h par ϖh, k par ϖk, ...

Il remarque également que, dans (11), si $h = \frac{p-1}{2}$, et comme $\Theta_{-\frac{p-1}{2}}\Theta_{\frac{p-1}{2}} = \Theta^2_{\frac{p-1}{2}}$ (puisque $-\frac{p-1}{2} \equiv \frac{p-1}{2} \pmod{p-1}$), on obtient:

$$\Theta^2_{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}}p$$

soit

$$(\theta - \theta^t + \theta^{t^2} + \cdots + \theta^{t^{p-3}} - \theta^{t^{p-2}})^2 = (-1)^{\frac{p-1}{2}}p, \tag{14}$$

ce qui «fournit un théorème, très remarquable, de M. Gauss» (Cauchy 1840a, p. 94). Il note habituellement cette expression Δ. Là encore, c'est une égalité qu'il utilise à

[44] Les deux égalités précédentes sont représentées comme des équivalences dans le texte de Cauchy: $(-1)^h \equiv 1$ et $\tau^h \equiv 1$.

de nombreuses reprises dans la partie principale de son mémoire et dans les quatorze notes qui le complètent.

Finalement, Cauchy manipule ici de nombreuses expressions dépendant de racines de l'unité, sans insister plus particulièrement sur telle ou telle formule. Néanmoins, certaines des égalités obtenues ici seront au centre de la méthode de Cauchy. Nous pensons particulièrement à l'égalité $\Theta_h\Theta_k = R_{h,k}\Theta_{h+k}$, où $R_{h,k}$ est une fonction entière de ρ. De plus, $\Theta_0 = -1$ et dans le cas où $p-1$ ne divise pas h:

$$\Theta_h\Theta_{-h} = (-1)^h p \quad \text{et} \quad R_{h,k}R_{-h,-k} = p.$$

Dans le cas où $h = \frac{p-1}{2}$, on obtient la formule (14) ci-dessus.

4.3 Propriétés des fonctions des racines primitives

Dans les notes VI à IX, Cauchy démontre des propriétés des fonctions symétriques et alternées des puissances de racines primitives et des exposants de ces puissances. Nous détaillons quelques extraits de ces notes et listons les résultats utiles pour la suite.

4.3.1 Propriétés des fonctions symétriques des racines primitives (Note VI)

Dans la sixième note, intitulée *Sur la somme des racines primitives d'une équation binôme, et sur les fonctions symétriques de ces racines*, Cauchy commence par énoncer des théorèmes sur les racines primitives d'équations binômes de la forme $x^n = 1$ où n est un nombre composé. Il aboutit ensuite à un résultat fondamental pour sa démonstration du résultat énoncé dans (Cauchy 1831): lorsque n est un nombre premier, toute fonction f symétrique des racines primitives de l'équation $x^n = 1$ est de la forme $f(\rho) = a_0 + a_1(\rho + \rho^2 + \cdots + \rho^{n-1})$.

Cauchy commence par rappeler des propriétés des racines des équations binômes. Par exemple, si m et n sont deux nombres entiers, et ω leur plus grand diviseur commun, alors une racine commune de $x^n = 1$ et $x^m = 1$ est également une racine de $x^\omega = 1$ (car il existe toujours deux nombres entiers u et v tels que $mu - nv = \omega$). De plus, si ρ est une racine primitive de $x^n - 1$ et si on désigne par $h, k, l, \ldots$, les nombres premiers à n et inférieurs à n, alors toutes les racines primitives de $x^n = 1$ sont représentées dans la suite ρ^h, ρ^k, ρ^l, ...Il en est de même pour la suite ρ^{mh}, ρ^{mk}, ρ^{ml}, ..., où m est premier à n.

Cauchy explique ensuite comment déterminer les racines primitives de l'équation $x^n = 1$, ainsi que leur nombre, lorsque le nombre n est composé de deux facteurs, puis d'un nombre quelconque de facteurs: il suffit de considérer sa décomposition en facteurs premiers. Ainsi, dans le cas général où $n = \nu^a \nu'^b \nu''^c \ldots$ et où on désigne par $\mathscr{S}$ la somme des racines primitives de l'équation $x^n = 1$ et N le nombre de racines primitives de cette équation, Cauchy montre que:

- $N = n\left(1 - \frac{1}{\nu}\right)\left(1 - \frac{1}{\nu'}\right)\left(1 - \frac{1}{\nu''}\right)\ldots$;

- $\mathscr{S}$ est égal au produit des sommes des racines primitives des équations $x^{\nu^a} = 1$, $x^{\nu'^b} = 1, \ldots$, et deux cas se présentent:

- Si n est composé d'au moins deux facteurs égaux entre eux, alors $\mathscr{S} = 0$.
- Si n est un nombre premier ou composé de facteurs premiers tous distincts, alors $\mathscr{S} = 1$ si le nombre de facteurs est pair, et $\mathscr{S} = -1$ si le nombre de facteurs est impair.

Cauchy considère ensuite une fonction entière d'une racine primitive ρ de $x^n = 1$, notée $f(\rho)$. Puisque $\rho^n = 1$, on a $f(\rho) = a_0 + a_1\rho + a_2\rho^2 + \cdots + a_{n-1}\rho^{n-1}$, où les a_i sont des *coefficients indépendants de* ρ. Cauchy ajoute une propriété supplémentaire à la fonction f:

> Supposons d'ailleurs que, dans la fonction $f(\rho)$, les différents termes se transforment les uns dans les autres, quand on y remplace la racine primitive ρ par une autre racine primitive ρ^m. Alors $f(\rho)$ sera ce qu'on peut nommer une *fonction symétrique* des racines primitives de l'équation (1), ou, ce qui revient au même, une fonction symétrique des puissances $\rho^h, \rho^k, \rho^l, \ldots, h, k, l, \ldots$, étant les entiers inférieurs à n et premiers à n (Cauchy 1840a, p. 235).

Cela signifie que les coefficients des termes en $\rho^h, \rho^k, \rho^l, \ldots$, seront les mêmes. De même, si n n'est pas un nombre premier et i un nombre entier positif, les coefficients des termes en $\rho^{ih}, \rho^{ik}, \rho^{il}, \ldots$, (soit les racines primitives d'une équation de la forme $x^\omega = 1$, où ω divise n) seront également les mêmes. Finalement:

> [...] une telle fonction se réduira toujours à une fonction linéaire des diverses valeurs que peut acquérir la somme des racines primitives de l'équation $[x^\omega = 1]$, quand on prend successivement pour ω chacun des diviseurs du nombre n, y compris ce nombre lui-même (Cauchy 1840a, p. 236).

On voit ainsi l'intérêt du travail précédent. Par exemple, si le nombre n est premier, alors la fonction $f(\rho)$ est de la forme $f(\rho) = a_0 + a_1(\rho + \rho^2 + \cdots + \rho^{n-1})$. Ce résultat est important car il permet à Cauchy d'obtenir des résultats dans la partie principale du mémoire.

4.3.2 Propriétés des fonctions alternées des racines primitives

Dans la note VII, Cauchy étudie les propriétés d'expressions contenant des sommes alternées de racines primitives. Cauchy entreprend le même travail que dans la note précédente à partir de fonctions alternées des racines primitives de $x^n = 1$. Il distingue les cas où n est un produit de facteurs premiers tous distincts ou non. Il commence par déterminer la valeur de la somme alternée des racines primitives de l'équation $x^n = 1$ en fonction de la forme de n, puis en déduit des résultats sur les fonctions alternées des racines primitives de la même équation.

Pour cela, il utilise les mêmes notations que dans la note précédente et va démontrer que l'on peut partager les entiers $h, k, l, \ldots$, en deux groupes $h, h', h'', \ldots$ et $k, k', k'', \ldots$ et donc partager les racines primitives de l'équation $x^n = 1$ en deux groupes: $\rho^h, \rho^{h'}, \rho^{h''}, \ldots$et $\rho^k, \rho^{k'}, \rho^{k''}, \ldots$, «de telle sorte qu'après la substitution de ρ^m à ρ,

les deux derniers groupes se trouvent encore composés chacun des mêmes racines, ou transformés l'un dans l'autre» (Cauchy 1840a, p. 240). Cauchy illustre ce partage des racines primitives avec le cas particulier où $n = 5$. Pour pouvoir partager les racines primitives de $x^n = 1$ en deux groupes répondant aux conditions exposées précédemment, le nombre N de ces racines primitives doit être pair pour que les deux groupes contiennent chacun le même nombre $\frac{n}{2}$ de racines.

Cauchy introduit alors la somme alternée $\mathcal{S} = \rho^h + \rho^{h'} + \rho^{h''} + \cdots - \rho^k - \rho^{k'} - \rho^{k''} - \cdots$, qui est invariable ou qui change seulement de signe lorsque l'on remplace la racine primitive ρ par une autre racine primitive ρ^m.

Si la substitution de ρ^m à ρ laisse invariable la somme $\mathcal{S}$, alors les termes $\rho^l, \rho^{ml}, \rho^{m^2 l}, \ldots, \rho^{m^{\iota-1} l}$, où ι est l'indice[45] de m modulo n, sont affectés du même signe. Par contre, si le signe de $\mathcal{S}$ est modifié après substitution de ρ^m à ρ, alors les termes $\rho^{m^i l}$ et $\rho^{m^{i+1} l}$ sont affectés de signes contraires. Ainsi, ρ^l et $\rho^{m^i l}$ seront affectés du même signe si i est pair, et de signes contraires si i est impair. En particulier, ρ^l et $\rho^{m^2 l}$ sont affectés du même signe. On suppose pour la suite que l'exposant 1 fait partie du groupe $h, h', h'', \ldots$, donc, pour tout nombre m premier à n, ρ et ρ^{m^2} sont affectés du même signe. On en déduit que le groupe $h, h', h'', \ldots$, contient tous les exposants équivalents à des carrés modulo n, soit les résidus quadratiques relatifs modulo n.

Là encore, Cauchy détermine la valeur de $\mathcal{S}$ en fonction de la forme du nombre n. Par exemple, dans le cas où n est un nombre premier impair ou une puissance d'un nombre premier impair, alors les entiers $h, k, l, \ldots$, inférieurs et premiers à n vérifient l'équivalence $x^N \equiv 1 \pmod{n}$, où N représente toujours le nombre de racines primitives de l'équation $x^n = 1$. Parmi ces nombres, $\frac{N}{2}$ sont des résidus quadratiques, que Cauchy note $h, h', h'', \ldots$, et $\frac{N}{2}$ sont des non-résidus quadratiques, alors notés $k, k', k'', \ldots$. Ainsi, si on considère une racine primitive s de l'équivalence $x^N \equiv 1 \pmod{n}$, les racines primitives de $x^n = 1$ sont représentées par $\rho, \rho^s, \rho^{s^2}, \ldots, \rho^{s^{N-1}}$.

Dans le cas où n est un nombre premier impair, alors $\mathcal{S} = \rho^h - \rho^k + \rho^{h'} - \rho^{k'} + \cdots = \rho - \rho^s + \rho^{s^2} - \rho^{s^3} + \cdots - \rho^{s^{n-2}}$ et d'après le résultat obtenu dans la note I: $\mathcal{S}^2 = (\rho - \rho^s + \rho^{s^2} - \rho^{s^3} + \cdots - \rho^{s^{n-2}})^2 = (-1)^{\frac{n-1}{2}} n$. Dans le cas où $n = \nu^a$, où $a > 1$, Cauchy montre que $\mathcal{S} = 0$. Il obtient ensuite des résultats similaires dans le cas où n est une puissance de 2, puis un nombre quelconque. Nous ne détaillons pas chaque résultat obtenu ici, mais revenons sur certains points du cas général.

Cauchy considère un nombre n entier quelconque donc la décomposition en facteurs premiers est $n = \nu^a \nu'^b \nu''^c \ldots$. Une racine primitive ρ de l'équation $x^n = 1$ est le produit de racines primitives $\xi, \eta, \zeta, \ldots$ des équations $x^{\nu^a} = 1, x^{\nu'^b} = 1, x^{\nu''^c} = 1, \ldots$ Plus généralement, les différentes racines primitives de $x^n = 1$ seront des nombres de la forme $\xi^l \eta^{l'} \zeta^{l''} \ldots$, où l est premier à ν, l' est premier à ν', l'' est premier à ν'', ...La somme alternée $\mathcal{S}$ est une fonction entière de ρ, et donc également de ξ, de η, ... Cauchy montre alors que $\mathcal{S}$ est nécessairement proportionnelle à la somme des racines primitives de $x^{\nu^a} = 1$ et à une somme alternée de ces racines. Il en est de même pour les autres racines primitives. Donc $\mathcal{S}$ est proportionnelle au produit dont chaque facteur est la somme ou une somme alternée des racines primitives d'une équation

[45] c'est-à-dire la plus petite puissance de m équivalente à l'unité modulo n.

$x^{\nu^a} = 1, \ldots$. Réciproquement, il montre que le produit de sommes symétriques ou de sommes alternées de ce type est nécessairement une fonction alternée des racines primitives de $x^n = 1$. D'après ce qui précède, pour l'équation $x^{\nu^a} = 1$, la somme de ses racines primitives est égale à -1, et a pour carré l'unité, et la somme alternée de ses racines primitives est nulle ou a pour carré $\pm\nu^a$. Ainsi, pour l'équation $x^n = 1$, $\mathcal{S}$ est nulle ou $\mathcal{S}^2 = \pm n$ ou $\mathcal{S} = \pm\omega$, où ω est un diviseur de n. Si chaque produit formant la somme $\mathcal{S}$ est une somme alternée, alors $\mathcal{S} = 0$ ou $\mathcal{S} = \pm n$. En particulier, pour que $\mathcal{S}^2 = \pm n$, la somme devra être composée de sommes alternées seulement, les facteurs impairs de n devront être tous distincts et le facteur pair devra être
4 ou 8.

Cauchy consacre la suite de cette note à la détermination des fonctions alternées des racines primitives de $x^n = 1$. Il considère une fonction entière de la racine primitive ρ, que l'on peut écrire sous la forme $f(\rho) = a_0 + a_1\rho + a_2\rho^2 + \cdots + a_{n-1}\rho^{n-1}$, et qui répond aux conditions suivantes:

> Supposons d'ailleurs que, dans le cas où l'on remplace la racine primitive ρ de l'équation (1) $[x^{n-1}]$ par une autre racine primitive ρ^m de la même équation, les différents termes contenus dans $f(\rho)$ se transforment, au signe près, les uns dans les autres, et que deux termes, qui se déduisent ainsi l'un de l'autre, se trouvent toujours affectés du même signe pour certaines valeurs $h, h', h'', \ldots$, du nombre m, mais affectés de signes contraires pour d'autres valeurs $k, k', k'', \ldots$du même nombre[...] (Cauchy 1840a, p. 257).

Cauchy appelle une telle fonction *fonction alternée*. Pour satisfaire ces conditions, a_0 doit être nul et $f(\rho)$ est une fonction linéaire de sommes alternées des racines primitives de $x^n = 1$ ou de $x^\omega = 1$, où ω est un diviseur de n. L'objectif est alors de déterminer les formes de ces fonctions dans des cas particuliers et pour ce faire, Cauchy s'appuie sur les résultats précédents. Par exemple, dans le cas où $n = \nu^a$, où ν est un nombre premier impair et a un entier positif non nul, on sait d'après ce qui précède que les sommes alternées des racines primitives de l'équation $x^{\nu^a} = 1$ sont nulles sauf si $i = 1$. Ainsi, si on note Δ la somme alternée des racines primitives de $x^\nu = 1$, on sait que $f(\rho) = a\Delta$, où a est un coefficient indépendant de ρ. Cauchy analyse ainsi tous les cas comme précédemment et applique à chaque fois les résultats obtenus sur les sommes alternées des racines primitives d'équations binômes $x^\omega = 1$, où ω est un diviseur de n. Finalement, il montre que $[f(\rho)]^2 = \pm\omega a^2$, où $\omega = n$ si n est composé de facteurs impairs distincts, et éventuellement du facteur 4 ou 8.

Dans les deux notes suivantes, Cauchy s'intéresse aux propriétés des exposants des racines primitives d'une équation binôme dans une somme alternée. Dans un premier temps, il démontre des théorèmes sur les sommes $h + h' + h'' + \cdots$ et $k + k' + k'' + \cdots$ selon la forme du nombre n. Il montre par exemple que si n est un nombre impair ou multiple de 4, dont la décomposition en facteurs premiers est $\nu^a\nu'^b\nu''^c \ldots$, et si la somme alternée des racines primitives de $x^n = 1$ est également une fonction alternée des racines primitives de $x^{\nu^a} = 1, \ldots$, alors $h + h' + h'' + \cdots \equiv k + k' + k'' + \cdots \equiv 0 \pmod{n}$. Il observe également que si dans la somme alternée des racines primitives de $x^n = 1$, on remplace la racine ρ par ρ^l (où l est premier à n), alors la somme est

inchangée si l fait partie des nombres h, h', ...et elle change de signe si l fait partie des nombres k, k', ... Il expose ensuite une technique pour savoir si deux racines primitives données ρ et ρ^l sont précédées du même signe ou non dans la somme $\mathcal{S}$, toujours selon la forme de n.

Nous venons de donner un aperçu des résultats et méthodes exposés par Cauchy dans les notes VI à IX: il nous donne à voir une étude détaillée des propriétés de certaines expressions symétriques et alternées des racines primitives des équations binômes. Comme nous l'avons déjà évoqué, certaines de ces propriétés sont fondamentales pour la démonstration de la méthode de Cauchy sur les formes quadratiques. Nous pensons notamment au fait que lorsque n est un nombre premier, une fonction symétrique des racines primitives de $x^n = 1$ est toujours de la forme $a_0 + a_1(\rho + \rho^2 + \cdots + \rho^{n-1})$. D'autre part, une somme alternée des racines primitives d'une équation $x^n = 1$, où $n = \nu^a \nu'^b \nu''^c \ldots$, est toujours proportionnelle à un produit dont chaque facteur est la somme ou une somme alternée des racines primitives d'une des équations $x^{\nu^a} = 1, \ldots$.

Il est également intéressant d'observer l'importance des fonctions symétriques et alternées dans les différents travaux de Cauchy. Bien évidemment, ce dernier n'a pas l'exclusivité des recherches sur ce thème mais il est néanmoins le seul savant de la scène française à donner une grande place à ce type de résultats en théorie des nombres. Il met d'ailleurs explicitement en avant l'importance de ces expressions en algèbre et théorie des nombres dans une note insérée aux *Comptes rendus* de l'Académie le 3 février 1840 : «La considération de ces fonctions [les fonctions alternées] conduit à un grand nombre de formules remarquables, soit dans l'Algèbre, soit dans la théorie des nombres» (Cauchy 1840d, p. 81).

4.4 Multiplication des sommes de Gauss (Note III)

Cauchy dédie la cinquantaine de pages de la troisième note à l'étude de la multiplication des expressions Θ_h et fait le lien avec certains résultats sur les formes quadratiques. Nous allons détailler certains passages de cette note, en nous focalisant sur la multiplication des sommes de Gauss.

4.4.1 Lorsque n est un nombre premier

Comme en début de chaque note, Cauchy rappelle certains résultats obtenus auparavant: si p est un nombre premier, n un diviseur de $p-1$, avec $p = n\varpi + 1$, et ρ une racine primitive de $x^n = 1$, et $\Theta_h = \theta + \rho^h\theta^t + \rho^{2h}\theta^{t^2} + \cdots + \rho^{(p-2)h}\theta^{t^{p-2}}$ alors

- $\Theta_h = \Theta_0 = -1$;
- si h n'est pas divisible par n : $\Theta_h\Theta_{-h} = (-1)^{\varpi h}p = \Theta_h\Theta_{n-h}$;
- Si h n'est pas divisible par $p-1$: $\Theta_h\Theta_{-h} = (-1)^h p$;
- $\Theta_h\Theta_k = R_{h,k}\Theta_{h+k}$, où $R_{h,k}$ est une fonction entière de ρ.

Soient h, k, l, des nombres entiers quelconques. En appliquant plusieurs fois l'égalité précédente, on trouve: $\Theta_h\Theta_k\Theta_l \ldots = R_{h,k,l,\ldots}\Theta_{h+k+l+\cdots}$, où $R_{h,k,l\ldots}$ est une fonction entière de ρ telle que $R_{h,k,l,\ldots} = R_{h,k}R_{h+k,l}\cdots$.

Enfin, Cauchy rappelle que comme le produit $\Theta_h\Theta_k\Theta_l \ldots$ et l'expression $\Theta_{h+k+l+\cdots}$ sont des fonctions symétriques et entières de $\rho^h, \rho^k, \rho^l, \ldots$, et donc des

fonctions linéaires à coefficients entiers des différentes sommes $\rho^{ih}+\rho^{ik}+\rho^{il}+\cdots$, où $1 \leq i \leq n-1$. On peut donc en déduire qu'il en est de même pour $R_{h,k,l,\ldots} = \dfrac{\Theta_h\Theta_k\Theta_l\ldots}{\Theta_{h+k+l+\cdots}}$.

Cauchy distingue alors les différents cas selon la forme du nombre n.

Si $n=2$, alors $\rho=-1$, $\varpi=\frac{p-1}{2}$ et $\Theta_1^2=(-1)^{\frac{p-1}{2}}p$, soit

$$(\theta-\theta^t+\theta^{t^2}-\cdots-\theta^{t^{p-2}})^2=(-1)^{\frac{p-1}{2}}p.$$

Si n est un nombre premier impair, alors les racines primitives de $x^n=1$ sont les ρ^i, avec $1 \leq i \leq n-1$. D'après l'égalité $\Theta_h\Theta_{-h}=(-1)^h p$, et puisque $\frac{p-1}{n}$ est pair (car p et n sont des nombres impairs):

$$\Theta_1\Theta_{n-1}=\Theta_2\Theta_{n-2}=\cdots=\Theta_{\frac{n-1}{2}}\Theta_{\frac{n+1}{2}}=(-1)^{\frac{p-1}{n}h}p=p.$$

On en déduit: $\Theta_1\Theta_2\Theta_3\ldots\Theta_{n-1}=p^{\frac{n-1}{2}}$.

Si s est une racine primitive de l'équivalence $x^{n-1}\equiv 1 \pmod n$, alors les puissances $1, s, s^2, \ldots, s^{n-2}$ représentent modulo n tous les entiers compris entre 1 et $n-1$. L'égalité précédente peut donc s'écrire sous la forme $\Theta_1\Theta_s\Theta_{s^2}\ldots\Theta_{s^{n-2}}=p^{\frac{n-1}{2}}$.

Cauchy utilise ensuite le fait que les racines $1, s^2, s^4, \ldots, s^{n-3}$ sont également racines de l'équivalence $x^{\frac{n-1}{2}}\equiv 1 \pmod n$ et que $s, s^3, \ldots, s^{n-2}$ sont racines de $x^{\frac{n-1}{2}}\equiv -1 \pmod n$. Il décompose le produit $\Theta_1\Theta_s\Theta_{s^2}\ldots\Theta_{s^{n-2}}$ en deux produits:

$$\Theta_1\Theta_{s^2}\ldots\Theta_{s^{n-3}}=R_{1,s^2,\ldots,s^{n-3}}\Theta_{1+s^2+\cdots+s^{n-3}} \text{ et } \Theta_s\Theta_{s^3}\ldots\Theta_{s^{n-2}}=R_{s,s^3,\ldots,s^{n-2}}\Theta_{s+s^3+\cdots+s^{n-2}}.$$

Or: $1+s^2+s^4+\cdots+s^{n-3}=\dfrac{s^{n-1}-1}{s^2-1}\equiv 0 \pmod n$ et

$s+s^3+s^5+\cdots+s^{n-2}=s\dfrac{s^{n-1}-1}{s^2-1}\equiv 0 \pmod n$.

Comme $\Theta_0=-1$, les égalités précédentes deviennent:

$$\Theta_1\Theta_{s^2}\ldots\Theta_{s^{n-3}}=-R_{1,s^2,\ldots,s^{n-3}} \text{ et } \Theta_s\Theta_{s^3}\ldots\Theta_{s^{n-2}}=-R_{s,s^3,\ldots,s^{n-2}}.$$

Finalement, $\Theta_1\Theta_{s^2}\ldots\Theta_{s^{n-3}}$ et $R_{1,s^2,\ldots,s^{n-3}}$ sont des fonctions entières et symétriques de $\rho, \rho^{s^2}, \ldots, \rho^{s^{n-3}}$; $\Theta_s\Theta_{s^3}\ldots\Theta_{s^{n-2}}$ et $R_{s,s^3,\ldots,s^{n-2}}$ sont des fonctions entières et symétriques de $\rho^s, \rho^{s^3}, \ldots, \rho^{s^{n-2}}$.

De plus, une fonction entière et symétrique de $\rho, \rho^{s^2}, \ldots, \rho^{s^{n-3}}$ est une fonction linéaire des sommes $\rho^m+\rho^{ms^2}+\cdots+\rho^{ms^{n-3}}$, $m \leq n$. Ces sommes sont toujours égales à $\rho+\rho^{s^2}+\cdots+\rho^{s^{n-3}}$ ou $\rho^s+\rho^{s^3}+\cdots+\rho^{s^{n-2}}$. Donc: $\Theta_1\Theta_{s^2}\ldots\Theta_{s^{n-3}}=c_0+c_1(\rho+\rho^{s^2}+\cdots+\rho^{s^{n-3}})+c_2(\rho^s+\rho^{s^3}+\cdots+\rho^{s^{n-2}})$, et, en remplaçant ρ par ρ^s: $\Theta_s\Theta_{s^3}\ldots\Theta_{s^{n-2}}=c_0+c_1(\rho^s+\rho^{s^3}+\cdots+\rho^{s^{n-2}})+c_2(\rho+\rho^{s^2}+\cdots+\rho^{s^{n-3}})$.

On a $\rho+\rho^s+\rho^{s^2}+\cdots+\rho^{s^{n-2}}=-1$. Si on remplace p par n, θ par ρ et t par s, et si on pose $\rho-\rho^s+\rho^{s^2}-\cdots-\rho^{s^{n-2}}=\Delta$, on a alors $\Delta^2=(-1)^{\frac{n-1}{2}}n$.

On en déduit: $\rho+\rho^{s^2}+\cdots+\rho^{s^{n-3}} = -\dfrac{1-\Delta}{2}$ et $\rho^s+\rho^{s^3}+\cdots+\rho^{s^{n-2}} = -\dfrac{1+\Delta}{2}$, soit:

$$\begin{cases} 2\Theta_1\Theta_{s^2}\Theta_{s^4}\ldots\Theta_{s^{n-3}} = A + B\Delta, \\ 2\Theta_s\Theta_{s^3}\Theta_{s^5}\ldots\Theta_{s^{n-2}} = A - B\Delta, \end{cases}$$

où $A = 2c_0 - c_1 - c_2$, $B = c_1 - c_2$ sont de même parité. Nous verrons que ces résultats permettent d'obtenir très facilement une forme quadratique de la forme souhaitée.

Finalement, Cauchy introduit ici deux nouvelles notations, avant de les utiliser pour traduire certaines des égalités précédentes:

- $[1] = \Theta_1\Theta_{s^2}\Theta_{s^4}\ldots\Theta_{s^{n-3}}$, produit composé des facteurs Θ_h tels que $h^{\frac{n-1}{2}} \equiv 1 \pmod{n}$.
- $[-1] = \Theta_s\Theta_{s^3}\Theta_{s^5}\ldots\Theta_{s^{n-2}}$, produit composé des facteurs Θ_h tels que $h^{\frac{n-1}{2}} \equiv -1 \pmod{n}$.

Il traduit ainsi les égalités obtenues précédemment par:

$$p^{\frac{n-1}{2}} = [1][-1], \quad 2[1] = A + B\Delta, \quad 2[-1] = A - B\Delta.$$

Remarquons que ces notations sont introduites dans cette note là uniquement, et semblent donc avoir été créées par Cauchy après ses travaux de 1830-1831.

4.4.2 Lorsque n est un nombre composé

Dans la deuxième partie de cette troisième note, Cauchy généralise sa méthode en redéfinissant tout d'abord les expressions Θ_h. Il considère les cas où le nombre n est produit de deux facteurs premiers impairs, puis trois facteurs premiers impairs, puis enfin des formes 2ν, 4ν et 8ν, où ν est un facteur premier impair. Nous nous arrêtons ici sur le premier cas considéré: lorsque $n = \nu\omega$, où ν et ω sont deux facteurs premiers impairs distincts.

Soit ς, une racine primitive de l'équation $x^\nu = 1$ et α, une racine primitive de l'équation $x^\omega = 1$. Alors, $\rho = \varsigma\alpha$ est bien une racine primitive de $x^n = 1$, et on aura $\rho^h = \varsigma^i\alpha^j$, où $h \equiv i \pmod{\nu}$ et $h \equiv j \pmod{\omega}$.

Ainsi, Θ_h, que Cauchy note également $\Theta_{i,j}$ ici, peut être exprimé en fonction des indices i et j : $\Theta_h = \theta + \varsigma^i\alpha^j\theta^t + \varsigma^{2i}\alpha^{2j}\theta^{t^2} + \cdots + \varsigma^{(p-2)i}\alpha^{(p-2)j}\theta^{t^{p-2}} = \Theta_{i,j}$.

Cauchy donne ensuite des propriétés de $\Theta_{i,j}$:

- $\Theta_{i,j} = \Theta_{i+k\nu,j+k'\omega}$;
- Si $\Theta_h = \Theta_{i,j}$, alors $\Theta_{-h} = \Theta_{-i,-j}$;
- h et i sont de même parité si $\varpi = \frac{p-1}{\nu\omega}$ est impair;
- Si i est divisible par ν et j est divisible par ω, alors $\Theta_{i,j} = \Theta_{0,0} = -1$;
- Dans le cas contraire, $\Theta_{i,j}\Theta_{-i,-j} = (-1)^{\varpi j}p = \Theta_{i,j}\Theta_{\nu-i,\omega-j}$.

Enfin, puisque $p - 1 = \nu\omega\varpi$, si ν et ω sont impairs, alors ϖ est pair, et donc la dernière égalité devient: $\Theta_{i,j}\Theta_{-i,-j} = p$.

Soit u une racine primitive de $x^{\nu-1} \equiv 1 \pmod{\nu}$ et a une racine primitive de $x^{\omega-1} \pmod{\omega}$. À partir des propriétés des racines primitives et de la définition de $\Theta_{i,j}$ donnée précédemment, toutes les valeurs de Θ_h, où h est premier à n, sont donc représentées par:

$$\begin{cases} \Theta_{1,1} & \Theta_{u,1} & \Theta_{u^2,1} & \dots \Theta_{u^{\nu-2},1} \\ \Theta_{1,a} & \Theta_{u,a} & \Theta_{u^2,a} & \dots \Theta_{u^{\nu-2},a} \\ \Theta_{1,a^2} & \Theta_{u,a^2} & \Theta_{u^2,a^2} & \dots \Theta_{u^{\nu-2},a^2} \\ \dots & \dots & \dots & \dots\dots \\ \Theta_{1,a^{\omega-2}} & \Theta_{u,a^{\omega-2}} & \Theta_{u^2,a^{\omega-2}} & \dots \Theta_{u^{\nu-2},a^{\omega-2}} \end{cases}$$

Ces différentes valeurs sont au nombre de $N = (\nu-1)(\omega-1)$. N est aussi égal au nombre de termes compris entre 1 et $n-1$, premiers à $n = \nu\omega$.

Cauchy applique les principes précédents au cas où $n = \nu\omega$. On cherche à obtenir $\Theta_{h+k+l+\dots} = -1$ pour avoir $\Theta_h\Theta_k\Theta_l \dots = -R_{h,k,l,\dots}$ comme précédemment et ainsi pouvoir utiliser les propriétés des fonctions symétriques. Pour cela, la somme $h+k+l+\cdots$ doit être divisible par $n = \omega\nu$. C'est le cas si on prend toutes les valeurs Θ_h de la forme $\theta_{u^{2i},a^{2j}}$. Dans ce cas, $h+k+l+\cdots$ est équivalente modulo ν à la somme des premiers indices dans $\Theta_{i,j}$, soit: $\frac{\omega-1}{2}(1+u^2+\cdots+u^{\nu-3}) = \frac{\omega-1}{2}\frac{u^{\nu-1}-1}{u^2-1} \equiv 0 \pmod{\nu}$. D'autre part, $h+k+l+\cdots$ est équivalente modulo ω à la somme des seconds indices dans $\Theta_{i,j}$, soit: $\frac{\nu-1}{2}(1+a^2+\cdots+a^{\omega-3}) = \frac{\nu-1}{2}\frac{u^{\omega-1}-1}{u^2-1} \equiv 0 \pmod{\omega}$.
De plus, si $\Theta_h = \Theta_{i,j}$, alors $\varsigma^h = \varsigma^i$ et $\alpha^h = \alpha^j$, donc le produit

$$(\Theta_{1,1}\Theta_{u^2,1}\dots\Theta_{u^{\nu-3},1})(\Theta_{1,a^2}\Theta_{u^2,a^2}\dots\Theta_{u^{\nu-3},a^2})\dots(\Theta_{1,a^{\omega-3}}\Theta_{u^2,\omega-3}\dots\Theta_{u^{\nu-3},\omega-3})$$

est une fonction symétrique de $\varsigma, \varsigma^{u^2}, \dots, \varsigma^{u^{\nu-3}}$ et de $\alpha, \alpha^{a^2}, \dots, \alpha^{a^{\omega-3}}$.

Cauchy introduit une notation similaire à [1] pour simplifier les raisonnements: $[1,1] = (\Theta_{1,1}\Theta_{u^2,1}\dots\Theta_{u^{\nu-3},1})(\Theta_{1,a^2}\Theta_{u^2,a^2}\dots\Theta_{u^{\nu-3},a^2})\dots(\Theta_{1,a^{\omega-3}}\Theta_{u^2,\omega-3}\cdots\Theta_{u^{\nu-3},\omega-3})$, ce qui correspond au produit des Θ_h tel que h est premier à n et vérifie les équivalences $x^{\frac{\nu-1}{2}} \equiv 1 \pmod{\nu}$ et $x^{\frac{\omega-1}{2}} \equiv 1 \pmod{\omega}$. De même, $[1,-1]$ désigne le produit des Θ_h tel que h est premier à n et vérifie les équivalences $x^{\frac{\nu-1}{2}} \equiv 1 \pmod{\nu}$ et $x^{\frac{\omega-1}{2}} \equiv -1 \pmod{\omega}$, et ainsi de suite. On a donc:

$$[1,1] = (\Theta_{1,1}\Theta_{u^2,1}\dots\Theta_{u^{\nu-3},1})(\Theta_{1,a^2}\Theta_{u^2,a^2}\dots\Theta_{u^{\nu-3},a^2})\dots(\Theta_{1,a^{\omega-3}}\Theta_{u^2,a^{\omega-3}}\dots\Theta_{u^{\nu-3},a^{\omega-3}}),$$
$$[1,-1] = (\Theta_{1,a}\Theta_{u^2,a}\dots\Theta_{u^{\nu-3},a})(\Theta_{1,a^3}\Theta_{u^2,a^3}\dots\Theta_{u^{\nu-3},a^3})\dots(\Theta_{1,a^{\omega-2}}\Theta_{u^2,a^{\omega-2}}\dots\Theta_{u^{\nu-3},a^{\omega-2}}),$$
$$[-1,1] = (\Theta_{u,1}\Theta_{u^3,1}\dots\Theta_{u^{\nu-2},1})(\Theta_{u,a^2}\Theta_{u^3,a^2}\dots\Theta_{u^{\nu-2},a^2})\dots(\Theta_{u,a^{\omega-3}}\Theta_{u^3,a^{\omega-3}}\dots\Theta_{u^{\nu-2},a^{\omega-3}}),$$
$$[-1,-1] = (\Theta_{u,a}\Theta_{u^3,a}\dots\Theta_{u^{\nu-2},a})(\Theta_{u,a^3}\Theta_{u^3,a^3}\dots\Theta_{u^{\nu-2},a^3})\dots(\Theta_{u,a^{\omega-2}}\Theta_{u^3,a^{\omega-2}}\dots\Theta_{u^{\nu-2},a^{\omega-2}}).$$

De manière similaire, le produit $[1,-1]$ est une fonction symétrique de $\varsigma, \varsigma^{u^2}, \dots, \varsigma^{u^{\nu-3}}$ et de $\alpha^a, \alpha^{a^3}, \dots, \alpha^{a^{\omega-2}}$, et ainsi de suite.

De plus, $u^{\frac{\nu-1}{2}} \equiv -1 \pmod{\nu}$ et $a^{\frac{\omega-1}{2}} \equiv -1 \pmod{\omega}$, donc l'égalité $\Theta_{i,j}\Theta_{-i,-j}$ devient: $\Theta_{u^m,a^{m'}}\Theta_{a^{m\pm\frac{\nu-1}{2}},u^{m'\pm\frac{\omega-1}{2}}} = \Theta_{u^m,a^{m'}}\Theta_{-u^m,-a^{m'}} = p$.

D'après cette dernière propriété, on peut déterminer la valeur des expressions $[\pm 1, \pm 1]$ ou au moins la valeur de leurs produits en fonction de la parité des nombres $\frac{\nu-1}{2}$ et $\frac{\omega-1}{2}$, et donc de la forme des facteurs ν et ω.

En effet, si ν est de la forme $4x+1$, alors les indices m et $m \pm \frac{\nu-1}{2}$ sont de même parité. Il en est de même pour ω. Ainsi, dans le cas où ν et ω sont tous deux de la forme $4x+1$, chacun des produits $[\pm 1, \pm 1]$ sont formés de $\frac{N}{4}$ produits de la forme correspondant à la formule précédente. Ainsi, $[\pm 1, \pm 1] = p^{\frac{N}{8}}$. Finalement:

$$p^{\frac{N}{2}} = [1, 1][1, -1][-1, 1][-1, -1].$$

Cauchy montre que l'on obtient la même égalité quelque soit la forme des nombres ν et ω.

Cauchy continue sa démonstration en commençant le cas où ν et ω sont des nombres de la forme $4x+3$. Alors, d'après ce qui précéde, le produit $[1, 1][1, -1]$ sera une fonction symétrique de $\varsigma, \varsigma u^2, \varsigma^{u^4}, \ldots, \varsigma^{u^{\nu-3}}$ et donc une fonction linéaire des sommes $\varsigma+\varsigma^{u^2}+\varsigma^{u^4}+\cdots+\varsigma^{u^{\nu-3}}$ et $\varsigma^u+\varsigma^{u^3}+\varsigma^{u^5}+\cdots+\varsigma^{u^{\nu-2}}$. Ce produit sera également une fonction symétrique de $\alpha, \alpha^a, \alpha^{a^2}, \ldots, \alpha^{a^{\omega-2}}$, et donc de leur somme, qui est égale à -1. Finalement, on a:

$$[1, 1][1, -1] = c_0 + c_1(\varsigma+\varsigma^{u^2}+\varsigma^{u^4}+\cdots+\varsigma^{u^{\nu-3}}) + c_2(\varsigma^u+\varsigma^{u^3}+\varsigma^{u^5}+\cdots+\varsigma^{u^{\nu-2}}).$$

On obtient une expression similaire du produit $[-1, 1][-1, -1]$ en substituant ς^u à ς:

$$[-1, 1][-1, -1] = c_0 + c_1(\varsigma^u+\varsigma^{u^3}+\varsigma^{u^5}+\cdots+\varsigma^{u^{\nu-2}}) + c_2(\varsigma+\varsigma^{u^2}+\varsigma^{u^4}+\cdots+\varsigma^{u^{\nu-3}}).$$

En reprenant des notations similaires à la première de la note, on pose $\varsigma-\varsigma^u+\varsigma^{u^2}-\varsigma^{u^3}+\cdots-\varsigma^{u^{\nu-2}} = \Delta$. On a alors: $\Delta^2 = (-1)^{\frac{\nu-1}{2}}\nu$. De plus: $\varsigma+\varsigma^u+\varsigma^{u^2}+\varsigma^{u^3}+\cdots+\varsigma^{u^{\nu-2}} = -1$. On a donc $[1, 1][1, -1] = \frac{1}{2}(A+B\Delta)$ et $[-1, 1][-1, -1] = \frac{1}{2}(A-B\Delta)$, où $A = 2c_0 - c_1 - c_2$ et $B = c_1 - c_2$. On remarque de grandes similitudes avec le type de formules obtenues par Cauchy précédemment, dans le cas où le nombre n était premier impair. En considérant plutôt les produits $[1, 1][-1, 1]$ et $[1, -1][-1, -1]$, on obtient des formules semblables, mais pour $\Delta^2 = (-1)^{\frac{\omega-1}{2}}\omega$.

Cauchy analyse les autres cas, et remarque que les formules ainsi obtenues coïncident bien avec ce qui a été obtenu dans les première, troisième et quatrième parties du mémoire, et qu'elles peuvent être généralisées.

Finalement, Cauchy obtient dans cette note la plupart des résultats fondamentaux pour obtenir des égalités de la forme $4p^\mu = x^2+ny^2$, en s'appuyant sur les propriétés démontrées dans les notes résumées précédemment. Il montre que les expressions $R_{h,k,l,\ldots}$ sont des fonctions symétriques et entières des racines ρ^h, ρ^k, ρ^l, ... Il en déduit que, dans le cas où le nombre n est premier, $\Theta_1\Theta_s\Theta_{s^2}\ldots\Theta_{s^{n-2}} = p^{\frac{n-1}{2}}$ d'une part et que $2\Theta_1\Theta_{s^2}\ldots\Theta_{s^{n-3}} = A+B\Delta$ et $2\Theta_s\Theta_{s^3}\ldots\Theta_{s^{n-2}} = A-B\Delta$ d'autre part.

Lorsque n est composé de deux facteurs premiers ν et ω, Cauchy adapte l'expression de Θ_h pour faire apparaître les racines primitives des équations binômes associés aux

deux facteurs premiers de n. Il obtient ainsi de la même façon une puissance de p à partir de produits de sommes de Gauss; ces produits peuvent également être mis sous la forme $A \pm B\Delta$ où $\Delta^2 = (-1)^{\frac{\nu-1}{2}}\nu$ ou $\Delta^2 = (-1)^{\frac{\omega-1}{2}}\omega$.

4.5 Utilisation des nombres de Bernoulli dans la théorie des nombres (Note IV)

Comme nous l'avons déjà signalé précédemment, c'est vraisemblablement Cauchy qui fait le lien pour la première fois entre résidus quadratiques et nombres de Bernoulli. En 1831, Cauchy énonce son théorème sans aucune justification; il fournit dans la quatrième note du mémoire de 1840 une démonstration détaillée de la relation alors annoncée entre nombres de Bernoulli et résidus quadratiques. Remarquons qu'un résumé de cette démonstration se trouve également dans le premier paragraphe de la partie principale du mémoire: cette preuve a donc été en partie annoncée par Cauchy en 1830 à l'Académie des sciences. Nous résumons ici ce que Cauchy expose dans la note IV. Cauchy y utilise des résultats de calcul intégral et différential; les nombres de Bernoulli interviennent lors de résultats sur le développement en série entière de $\tan z$.

Cauchy commence par rappeler des propriétés sur les résidus et non-résidus quadratiques d'un nombre premier p, dont l'égalité:

$$\left[\frac{1}{p}\right] + \left[\frac{2}{p}\right] + \left[\frac{3}{p}\right] + \cdots + \left[\frac{p-1}{p}\right] = 0. \tag{10}$$

Il se place ensuite dans un cas plus général, où il considère un ensemble fini de nombres premiers à p; l'objectif est ici de déterminer la valeur de la différence entre le nombre de résidus et non-résidus quadratiques contenus dans cet ensemble de nombres.

Soient $a, b, c, \ldots, l$, un ensemble de n nombres premiers à p. Soit n', le nombre de résidus quadratiques contenus dans cet ensemble, et n'' le nombre de non-résidus quadratiques. Alors $n' + n'' = n$ et $n' - n'' = \left[\frac{1}{p}\right] + \left[\frac{2}{p}\right] + \left[\frac{3}{p}\right] + \cdots + \left[\frac{p-1}{p}\right]$ ce qui donne l'égalité

$$n' - n'' = a^{\frac{p-1}{2}} + b^{\frac{p-1}{2}} + c^{\frac{p-1}{2}} + \cdots + l^{\frac{p-1}{2}} \pmod{p}, \tag{13}$$

que Cauchy réécrit en utilisant le calcul différentiel:

$$n' - n'' \equiv \frac{d^{\frac{p-1}{2}}(e^{az} + e^{bz} + e^{cz} + \cdots + e^{lz})}{dz^{\frac{p-1}{2}}} \pmod{p}, \tag{14}$$

où l'on pose $z = 0$ aprés la différenciation. Selon Cauchy, utiliser l'outil du calcul différentiel permet d'obtenir facilement la valeur de la différence $n' - n''$, et d'en déduire les valeurs de n' et n'', dans le cas où $n < p$ et où les nombres $a, b, c, \ldots l$, peuvent être mis sous la forme d'une progression arithmétique $h, h+k, h+2k, \ldots, h+$

$(n-1)k$. Dans ce cas:

$$e^{az}+e^{bz}+e^{cz}+\cdots+e^{lz}=\sum_{i=0}^{n-1}e^{(h+ikz)}=e^{hz}\sum_{i=0}^{n-1}e^{ikz}=e^{hz}\frac{e^{nkz-1}}{e^{kz-1}}.$$

Donc (14) devient:

$$n'-n''=\frac{d^{\frac{p-1}{2}}}{dz^{\frac{p-1}{2}}}\left[e^{hz}\frac{e^{nkz-1}}{e^{kz-1}}\right]. \tag{15}$$

Cauchy développe alors un exemple «pour fixer les idées»: le cas où l'on cherche le nombre de résidus quadratiques et de non-résidus quadratiques inférieurs à $\frac{p}{2}$. On considère donc la progression arithmétique 1, 2, 3, ..., $\frac{p-1}{2}$, soit $n=\frac{p-1}{2}$, $h=1$, $k=1$ et

$$n'-n''=\frac{d^{\frac{p-1}{2}}}{dz^{\frac{p-1}{2}}}\left(\frac{e^{\frac{p+1}{2}z}-e^{z}}{e^{z-1}}\right). \tag{16}$$

Il détermine ensuite la différence entre le rapport $\frac{e^{\frac{p+1}{2}z}-e^{z}}{e^{z-1}}$ et ce même rapport lorsque $p=0$: $\frac{e^{\frac{p+1}{2}z}-e^{z}}{e^{z}-1}-\frac{e^{\frac{1}{2}z}-e^{z}}{e^{z}-1}=\frac{e^{\frac{p+1}{2}z}-e^{\frac{1}{2}z}}{e^{z}-1}=\left(e^{\frac{p+1}{2}z}-e^{\frac{1}{2}z}\right)(e^{z}-1)^{-1}$. Cauchy en déduit que la dérivée d'ordre $\frac{p-1}{2}$ de cette expression est composée de termes proportionnels à $e^{\frac{p+1}{2}z}-e^{\frac{1}{2}z}$ ou à une de ses dérivées. Comme $e^{\frac{p+1}{2}z}-e^{\frac{1}{2}z}$ et ses dérivées s'annulent lorsque l'on prend $z=0$ et $p=0$, et comme $\frac{e^{\frac{1}{2}z}-e^{z}}{e^{z}-1}=-\frac{1}{2}\left(1+\frac{e^{\frac{1}{4}z}-e^{-\frac{1}{4}z}}{e^{\frac{1}{4}z}+e^{-\frac{1}{4}z}}\right)$, on obtient, pour $z=0$:

$$\frac{d^{\frac{p-1}{2}}}{dz^{\frac{p-1}{2}}}\left(\frac{e^{\frac{p+1}{2}z}-e^{z}}{e^{z}-1}-\frac{e^{\frac{1}{2}z}-e^{z}}{e^{z}-1}\right)\equiv 0 \pmod{p}.$$

On obtient donc, d'après (16) et ce qui précède:

$$n'-n''\equiv-\frac{1}{2}\frac{d^{\frac{p-1}{2}}}{dz^{\frac{p-1}{2}}}\left(\frac{e^{\frac{1}{4}z}-e^{-\frac{1}{4}z}}{e^{\frac{1}{4}z}+e^{-\frac{1}{4}z}}\right) \pmod{p}. \tag{18}$$

Comme après les différenciations, on pose $z=0$, on peut remplacer z par $z\sqrt{-1}$, ce qui permet d'introduire la fonction tangente, et donc les nombres de Bernoulli:

$$n'-n''\equiv(-1)^{1-\frac{p-1}{4}}\frac{1}{2}\frac{d^{\frac{p-1}{2}}\tan\frac{z}{4}}{dz^{\frac{p-1}{2}}}. \tag{19}$$

Enfin, Cauchy rappelle le développement de $\tan z$:

$$\tan\frac{z}{4} = 2\left(\frac{1}{6}\frac{2^2-1}{2}\frac{z}{1.2} + \frac{1}{30}\frac{2^4-1}{2^3}\frac{z^3}{1.2.3.4} + \frac{1}{42}\frac{2^4-1}{2^4}\frac{z^4}{1.2.3.4.5.6} + \cdots\right), \tag{20}$$

où $\frac{1}{6}, \frac{1}{30}, \frac{1}{42}, \ldots$ représentent les nombres de Bernoulli, notés comme précédemment $\mathscr{A}_1, \mathscr{A}_2, \mathscr{A}_3, \ldots$

L'introduction des nombres de Bernoulli peut paraître étonnante voire artificielle ici: en effet, Cauchy travaille initialement avec une somme de puissances de nombres entiers, et passe par des manipulations liées à l'analyse pour finalement obtenir une expression dépendant de $\tan z$, et ainsi utiliser son développement avec les nombres de Bernoulli. Rappelons néanmoins que les nombres de Bernoulli ont d'abord été introduits par Jacques Bernoulli lors de son étude de sommes de puissances semblables, de la forme $1^k+2^k+\cdots+x^k$. Cela est d'ailleurs indiqué dans un des ouvrages de Lacroix intitulé *Traité des différences et des séries, faisant suite au traité du calcul différentiel et du calcul intégral*, publié en 1800 et qui est bien connu.[46] D'autre part, les nombres de Bernoulli apparaissent dans les séries de Taylor des fonctions trigonométriques: dans son traité, Lacroix donne également le développement de la cotangente en fonction des nombres de Bernoulli (Lacroix 1800, p. 427). Ces développements trigonométriques sont donc présents dans certains traités d'analyse.

Cauchy va maintenant considérer deux cas, selon que p est de la forme $4x+1$, et donc $\frac{p-1}{2}$ pair, ou p est de la forme $4x+3$, soit $\frac{p-1}{2}$ impair.

Si p est de la forme $4x+1$, alors $n'-n'' \equiv 0 \pmod p$ (car d'après le développement de $\tan z$, la dérivée k^e de $\tan z$ est nulle pour $z=0$ si k est pair). Dans ce cas, $n' \equiv n'' \equiv \frac{p-1}{4} \pmod p$, soit $n' = n'' = \frac{p-1}{4}$.

Si p est de la forme $4x+3$, alors on utilise les formules précédentes ainsi que l'équivalence $2^{p-1} \equiv 1 \pmod p$ et on obtient:

$$n' - n'' \equiv (-1)^{\frac{p+1}{2}} 2\left(2 - 2^{\frac{p-1}{2}}\right)\mathscr{A}_{\frac{p+1}{4}} \pmod p. \tag{21}$$

Cauchy utilise ensuite des résultats qu'il ne démontrera que plus loin:

- Si p est de la forme $8x+3$, alors $2^{\frac{p-1}{2}} \equiv -1 \pmod p$ et donc $n' - n'' \equiv -6\mathscr{A}_{\frac{p+1}{4}}$. On en déduit donc, puisque $n' + n'' = \frac{p-1}{2}$: $n' \equiv \frac{p-1}{4} - 3\mathscr{A}_{\frac{p+1}{4}}$ et $n'' \equiv \frac{p-1}{4} + 3\mathscr{A}_{\frac{p+1}{4}}$
- Si p est de la forme $8x+7$, alors $2^{\frac{p-1}{2}} \equiv 1 \pmod p$ et donc $n' - n'' \equiv 2\mathscr{A}_{\frac{p+1}{4}}$. On en déduit donc: $n' \equiv \frac{p-1}{4} + \mathscr{A}_{\frac{p+1}{4}}$ et $n'' \equiv \frac{p-1}{4} - \mathscr{A}_{\frac{p+1}{4}}$.

[46] De nombreuses études sont consacrées à Lacroix, son oeuvre didactique et ses traités. Nous renvoyons par exemple aux travaux de P. Lamandé (2004) pour la conception de nombre chez Lacroix, C. J. Domingues (2008) pour une approche conceptuelle du contenu mathématique du *Traité du calcul différentiel et du calcul intégral* de Lacroix et c. Ehrhardt (2009) pour une analyse de l'identité sociale de Lacroix comme mathématicien et enseignant.

Cauchy rappelle qu'il a déjà présenté ces résultats en 1830, et publié un extrait en 1831 dans le *Bulletin de Férussac*.

Signalons également que dans la partie principale de son mémoire, après avoir résumé la preuve détaillée ici, Cauchy reprend les exemples $n = 7$ et $n = 11$ qu'il avait déjà donnés dans (Cauchy 1831). Il développe également l'exemple $n = 163$, mais sans utiliser les nombres de Bernoulli: à partir de la liste des puissances successives d'une racine primitive, il détermine directement les valeurs de nombres n' et n''. Cela vient du fait que seuls les premiers nombres de Bernoulli sont connus, mais il est remarquable que Cauchy ne fasse aucun commentaire à ce sujet. D'autre part, comme en 1831, Cauchy ne justifie pas l'existence de l'inverse des dénominateurs des nombres de Bernoulli dans les équivalences considérées.

4.6 Déterminer un équivalent des expressions $R_{h,k}$ modulo p (Note V)

Dans cette note, Cauchy s'appuie sur une manipulation qu'il utilise à plusieurs reprises dans ses travaux: transposer une équation en équivalence afin de déterminer un équivalent des expressions $R_{h,k}$. Ce résultat permet notamment de déterminer les valeurs des x et y dans l'équation indéterminée $4p^{\mu} = x^2 + ny^2$ pour des valeurs données de p et n.

Comme dans la première note, Cauchy considère le cas particulier où τ est une racine $(p-1)^e$ de l'unité et généralise finalement en remplaçant τ par une racine n^e de l'unité notée ρ. Il commence par rappeler des formules prouvées précédemment: si $h + k$ n'est pas divisible par $p - 1$, alors[47]

$$R_{h,k} = \sum_{\substack{1 \le i \le p-2 \\ t^i + t^j \equiv 1 \pmod p}} = \sum_{i=0}^{p-2} a_i \tau^i,$$

où les a_i sont des coefficients entiers dont la somme est égale à $p - 2$ et t, une racine primitive de p. Cauchy démontre des formules semblables pour les valeurs de $R_{mh,mk}$ en fonction des valeurs de m, h et k.

Cauchy donne ensuite un exemple de calcul des a_i à partir des formules précédentes puis détermine des formules permettant de calculer les coefficients a_i en fonction des sommes $\sum_{\substack{1 \le i \le p-2 \\ t^i + t^j \equiv 1 \pmod p}} (\tau^{ih+jk})$. Ainsi:

$$(p-1)a_m = p - 2 + \sum_{s=1}^{p-2} \tau^{-sm} S(\tau^{s(ih+jk)}).$$

[47] Notons d'ailleurs qu'il utilise presque systématiquement la notation S pour désigner la somme $\sum_{\substack{1 \le i \le p-2 \\ t^i + t^j \equiv 1 \pmod p}}$.

Cauchy traduit ensuite les égalités obtenues en termes d'équivalences:

$$(p-1)a_m \equiv p-2+\sum_{s=1}^{p-2} t^{-sm} S(t^{s(ih+jk)}) \pmod{p}, \text{ soit}$$

$$a_m \equiv 2 - t^{(p-2)m} S(t^{ih+jk}) - t^{(p-3)m} S(t^{2(ih+jk)}) - \cdots - t^{m} S(t^{(p-2)(ih+jk)}) \pmod{p}.$$

À partir de cette formule, on voit qu'il est nécessaire de savoir calculer des équivalents modulo p des sommes $S(t^{s(ih+jk)})$: Cauchy consacre donc la suite de sa note à exposer une méthode permettant d'évaluer des équivalents de ces sommes. Cauchy distingue ainsi trois cas:

- Si $h+k=0$, soit $h=k=0$, alors $S(t^{ih+jk}) \equiv -2 \pmod{p}$.
- Si $h+k=p-1$, alors $S(t^{ij+jk}) \equiv -1 \pmod{p}$.
- Si $h+k$ n'est pas divisible par $p-1$, $S(t^{ih+jk}) \equiv -\Pi_{h,k} \pmod{p}$, avec $\Pi_{h,k} = \frac{1.2.3....(H+K)}{(1.2....H)(1.2....K)}$, où $0 \leq H, K \leq p-1$ sont les résidus de h et k.

Après avoir illustré sa méthode par un exemple, Cauchy conclut: les formules précédentes permettent de déduire que, lorsque $h+k$ n'est pas divisible par $p-1$, «l'expression $\Pi_{-h,-k}$ équivaut, au signe près, à ce que devient la fonction entière de τ représentée par $R_{h,k}$, quand on y remplace une racine primitive τ de l'équation $x^{p-1}=1$ par une racine primitive t de l'équivalence $x^{p-1} \equiv 1 \pmod{p}$» (Cauchy 1840a, p. 196).

Cauchy clôt cette note en mettant en avant la difficulté pratique de sa méthode: il est nécessaire de déterminer des équivalents modulo p des expressions $\Pi_{h,k}$. Il propose d'utiliser la notion d'indice, introduite par Gauss dans les *Disquisitiones Arithmeticae*,[48] et les tables insérées dans (Jacobi 1839). Comme l'indice d'un produit est égal à la somme des indices de ses facteurs et l'indice d'un quotient est égal à la différence entre les indices des deux termes, le calcul des équivalents des $\Pi_{h,k}$ se réduit à effectuer des additions et des soustractions.

Ainsi, Cauchy montre ici comment déterminer des équivalents des sommes de Jacobi modulo p. Ce point permet de compléter l'ensemble des outils et résultats mathématiques nécessaires pour bien comprendre la méthode développée par Cauchy dans la partie principale du mémoire. Avant de nous étendre sur cette partie, nous donnons un aperçu des notes de Cauchy parues dans les *Comptes rendus* de l'Académie entre octobre 1839 et mai 1840.

[48] Gauss introduit la notion d'indice dans la troisième section des *Disquisitiones Arithmeticae*. Il indique d'ailleurs, lorsqu'il met en avant le fait que les diverses puissances d'une racine primitive d'un nombre premier p sont congrues modulo p aux nombres entiers compris entre 1 et $p-1$: «Cette propriété remarquable est d'une bien grande utilité, et peut considérablement abréger les opérations arithmétiques relatives aux congruences, à peu près de la même manière que l'introduction des logarithmes dans l'arithmétique ordinaire en abrège les opérations» (Gauss 1801, art. 57). Il ajoute un peu plus loin: «Les théorèmes qui regardent les indices sont absolument analogues à ceux qui regardent les logarithmes» (Gauss 1801, art. 58).

5 Cauchy et les *Comptes rendus* de l'Académie des sciences: formes quadratiques, cyclotomie et résidus

C'est à partir de 1835 que sont mis en place les *Comptes rendus hebdomadaires des séances de l'Académie des sciences.*[49] Dès son retour en France en 1839, Cauchy fait une utilisation intensive de ces comptes rendus.[50] Entre octobre 1839 et mai 1840, Cauchy publie une dizaine de notes de théorie des nombres qui ne semblent pas former un ensemble cohérent à première vue.[51] C'est aussi la vision que certains de ses contemporains ont des publications de Cauchy dans les *Comptes rendus* de l'Académie. Ainsi, Jean-Baptiste Biot est très critique envers Cauchy sur ce sujet et observe dans le *Journal des savants* de novembre 1842:

> Un géomètre, assurément très habile, a profité de l'opportunité des comptes rendus pour publier, presque dans chaque numéro, une série de mémoires entiers, hérissés de symboles, sans connexion entre eux, reproduisant plusieurs fois les mêmes résultats ou les mêmes idées sous diverses formes, à mesure qu'elles se présentent à son esprit, brisés aussi de renvois qui se rapportent à une multitude de publications éparses; de sorte qu'aujourd'hui, s'ils se correspondent dans la pensée de l'auteur, comme je n'en fais aucun doute, il semblerait être à peu près le seul qui puisse en profiter, ou qui soit capable d'en suivre le fil (Biot 1842, pp. 659–660).

C'est effectivement la première impression qui ressort lors de la lecture de ces notes.

Leurs titres suggèrent deux thématiques principales. En effet, le titre des sept premières (du 14 octobre 1839 au 10 février 1840) contient l'expression «formes quadratiques», tandis que les titres des notes suivantes évoquent les résidus quadratiques et cubiques, ainsi que les expressions formées avec les racines primitives des équations binômes. Dans une première série d'interventions à l'Académie, Cauchy présente donc les points principaux de sa méthode sur les formes quadratiques, puis il développe certains résultats en lien avec les outils utilisés dans son travail sur les formes quadratiques.

5.1 Présentation de la méthode de Cauchy sur les formes quadratiques à l'Académie

Lors de la séance du 14 octobre 1839, Cauchy rappelle que Libri a récemment découvert des manuscrits de Fermat contenant des résultats sur certaines formes quadratiques, comme le théorème des deux carrés par exemple,[52] et se réfère à Gauss (Gauss

[49] Se reporter à (Crosland 1992) et (Brian 1996).

[50] Utilisation considérée comme abusive pour beaucoup: selon (Belhoste 1991, p 191), Cauchy présente environ 240 notes aux *Comptes rendus* entre 1838 et 1848.

[51] Parmi ces notes, les deux qui paraissent en 1839 contiennent l'expression "théorie des nombres" dans leur titre (aucun texte publié dans les *Comptes rendus* de l'Académie des sciences en 1839 n'est classé dans la catégorie "théorie des nombres"). Pour l'année 1840, nous avons pris en comptes les notes de la catégorie "théorie des nombres".

[52] Tout nombre premier de la forme $4n + 1$ peut se décomposer en deux carrés d'entiers.

1828) et Jacobi (Jacobi 1827) pour leurs recherches liées à la représentation d'un nombre premier par une expression de la forme $x^2 + ny^2$. Cauchy revient enfin sur ses propres travaux des années 1829-1830 dans lesquels il a développé des méthodes plus générales permettant la «recherche directe des formes quadratiques des nombres premiers», c'est-à-dire les formes quadratiques de la forme $p^m = x^2 + ny^2$ ou $4p^m = x^2 + ny^2$, où p est un nombre premier de la forme $nk + 1$ et où m peut être calculé à partir des nombres de Bernoulli. Cauchy demande finalement l'autorisation de rendre compte de ses recherches lors des prochaines séances de l'Académie.

Lors de sa seconde intervention sur les formes quadratiques, le 28 octobre 1839, Cauchy introduit les expressions Θ_h à partir de considérations sur les *fonctions principales* de Lagrange[53] et commente l'égalité $\Theta_h\Theta_{-h} = (-1)^h p$ (lorsque h n'est pas divisible par $p - 1$) qu'il énonce déjà dans (Cauchy 1829a):

> [...] le produit des deux valeurs obtenues
>
> $$\Theta_h, \quad \Theta_{-h}$$
>
> sera égal au nombre p pris avec le signe + ou avec le signe −, suivant que l'indice h sera pair ou impair, pourvu toutefois que h ne soit pas divisible par p.[...] Pour cette raison, nous désignerons les deux expressions imaginaires
>
> $$\Theta_h, \quad \Theta_{-h}$$
>
> sous le nom de *facteurs primitifs* de $\pm p$, et nous dirons que ces deux facteurs sont *conjugués* l'un de l'autre (Cauchy 1839b, p. 510).

La formule "facteur primitif" apparaît ici pour la première fois dans les travaux de Cauchy, et peut rappeler l'expression "facteur premier". Cauchy ne fait néanmoins aucune remarque sur l'existence d'une analogie de la sorte, et ne détaille pas les propriétés de ces facteurs primitifs. Il est cependant remarquable que Cauchy utilise à plusieurs reprises l'adjectif "primitif" pour définir des objets de l'algèbre et de la théorie des nombres. Il reprend bien sûr l'appellation *racine primitive* introduite par Euler. Dans son mémoire de 1846 sur *les arrangements donnés que l'on peut former avec des lettres données et sur les permutations ou substitutions à l'aide desquelles on passe d'un arrangement à un autre* (Cauchy 1846), il introduit également ce qu'il nomme les *substitutions primitives* et les *facteurs primitifs des substitutions*. Dans ce mémoire, Cauchy définit l'*ordre* d'une substitution comme l'exposant de la plus petite puissance de cette substitution équivalente à l'unité, c'est-à-dire à la substitution identité. Il démontre plus loin que si l'on considère une substitution P d'ordre i dont la décomposition en facteurs premiers est $i = p^f q^g r^h \ldots$, alors il existe des substitutions U, V, W, ..., dont les ordres respectifs sont p^f, q^g, r^h et telles que $P = U^\alpha V^\beta W^\gamma \ldots$, où $\alpha, \beta, \gamma, \ldots$, sont des nombres entiers déterminés à partir des

[53] Ces fonctions principales correspondent aux résolvantes de Lagrange déjà évoquées précédemment: ce sont des fonctions linéaires des différentes puissances d'une racine de n^e de l'unité utilisées par ce dernier. C'est la première fois que Cauchy se réfère aux travaux de Lagrange sur la théorie algébrique des équations dans le cadre de ses travaux de théorie des nombres.

facteurs premiers du nombre i. Cauchy met d'ailleurs en avant l'analogie existant entre les substitutions U, V, W, ..., les facteurs premiers du nombre i et les racines primitives des équations binômes:

> Cela posé, les substitutions
>
> $$U, V, W, \ldots$$
>
> joueront, par rapport à la substitution P de l'ordre i, un rôle analogue à celui des facteurs
>
> $$p^f, q^g, r^h, \ldots,$$
>
> dont chacun est une puissance d'un nombre premier, jouent aux-mêmes par rapport au nombre entier i. On peut remarquer aussi que les substitutions U, V, W, ...représentent des puissances de P desquelles on peut déduire toutes les autres [...] Elles offrent donc encore, pour cette raison, une certaine analogie avec certaines racines des équations binômes, savoir, avec celles qui sont désignées sous le nom de primitives, et qui, élevées à des puissances diverses, reproduisent toutes les autres racines. Pour conserver le souvenir de ces diverses analogues, nous dirons que les substitutions
>
> $$U, V, W, \ldots,$$
>
> [...] sont les *facteurs primitifs* de la substitution P.
> De plus, nous appellerons *substitution primitive* celle qui n'aura d'autres facteurs primitifs qu'elle-même, ou, en d'autres termes, celle dont l'ordre sera une puissance d'un nombre premier (Cauchy 1846, pp. 204–205).

Cauchy met donc en avant les analogies que l'on retrouve entre les racines primitives, les facteurs premiers d'un nombre entier et les substitutions primitives. Il est donc étonnant qu'il ne justifie pas plus en détails l'introduction de la notion de *facteurs primitifs* dans le cas présent.

Dans la suite de cette note, Cauchy s'arrête également sur le sens de l'égalité $\Theta_h\Theta_k = R_{h,k}\Theta_{h+k}$ et explique comment on peut obtenir des formes quadratiques de la forme voulue à partir des facteurs primitifs:

> Une propriété remarquable des facteurs primitifs de p, c'est que le produit de deux ou plusieurs facteurs de cette espèce est proportionnel à un semblable facteur. En d'autres termes, on a
>
> $$\Theta_h\Theta_k = R_{h,k}\Theta_{h+k}$$
>
> [...] à l'aide de cette proposition, jointe à celles que nous avons déjà rappelées, on transforme aisément certaines puissances du nombre p, ou le quadruple de ces puissances, en expressions de la forme
>
> $$x^2 + ny^2,$$

> n étant un diviseur de $p-1$. Il suffit, en effet, pour y parvenir, de multiplier l'un par l'autre, dans un certain ordre, les facteurs primitifs du nombre p[...] (Cauchy 1839b, pp. 512–513)

Cet extrait est fondamental pour la suite: en effet, nous verrons que toute sa méthode s'appuie sur ce principe: déterminer dans quel ordre multiplier entre elles des sommes de Gauss pour obtenir une expression de la forme $x^2 + ny^2$.

Les notes suivantes contiennent les principaux résultats permettant d'obtenir concrètement une égalité de la forme $4p^{\mu} = x^2+ny^2$, lorsque n est un nombre impair composé de facteurs premiers distincts, puis un nombre de la forme $4\nu\nu' \ldots$ ou $8\nu\nu' \ldots$. Il commence par exemple par démontrer: «Le quadruple de la puissance de p qui aura pour exposant, ou la différence obtenue, si n est de la forme $8x+7$, ou le tiers de cette différence dans le cas contraire, pourra toujours être converti en un binôme de la forme x^2+ny^2; et l'on pourra effectuer immédiatement cette conversion en multipliant l'un par l'autre, dans un certain ordre, les facteurs primitifs du nombre premier p» (Cauchy 1840e, p. 53).[54] Dans le cas où le nombre n est de la forme $4\nu\nu' \ldots$ ou $8\nu\nu' \ldots$, il adapte la définition de $(\frac{h}{n})$: dans le premier cas, il détermine combien de nombres h inférieurs à $\frac{1}{2}n$ sont tels que $(\frac{h}{\frac{1}{4}n}) = 1$ ou -1. Il expose plusieurs résultats déjà évoqués lors de notre analyse des notes du mémoire de 1840, comme par exemple des propriétés des fonctions symétriques et alternées des racines primitives des équations binômes, et développe plusieurs façons de réduire l'exposant de la puissance de p de la forme quadratique considérée. Remarquons qu'il ne justifie à aucun moment le lien entre les nombres de Bernoulli et l'exposant de la puissance de p. Il donne par contre plusieurs variantes dans l'exposition de sa méthode et introduit du vocabulaire et des commentaires inédits dans ses travaux des années 1829-1831. Ces variantes et ce vocabulaire sont par contre utilisés en partie dans les deux dernières notes du mémoire de 1840: cela laisse vraisemblablement transparaitre des efforts de la part de Cauchy pour rendre sa méthode plus abordable.

5.2 À côté des formes quadratiques: résidus et sommes de Gauss

Les notes suivantes sont consacrées à des développements sur les résidus quadratiques et cubiques, et à des démonstrations de nature différente sur les sommes de Gauss. Notons que sur ces quatre notes, deux sont reproduites dans le *Journal de Liouville* la même année, tandis que l'on ne trouve alors aucune trace du travail de Cauchy sur les formes quadratiques dans un périodique non académique.

La note du 16 mars 1840 se partage en deux paragraphes: un premier intitulé *Sur les résidus inférieurs à un module donné*, et un deuxième *Sur les résidus et les non-résidus quadratiques inférieurs à la moitié d'un module donné*. À partir de la formule annoncée lors de la séance du 3 février 1840 dans une note intitulée *Sur les fonctions alternées et sur diverses formules d'Analyse*

[54] La différence évoquée par Cauchy correspond à la différence de la quantité de nombres h inférieurs à $\frac{n}{2}$ tels que $(\frac{h}{n}) = 1$ ou -1 (avec $(\frac{h}{n}) = (\frac{h}{\nu})(\frac{h}{\nu'})\ldots$).

$$(1-x)(1-x^3)\cdots(1-x^{2m-1}) = 1 - \frac{1-x^{2m}}{1-x} + \frac{(1-x^{2m})(1-x^{2m-2})}{(1-x)(1-x^2)}\cdots + 1,$$

il obtient, en posant $2m = n-1$ et $x = \rho$ (où ρ est une racine primitive de l'équation $x^n = 1$), l'égalité évoquée déjà à plusieurs reprises: $\Delta^2 = (-1)^{\frac{n-1}{2}}$, où Δ est définie comme la somme[55] $\rho+\rho^4+\rho^9+\cdots+\rho^{(n-1)^2}$ avec ρ une racine primitive de $x^n = 1$. Cauchy s'appuie ensuite sur l'expression trigonométrique des racines primitives de $x^n = 1$ pour montrer que $\Delta = n^{\frac{1}{2}}(\sqrt{-1})^{\left(\frac{n-1}{2}\right)^2}$. Comme nous l'avons noté précédemment, la détermination de Δ a été l'objet de recherches pour plusieurs savants, dont Gauss (Gauss 1801, 1811), Dirichlet (Dirichlet 1838) et Cauchy. Comme il le signale au début de sa note, Cauchy s'appuie ici sur des arguments semblables à ceux utilisés dans la démonstration de (Gauss 1811).

Dans la suite de cette note, Cauchy démontre des résultats en lien avec les résidus et non-résidus quadratiques. Il détermine par exemple la valeur des sommes trigonométriques

$$\sum_{0\le h\le \frac{n}{2}} \cos h\omega - \sum_{0\le k\le \frac{n}{2}} \cos k\omega,$$

où h (respectivement k) appartient à l'ensemble des résidus (respectivement non-résidus) quadratiques et introduit des notations qu'il réutilise dans la note du 11 mai:

$$s_m = \sum_{0\le h\le \frac{n}{2}} h^m; \quad t_m = \sum_{0\le k\le \frac{n}{2}} k^m; \quad i = s_0; \quad j = t_0,$$

ainsi que des notations S_m et T_m similaires pour des résidus et non-résidus quadratiques inférieurs à n. Il obtient par exemple les valeurs de $T_1 - S_1$ et $T_2 - S_2$ en fonction de la valeur de n.

Cauchy conclut en rappelant que Dirichlet a également travaillé sur ce thème (Dirichlet 1838) et que Joseph Liouville lui a dit avoir obtenu des résultats similaires. Le fait que Cauchy présente ses recherches sur le nombre de résidus et non-résidus quadratiques est implicitement en lien avec ses travaux sur les formes quadratiques de la forme $4p^\mu = x^2 + ny^2$; il a en effet démontré dans de précédentes notes que l'exposant μ dépend de la différence qu'il note ici $i - j$.

Des réflexions sur ces différentes expressions sont reprises par Cauchy dans la note présentée à l'Académie le 11 mai 1840, sous le nom *Sur quelques séries dignes de remarque, qui se présentent dans la théorie des nombres*. Dans ces deux notes, Cauchy observe une fois de plus qu'il obtient des formules semblables à celles obtenues par Dirichlet et Liouville. En effet, ce dernier reprend une partie des travaux de Dirichlet pour les exposer dans ses leçons données au Collège de France pendant le premier semestre 1839–1840; certaines de ces leçons sont dédiées à la théorie des nombres, et

[55] Cela correspond bien à la définition habituelle: en effet, $(n-i)^2 \equiv i^2 \pmod n$ donc $1+\rho+\rho^4+\rho^9+\cdots+\rho^{(n-1)^2} = 1+2(\rho+\rho^{s^2}+\rho^{s^4}+\cdots+\rho^{s^{n-3}})$, où s est une racine primitive de n. Il suffit alors de soustraire à cette somme l'expression nulle $1+\rho+\rho^2+\cdots+\rho^{n-1}$.

il semble que Liouville ait communiqué avec Cauchy sur ces dernières.[56] Cela peut expliquer pourquoi Cauchy présente cet ensemble de résultats à l'Académie, qui n'est a priori pas inclus dans ses recherches sur les formes quadratiques.[57]

Dans les notes des 6 et 13 avril 1840, Cauchy ne revient pas sur son travail en lien avec les formes quadratiques mais démontre des résultats sur les sommes de Gauss. Dans la note du 6 avril, qui contient un extrait des notes X et XI du mémoire de 1840, Cauchy propose deux méthodes permettant d'obtenir la valeur de l'expression Δ. Il commence d'ailleurs par rappeler que cette question date de trente ans et qu'elle a également été l'objet de publications récentes.[58] La première méthode présentée par Cauchy s'appuie sur une formule démontrée par lui-même en 1817 à partir des fonctions réciproques:[59]

$$a^{\frac{1}{2}}\left(\frac{1}{2}+e^{-a^2}+e^{-4a^2}+\cdots\right)=b^{\frac{1}{2}}\left(\frac{1}{2}+e^{-b^2}+e^{-4b^2}+\cdots\right),$$

où a et b sont deux nombres positifs tels que $ab=\pi$.

Mais Cauchy insiste plus particulièrement sur le fait que sa deuxième méthode ne s'appuie pas sur la considération de calcul intégral:

> [...] et ce que les géomètres apprendront sans doute avec plaisir, c'est que, sans recourir ni au Calcul intégral, ni aux séries singulières dont M. Gauss a fait usage, on peut directement, et par une méthode fort simple, transformer en produit une somme alternée, en déterminant le signe qui doit affecter ce même produit. Cette méthode a d'ailleurs l'avantage d'être applicable à d'autres questions du même genre. Ainsi, en particulier, on reconnaîtra sans peine que, si, n étant un nombre premier, $n-1$ est divisible par 3, ou par 5, etc., un facteur primitif de n, correspondant au diviseur 3, sera proportionnel au produit de $\frac{n-1}{3}$ facteurs trinômes, tandis qu'un facteur primitif de n, correspondant au diviseur 5, sera proportionnel au produit de $\frac{n-1}{5}$ facteurs pentanômes ou composés chacun de cinq termes; et le rapport du produit en question au facteur primitif de n sera la somme de certaines racines de l'unité respectivement multipliées par des coefficients qui seront équivalents, suivant le module n, à des quantités connues (Cauchy 1840b, pp. 153–154).

[56] Il semble même, d'après une invitation de Cauchy à Dirichlet datée du 25 juillet 1839, que Cauchy ait convié Dirichlet à se joindre à Liouville et lui pour un dîner à Sceaux: voir (Belhoste 1984, p. 266).

[57] Liouville se plaint d'ailleurs dans une lettre à Dirichlet, datée de mai ou juin 1840, que Cauchy ait communiqué deux notes sur ces résultats en citant prioritairement Liouville, et non pas Dirichlet: voir (Belhoste 1984, pp. 266–267).

[58] Il cite notamment Dirichlet et Lebesgue.

[59] Cauchy aborde notamment ces fonctions dans le *Bulletin de la Société Philomathique* de 1817. Une fonction réciproque de première espace est de la forme $f(x)=\left(\frac{2}{\pi}\right)^{\frac{1}{2}}\int_0^\infty \varphi(u)\cos(\dot{ux})du$, où x est positif et est telle que $\varphi(u)=\left(\frac{2}{\pi}\right)^{\frac{1}{2}}\int_0^\infty f(v)\cos(uv)dv$. Les fonctions réciproques de seconde espèce sont semblables, mais dépendent de la fonction sinus.

Dans ce deuxième cas, Cauchy considère le produit

$$P = (\rho^1 - \rho^{-1})(\rho^3 - \rho^{-3}) \dots (\rho^{n-2} - \rho^{-(n-2)}),$$

lui-même égal au produit $(\rho^1 - \rho^{n-1})(\rho^2 - \rho^{n-2}) \dots \left(\rho^{\frac{n-1}{2}} - \rho^{\frac{n+1}{2}}\right)$ qui est une fonction alternée des racines primitives considérées.[60] P est donc de l'une des deux formes a ou $a\Delta$, le nombre a étant entier relatif. Cauchy montre alors que P, ne pouvant pas être de la forme a, est nécessairement de la forme $a\Delta$. Ici, Cauchy utilise donc les propriétés des fonctions symétriques et alternées des racines primitives de l'équation $x^n = 1$, abordées dans une des notes précédentes, et démontrées en détails dans le *Mémoire sur la théorie des nombres* de 1840. Il montre enfin que $P = \pm\Delta$, puis que $P = \Delta$.

Cauchy conclut en indiquant que sa méthode peut être appliquée dans d'autres cas; il donne quelques précisions concernant le cas cubique. Soit n un nombre premier de la forme $3x + 1$, α une racine primitive cubique de l'unité et m une racine primitive de $x^{n-1} \equiv 1 \pmod{n}$. Dans ce cas, le produit P est de la forme

$$P = \left(\rho + \alpha\rho^{m^{\frac{n-1}{3}}} + \alpha^2\rho^{m^{2\frac{n-1}{3}}}\right)\left(\rho^m + \alpha\rho^{m^{1+\frac{n-1}{3}}} + \alpha^2\rho^{m^{1+2\frac{n-1}{3}}}\right)\dots.$$

Ce produit est alors proportionnel au «facteur primitif de n» (Cauchy 1840b, p. 165), ce dernier étant $\Theta = \rho + \alpha\rho^m + \alpha^2\rho^{m^2} + \rho^{m^3} + \dots + \alpha^2\rho^{m^{n-2}}$, ce qui correspond à une somme cubique de Gauss. Puisque P et Θ sont proportionnels, Cauchy observe que le quotient $\frac{P}{\Theta}$ est de la forme $a + b\alpha$, où a et b sont des nombres entiers et peuvent être déterminés par les méthodes exposées précédemment. Ainsi, Cauchy ne le précise pas, mais P et α sont proportionnels dans $\mathbb{Z}[\alpha]$, où α est une racine cubique de l'unité. Dans la prochaine note, Cauchy développe des résultats similaires à ceux présentés lors de la séance précédente, mais relativement aux résidus cubiques d'un nombre premier p de la forme $3x + 1$. Il met d'ailleurs en avant la ressemblance des deux méthodes dans son introduction: «Or la détermination complète de cette somme est évidemment un problème analogue à celui dont j'ai donné deux solutions nouvelles dans la dernière séance. Seulement ce nouveau problème est d'un ordre plus élevé, attendu que les résidus quadratiques se trouvent ici remplacés par des résidus cubiques. Mais, quoique, en raison de cette circonstance, la difficulté semble s'accroître, toutefois je parviens à la surmonter en suivant une marche semblable à celle que j'ai adoptée dans mon dernier Mémoire» (Cauchy 1840c, pp. 166–167).

Dans la note du 13 avril 1840, Cauchy s'intéresse aux sommes cubiques de Gauss. Il commence par introduire les notations habituelles: p est un nombre premier impair, θ est une racine primitive de $x^p = 1$, t est une racine primitive de l'équivalence $x^{p-1} \equiv 1 \pmod{p}$. Les racines primitives de $x^p = 1$ peuvent donc s'écrire $\theta, \theta^2, \dots, \theta^{p-1}$ ou encore $\theta, \theta^t, \theta^{t^2}, \dots, \theta^{t^{p-2}}$. Il pose: $\mathcal{S} = \theta + \theta^t + \theta^{t^2} + \dots \theta^{t^{p-2}}$ et rappelle que $\mathcal{S} = -1$.

[60] Cauchy précise en effet que ce produit reste invariable ou change seulement de signe lorsque l'on remplace ρ par ρ^m, où m est premier à n.

Dans les travaux liés à la somme Δ et aux résidus quadratiques, Cauchy considérait d'une part les racines ρ^h, où h représentait les différents résidus quadratiques et d'autre part les racines ρ^k, où k représentait les différents résidus non-quadratiques. Il considère ici trois sommes[61] de puissances de θ. Dans la première, les exposants dont les résidus cubiques t^{3k}, dans la seconde, les exposants sont des non-résidus cubiques de la forme t^{3k+1}, et dans la dernière, les exposants sont des non-résidus cubiques de la forme t^{3k+2}:

$$\begin{cases} \mathcal{S}_0 = \theta + \theta^{t^3} + \theta^{t^6} + \cdots + \theta^{t^{p-4}}, \\ \mathcal{S}_1 = \theta^t + \theta^{t^4} + \theta^{t^7} + \cdots + \theta^{t^{p-3}}, \\ \mathcal{S}_0 = \theta^{t^2} + \theta^{t^5} + \theta^{t^8} + \cdots + \theta^{t^{p-2}}. \end{cases}$$

Chacune des sommes $\mathcal{S}_i$ est composée de couples de racines de la forme θ^l et θ^{-l}. Or les sommes de la forme $\theta^l + \theta^{-l}$ sont réelles donc les expressions $\mathcal{S}_i$ sont des quantités réelles. Cauchy se propose alors de déterminer les équations du troisième degré dont les sommes $\mathcal{S}_i$ sont solutions. Pour cela, Cauchy élève au carré la somme $\mathcal{S}_0$ et montre que $\mathcal{S}_0^2 = \frac{p-1}{3} + a\mathcal{S}_0 + b\mathcal{S}_1 + c\mathcal{S}_2$. Pour déterminer les coefficients a, b et c, Cauchy va utiliser une méthode similaire à celle utilisée dans la note précédente: il va remplacer dans les deux expressions données précédemment de $\mathcal{S}_0^2$ les termes θ^l par l^{ϖ}, où $\varpi = \frac{p-1}{3}$, et les considérer modulo p. Cette méthode est bien similaire à celle donnée dans le cas des résidus quadratiques puisque, d'après (Cauchy 1829a), on a en général: $(\frac{k}{p}) \equiv k^{\frac{p-1}{n}} \pmod{p}$. Il obtient ainsi un système de trois équivalences pour les coefficients a, b et c, ainsi qu'une équation dont les $\mathcal{S}_i$ sont les trois solutions:

$$\mathcal{S}^3 + \mathcal{S}^2 + \varpi\mathcal{S} + \frac{\varpi^2 - 3\varpi - 1 - ap}{3} = 0.$$

À partir de cela, Cauchy retrouve notamment que l'équation $4p = A^2 + 27B^2$ est vérifiée pour $A \equiv -\Pi$, $B \equiv \frac{r^2-r}{9}\Pi \pmod{p}$, où $\Pi = \dfrac{(\varpi+1)(\varpi+2)\ldots(2\varpi)}{1.2.3\ldots.\varpi}$, et rappelle que ce résultat est déjà donné dans (Jacobi 1827).

La deuxième partie de ce mémoire, très courte, contient quelques réflexions sur les résultats obtenus précédemment. Cauchy conclut finalement:

> Au reste, les formules obtenues dans le premier paragraphe peuvent encore être déduites, comme je le montrerai dans un autre article, de la considération des facteurs primitifs du nombre premier p; et l'on peut, à l'aide des mêmes méthodes, établir des formules analogues, qui soient relatives, non plus aux résidus cubiques, mais aux résidus des puissances supérieures à la troisième (Cauchy 1840c, p. 180).

[61] Ces sommes correspondent aux périodes considérées par Gauss dans l'article 358 des *Disquisitiones Arithmeticae*, article dans lequel il démontre également que le quadruple d'un nombre premier de la forme $3k + 1$ peut être mis sous la forme $x^2 + 27y^2$.

Cauchy n'a pas publié cet article; cette conclusion confirme néanmoins que Cauchy veut obtenir des résultats sur les sommes de Gauss en utilisant sa notion de facteurs primitifs et en évitant l'utilisation de l'analyse.

5.3 L'apport des notes aux *Comptes rendus* pour la compréhension des recherches arithmétiques de Cauchy

Dans cette série de notes, Cauchy semble avoir deux objectifs: présenter sa méthode générale pour obtenir des formes quadratiques de la forme $4p^{\mu} = x^2 + ny^2$, où n est un diviseur de $p - 1$, et travailler sur certaines sommes de Gauss. Tout ce qu'expose Cauchy sur les formes quadratiques est également dans le mémoire de 1840. Mais, par rapport à ses écrits précédents, Cauchy propose au lecteur des remarques très éclairantes sur sa méthode. Cauchy donne du sens aux expressions Θ_h en les nommant «facteurs primitifs» et met en avant le principe fondamental de sa méthode: multiplier dans un certain ordre ces facteurs primitifs pour obtenir une égalité de la forme $4p^{\mu} = x^2 + ny^2$. Néanmoins, les raisonnements exposés ici sont la plupart du temps incomplets, et Cauchy ne propose souvent que des pistes de recherche. Par exemple, il rappelle que l'exposant μ peut être exprimé en fonction des nombres de Bernoulli mais n'aborde à aucun moment la justification de ce lien dans les *Comptes rendus*. On voit donc que l'étude de ces notes permet d'avoir un aperçu de la méthode de Cauchy, mais c'est dans son mémoire qu'il donne les détails nécessaires à la compréhension fine des démonstrations, des différents cas étudiés et exemples obtenus. Pour le lecteur, ces notes constituent ce que l'on pourrait qualifier de fil directeur: elles permettent de concevoir plus facilement les grandes lignes du travail de Cauchy et l'examen du mémoire devient plus facile, les longues séries de formules moins obscures.

Cauchy nous donne également à voir sa volonté d'obtenir des preuves d'un même résultat à partir d'outils de nature différente. Ainsi, comme nous venons de l'observer, il propose plusieurs démonstrations pour obtenir la valeur de Δ et donne de la valeur à celle qui ne s'appuie pas sur des arguments d'analyse. Il insiste d'ailleurs à plusieurs reprises sur l'utilisation des facteurs primitifs et semble avoir la volonté de fonder d'autres démonstrations sur ces expressions. Mais, après la note du 11 mai 1840, il faudra attendre l'année 1847 pour une nouvelle publication où Cauchy utilise les sommes de Gauss.

Enfin, lorsque l'on relève les différents noms de savants cités par Cauchy dans ses publications, on observe deux situations. Dans les travaux sur les formes quadratiques, Cauchy cite principalement les travaux de deux auteurs: Gauss et Jacobi.[62] Par contre, dans les quatre dernières notes aux *Comptes rendus*, Cauchy évoque toujours les travaux de Gauss et Jacobi, mais aussi ceux de Dirichlet, Liouville et Lebesgue. Ces trois derniers hommes publient effectivement des travaux sur la détermination de certaines sommes de Gauss à la même époque; ce sont d'ailleurs ces notes de Cauchy précisément qui sont reproduites dans le *Journal de Liouville*.

[62] Certains autres noms, comme Poinsot, Lagrange et Legendre ne sont évoqués que pour signaler une paternité de définition ou de notation.

6 Le *Mémoire sur la théorie des nombres* (2): pour une méthode générale sur les formes quadratiques

Après cette analyse détaillée, nous voici prêts pour donner une vision d'ensemble des principales étapes de la méthode de Cauchy. Nous pourrons alors déterminer comment s'articulent les différents thèmes abordés dans son travail sur les formes quadratiques.

La méthode est donc basée sur l'utilisation d'expressions dépendant de racines primitives de l'unité: les sommes $\Theta_h = \theta + \rho^h\theta^t + \rho^{2h}\theta^{t^2} + \cdots + \rho^{(p-2)h}\theta^{t^{p-2}}$, où θ est une racine primitive de $x^p = 1$, ρ une racine primitive de $x^n = 1$ et t une racine primitive du nombre premier p. On peut ainsi définir les expressions $R_{h,k}$ à partir de l'égalité $\Theta_h\Theta_k = R_{h,k}\Theta_{h+k}$ et démontrer que ce sont des fonctions entières de ρ. D'une part, Cauchy étudie les propriétés de ces expressions, et plus généralement, les formes des fonctions symétriques et alternées dépendant de racines primitives de l'unité. Il prouve par exemple que toute fonction symétrique des racines n^e de l'unité $\rho, \rho^2, \ldots, \rho^{n-1}$ (n nombre premier) est de la forme $a_0 + a_1(\rho + \rho^2 + \cdots + \rho^{n-1})$. D'autre part, il démontre des formules fondamentales qui lui permettent d'obtenir des égalités de la forme $4p^\mu = x^2 + ny^2$, où p est un nombre premier et n un diviseur de $p - 1$. Parmi celles-ci, on retrouve notamment:

- $\Theta_h\Theta_k = R_{h,k}\Theta_{h+k}$;
- $\Theta_h\Theta_{-h} = (-1)^{h\varpi}p$;
- $(\rho - \rho^s + \rho^{s^2} - \rho^{s^3} + \cdots - \rho^{s^{n-2}})^2 = (-1)^{\frac{n-1}{2}}n$, où s est une racine primitive de n.

Il expose sa méthode sur les formes quadratiques en deux temps: il suppose d'abord que le nombre n est premier dans le premier paragraphe,[63] puis consacre le reste de la partie principale de son mémoire au cas où le nombre n est composé, et tout particulièrement de la forme $n = \omega\nu$, ν premier. Dans ces deux cas, les principes généraux de sa méthode restent les mêmes: il considère des produits d'expressions Θ_h qu'il note $\mathcal{F}$ afin d'obtenir d'une part une puissance de p et d'autre part une somme de carrés $x^2 + ny^2$.

6.1 Lorsque n est un nombre premier

Lorsque n est un nombre premier, il pose $\mathcal{F}(\rho) = \Theta_1\Theta_{s^2}\Theta_{s^4}\ldots\Theta_{s^{n-3}}$.

Comme $\Theta_h\Theta_{-h} = (-1)^{h\varpi}p$, $\mathcal{F}(\rho)$ est une puissance de p. De plus, cette fonction entière est symétrique par rapport aux racines $\rho, \rho^{s^2}, \ldots, \rho^{s^{n-3}}$ d'une part et par rapport aux racines $\rho^s, \rho^{s^3}, \ldots, \rho^{s^{n-2}}$ d'autre part. À partir des propriétés étudiées sur la multiplication des Θ_h et sur les fonctions symétriques et alternées des racines primitives de $x^n = 1$, on sait qu'elle est de la forme

$$\mathcal{F}(\rho) = c_0 + c_1(\rho + \rho^{s^2} + \cdots + \rho^{s^{n-3}}) + c_2(\rho^s + \rho^{s^3} + \cdots + \rho^{s^{n-2}}).$$

[63] Cela correspond en partie à l'extrait que nous avons reproduit dans l'Annexe C.

Cauchy prouve ensuite qu'elle peut être mise sous la forme $2\mathscr{F}(\rho) = A + B(\rho - \rho^s + \rho^{s^2} - \rho^{s^3} + \cdots - \rho^{s^{n-2}}) = A + B\Delta$, où A et B sont des nombres entiers. Donc $2\mathscr{F}(\rho^s) = A - B(\rho - \rho^s + \rho^{s^2} - \rho^{s^3} + \cdots - \rho^{s^{n-2}}) = A - B\Delta$. Par conséquent, et en utilisant l'égalité $\Delta = (-1)^{\frac{n-1}{2}}$, le produit $4\mathscr{F}(\rho)\mathscr{F}(\rho^s)$ est de la forme $A^2 - (-1)^{\frac{n-1}{2}} nB^2$.

Ainsi, lorsque n est de la forme $4k+3$, Cauchy obtient l'égalité de la forme $4p^{\frac{n-1}{2}} = A^2 + nB^2$. Il termine l'étude de ce cas en expliquant comment réduire au maximum l'exposant de la puissance de p et démontre que l'exposant ainsi réduit dépend d'une part de la différence entre le nombre de résidus et non-résidus quadratiques de n inférieurs à $\frac{n}{2}$ et d'autre part du nombre de Bernoulli $\mathscr{A}_{\frac{n+1}{4}}$.

6.2 Lorsque n est un nombre composé

Arrêtons-nous sur le cas où $n = \omega\nu$, où ν est premier et ν et ω sont premiers entre eux. Il introduit alors de nouvelles notations : ς et α sont des racines primitives respectives des équations $x^\nu = 1$ et $x^\omega = 1$ et s et u sont des racines primitives respectives des congruences $x^\nu \equiv 1 \pmod{p}$ et $x^{\nu-1} \equiv 1 \pmod{\nu}$. Par rapport au premier paragraphe, s joue le rôle de r, qui était une racine primitive de $x^n \equiv 1 \pmod{p}$, et u joue le rôle de t, qui était une racine primitive de $x^{n-1} \equiv 1 \pmod{n}$. L'expression Θ_h peut donc s'écrire:

$$\Theta_h = \theta + \alpha^h \varsigma^h \theta^t + \alpha^{2h} \varsigma^{2h} \theta^{t^2} + \cdots + \alpha^{(p-2)h} \varsigma^{(p-2)h} \theta^{t^{p-2}}$$

et, même si les expressions et calculs en jeu sont plus longs, il construit comme précédemment une fonction entière produit de ces expressions, et ayant des propriétés de symétrie par rapport aux différentes racines primitives en jeu. Il obtient ainsi de nouveaux cas d'égalités de la forme $4p^\mu = x^2 + ny^2$, où n est un diviseur de $p-1$.

Comme ν et ω sont premiers entre eux, Cauchy pose $\upsilon = \frac{1}{\nu} \pmod{\omega}$, remarque que

$$1 + u^2 + \cdots + u^{\nu-3} + \upsilon\nu\left[\frac{\nu-1}{3} - (u^2 + \cdots + u^{\nu-3})\right] \equiv \upsilon\nu\frac{\nu-1}{2} \pmod{\nu}$$

et considère l'égalité

$$\Theta_1 \Theta_{u^2 + \upsilon\nu(1-u^2)} \cdots \Theta_{u^{\nu-3} + \upsilon\nu(1-u^{\nu-3})} = \mathscr{F}(\alpha, \varsigma)\Theta_{\upsilon\nu\frac{\nu-1}{2}}.$$

Dans la première partie du mémoire, on avait $\mathscr{F}(\rho) = \Theta_1 \Theta_{s^2} \Theta_{s^4} \ldots \Theta_{s^{n-3}}$. On observe donc que $\mathscr{F}(\alpha, \varsigma)$ correspond au produit $\mathscr{F}(\rho)$, en remplaçant s^{2k} par $u^{2k} + \upsilon\nu(1 - u^{2k})$. Comme précédemment, on a: $\mathscr{F}(\alpha, \varsigma) = \mathscr{F}(\alpha, \varsigma^{u^2}) = \mathscr{F}(\alpha, \varsigma^{u^4}) = \cdots = \mathscr{F}(\alpha, \varsigma^{u^{\nu-3}})$.

Cauchy donne ensuite deux autres produits possibles des Θ_h, qui permettent d'obtenir des égalités du même type. D'une part, si h est impair,

$$\Theta_{1+\upsilon\nu(h-1)} \Theta_{u^2 + \upsilon\nu(h-u^2)} \cdots \Theta_{u^{\nu-3} + \upsilon\nu(h-u^{\nu-3})} = \mathscr{F}(\alpha^h, \varsigma)\Theta_{\upsilon\nu\frac{\nu-1}{2}h}$$

et

$$\mathscr{F}(\alpha^h, \varsigma) = \mathscr{F}(\alpha^h, \varsigma^{u^2}) = \mathscr{F}(\alpha^h, \varsigma^{u^4}) = \cdots = \mathscr{F}(\alpha^h, \varsigma^{u^{\nu-3}}).$$

D'autre part, toujours en supposant h impair:

$$\Theta_{-1-\upsilon\nu(h-1)}\Theta_{-u^2-\upsilon\nu(h-u^2)}\cdots\Theta_{-u^{\nu-3}-\upsilon\nu(h-u^{\nu-3})} = \mathscr{F}(\alpha^{-h}, \varsigma^{-1})\Theta_{-\upsilon\nu\frac{\nu-1}{2}h}$$

et

$$\mathscr{F}(\alpha^{-h}, \varsigma^{-1}) = \mathscr{F}(\alpha^{-h}, \varsigma^{-u^2}) = \mathscr{F}(\alpha^{-h}, \varsigma^{-u^4}) = \cdots = \mathscr{F}(\alpha^{-h}, \varsigma^{-u^{\nu-3}}).$$

Finalement, on obtient:

$$\mathscr{F}(\alpha^h, \varsigma)\mathscr{F}(\alpha^{-h}\varsigma^{-1}) = \frac{\theta_{1+\upsilon\nu(h-1)}\theta_{-1-\upsilon\nu(h-1)}\cdots\Theta_{u^{\nu-3}+\upsilon\nu(h-u^{\nu-3})}\Theta_{-u^{\nu-3}-\upsilon\nu(h-u^{\nu-3})}}{\Theta_{\upsilon\nu\frac{\nu-1}{2}h}\Theta_{-\upsilon\nu\frac{\nu-1}{2}h}}.$$

En utilisant la propriété $\Theta_h\Theta_{-h} = (-1)^{\varpi h}p$, Cauchy déduit finalement que[64] $\mathscr{F}(\alpha^h, \varsigma)\mathscr{F}(\alpha^{-h}, \varsigma^{-1})$ est égal à $\pm p^{\frac{n-1}{2}}$ ou $\pm p^{\frac{n-1}{3}}$. Cauchy utilise donc toujours la même méthode pour obtenir les formes quadratiques voulues: il cherche à déterminer un produit composé de deux facteurs de la forme $\mathscr{F}(\alpha^a, \varsigma^b)$ tel qu'il soit égal à une puissance de p.

Rappelons que nous nous appuyons ici sur la partie principale du mémoire, qui a été présentée par Cauchy devant l'Académie en 1830. Comme nous l'avons vu précédemment, Cauchy introduit dans la note III la notation $\Theta_{i,j}$ qui lui permet ensuite de définir les notations [1, 1], [1, −1], ...De plus, plutôt que de travailler avec des expressions de la forme $\Theta_{u^2+\upsilon\nu(1-u^2)}$, Cauchy introduit les expressions notées $\Theta_{1,1}$, Θ_{1,u^2}, ...et les produits $\Theta_{1,1}\Theta_{u^2,1}\ldots\Theta_{u^{\nu-3},1}$ ce qui rappelle directement les produits considérés dans le cas où n est un nombre premier. On voit donc qu'en 1840, Cauchy propose une présentation simplifiée de son travail, en adoptant des notations qui permettent de passer plus facilement d'un cas à un autre.

Comme il le fait régulièrement dans la suite de ce mémoire, Cauchy étudie des cas particuliers «pour fixer les idées» (Cauchy 1840a, p. 23). Pour finir, nous nous arrêtons sur un de ces exemples: $\omega = 4$ et ν est impair, de la forme $4x + 1$. On peut donc poser $\upsilon = 1$: dans ce cas $\upsilon\nu = 4x + 1 \equiv 1 \pmod{\omega}$, ce qui correspond à la définition de υ. Cauchy suppose également que h et $\frac{\nu-1}{4}$ sont impairs (ν est donc de la forme $8x + 3$) et détermine la valeur des différents produits de la forme $\Theta_k\Theta_{-k}$ pour aboutir à l'égalité $\mathscr{F}(\alpha^h, \varsigma)\mathscr{F}(\alpha^{-h}, \varsigma^{-1}) = p^{\frac{\nu-3}{2}}$.

Cauchy développe ensuite le cas particulier où $h = 1$: $\mathscr{F}(\alpha, \varsigma)\mathscr{F}(\alpha, \varsigma^{-1}) = p^{\frac{\nu-3}{2}}$.

[64] Le numérateur est composé de $\frac{\nu-1}{2}$ facteurs de la forme $\Theta_h\Theta_{-h}$ donc le numérateur est égal à $\pm p^{\frac{n-1}{2}}$. D'autre part, le dénominateur est égal à $(-1)^{\varpi\upsilon\nu\frac{\nu-1}{2}h}p = \pm p$ lorsque $\varpi\upsilon\nu\frac{\nu-1}{2}h$ ne divise pas $p - 1$ et est égal à 1 lorsque $\varpi\upsilon\nu\frac{\nu-1}{2}h$ divise $p - 1$. Cela dépend donc de la valeur de υ.

Comme α est ici une racine primitive de $x^4 = 1$, Cauchy pose $\alpha = \sqrt{-1}$, et développe le cas particulier où $\omega = 4$, $\nu = 5$, soit $n = 20$. Il considère les expressions

$$2\mathscr{F}(\alpha, \varsigma) = \lambda' + \mu'\sqrt{-1} + (\lambda'' + \mu''\sqrt{-1})(\varsigma - \varsigma^2 - \varsigma^3 + \varsigma^4),$$
$$2\mathscr{F}(\alpha, \varsigma^3) = \lambda' + \mu'\sqrt{-1} - (\lambda'' + \mu''\sqrt{-1})(\varsigma - \varsigma^2 - \varsigma^3 + \varsigma^4),$$
$$2\mathscr{F}(\alpha^{-1}, \varsigma) = \lambda' - \mu'\sqrt{-1} + (\lambda'' - \mu''\sqrt{-1})(\varsigma - \varsigma^2 - \varsigma^3 + \varsigma^4),$$
$$2\mathscr{F}(\alpha^{-1}, \varsigma^3) = \lambda' - \mu'\sqrt{-1} - (\lambda'' - \mu''\sqrt{-1})(\varsigma - \varsigma^2 - \varsigma^3 + \varsigma^4).$$

Il ne justifie pas ces égalités. Néanmoins, la première est semblable à celle utilisée dans le cas où n est un nombre premier: en effet, Cauchy a démontré que les propriétés de $\mathscr{F}(\rho)$ impliquent que cette expression est de la forme $a + b(\rho - \rho^s + \rho^{s^2} - \rho^{s^3} + \cdots - \rho^{s^{n-2}})$, où a et b sont des nombres entiers. Or, ici, Cauchy pose également $\mathscr{F}(\alpha, \varsigma) = \lambda' + \mu'\sqrt{-1} + (\lambda'' + \mu''\sqrt{-1})(\varsigma - \varsigma^2 + \varsigma^4 - \varsigma^3)$, où la somme alternée considérée correspond bien aux sommes considérées précédemment. Cauchy utilise donc toujours une expression de la forme $a + b(\rho - \rho^s + \rho^{s^2} - \rho^{s^3} + \cdots - \rho^{s^{n-2}})$, mais ici, les nombres a et b sont des nombres de l'anneau $\mathbb{Z}[i]$. Cauchy ne commente absolument pas le fait qu'il utilise dans ce cas des coefficients qui sont des nombres entiers complexes: il semble simplement transposer ses raisonnements précédents.

Les trois égalités suivantes s'obtiennent facilement: en effet, $\alpha^{-1} = -\sqrt{-1}$ et en remplaçant ς par ς^3 dans la somme alternée $\varsigma - \varsigma^2 - \varsigma^3 + \varsigma^4$, on obtient l'opposé $-(\varsigma - \varsigma^2 - \varsigma^3 + \varsigma^4)$.

Finalement, on a: $4p = \lambda'^2 + \mu'^2 + 5(\lambda''^2 + \mu''^2)$ et $\lambda'\lambda'' = -\mu'\mu''$, et Cauchy explique comment obtenir les valeurs de λ', λ'', μ' et μ'' en utilisant une correspondance équation - équivalence à l'aide de la correspondance $R_{h,k} \equiv -\Pi - h, -k \pmod{p}$.

À l'aide de cette méthode, Cauchy démontre notamment que tout nombre premier de la forme $20x + 1$ est tel que l'équation $p = x^2 + 5y^2$ est résoluble en nombres entiers. De nombreux autres exemples ponctuent la démonstration de sa méthode en fonction des formes des diviseurs du nombre n.

Notons pour finir que dans ce cas également, Cauchy propose de déterminer en général l'exposant μ minimum de la puissance de p. Il ne démontre rien à ce sujet dans la partie principale mais il revient sur cette question dans la note II. Il démontre notamment le théorème général suivant:

> ν et p étant deux nombres premiers, l'un de la forme $4x + 1$ et l'autre de la forme $4\nu x + 1$, supposons que la suite des nombres $1, 5, 9, \ldots, 2\nu - 9, 2\nu - 5, 2\nu - 1$ offre ν' racines de l'équivalence $x^{\frac{\nu-1}{2}} \equiv 1 \pmod{\nu}$ et ν'' racines de l'équivalence $x^{\frac{\nu-1}{2}} \equiv -1 \pmod{\nu}$, on aura $\nu' + \nu'' = \frac{\nu-1}{2}$ et, si l'on nomme μ la valeur numérique de $\frac{\nu'-\nu''}{2}$, on pourra satisfaire, par des nombres x, y entiers et premiers entre eux, à l'équation $x^2 + \nu y^2 = p^\mu$, non seulement lorsque ν sera de la forme $8x + 5$, [...] (Cauchy 1840a, p. 107).

Il démontre ce théorème de la même façon que dans le cas où n est un nombre premier: il considère la différence $\nu' - \nu''$ comme équivalente à une somme de puissances

dont l'exposant est $\frac{\nu-1}{2}$, et traduit cette équivalence à l'aide d'une différenciation d'ordre $\frac{\nu-1}{2}$.

7 Conclusion

Entre 1829 et 1840, Cauchy use de plusieurs stratégies de communication pour faire connaître ses activités en théorie des nombres, comme la plupart de ses contemporains. Entre le *Bulletin de Férussac* qui lui permet de publier rapidement les premiers résultats qu'il obtient, les *Comptes rendus* de l'Académie des sciences qu'il utilise abondamment et son imposant mémoire de 1840, Cauchy présente ses recherches arithmétiques sous des formes très variées. Comme nous l'avons montré ici, c'est grâce à l'étude méthodique de l'ensemble de ses textes, sans *a priori* sur les thématiques abordées, qui nous avons réussi à comprendre l'objectif principal de Cauchy: développer une méthode générale pour obtenir des formes quadratiques $4p^{\mu} = x^2 + ny^2$ à partir de l'utilisation des sommes de Gauss. Nous avons également vu que dans ses dernières publications, Cauchy introduit de nouvelles notations et des ajouts par rapport à son mémoire initial de 1830, qui montrent l'évolution de son travail, tant sur le fond que sur la forme. Cette analyse ne nous a pas seulement permis de faire sens des écrits en question; nous avons également pu mettre à jour certaines caractéristiques du travail de Cauchy en théorie des nombres.

Nous avons ainsi montré que les recherches de Cauchy se situent dans la continuité de la section VII des *Disquisitiones Arithmeticae*: la place centrale des sommes de Gauss et l'utilisation intensive des propriétés des racines primitives en témoignent. Cauchy se sert également très régulièrement d'une correspondance entre équation et équivalence, en substituant à une racine d'une équation une racine de l'équivalence associée par exemple: cette pratique est alors utilisée sous différentes formes en théorie des nombres, par exemple par Jacobi dans ses travaux sur le même thème. Cependant, Cauchy semble à plusieurs reprises manipuler des égalités ou des équivalences sans interroger explicitement la validité des opérations en cours. Nous avons notamment évoqué le fait de considérer une équivalence mettant en jeu des nombres de Bernoulli, qui sont des nombres rationnels non entiers, sans justifier leur existence suivant le module considéré. D'autre part, des entiers complexes interviennent dans certains des raisonnements de Cauchy, nombres qui ont été l'objet de recherches approfondies particulièrement chez Gauss (Gauss 1828, 1832) et Dirichlet (Dirichlet 1832) ; ces derniers ont effectivement consacré des mémoires à démontrer que certaines propriétés des nombres entiers sont bien valables pour cet ensemble d'entiers complexes. Or, de son côté, Cauchy ne fait aucun commentaire à ce sujet. Cela est d'autant plus étonnant qu'il est célèbre pour ses nombreuses réflexions sur les nombres imaginaires dans ses travaux d'analyse par exemple (Dahan Dalmedico 1997; Flament 2003). Ces non-dits suggèrent que Cauchy transpose directement des manipulations algébriques des nombres entiers aux entiers complexes, ou encore d'égalités à des congruences sans questionner explicitement la validité de ces transferts.

Nous avons également observé chez Cauchy des liens entre certains de ses travaux de théorie des nombres, d'algèbre et d'analyse. Ainsi, l'utilisation des fonctions

symétriques et alternées traversent plusieurs de ses thématiques de recherches, en algèbre, dans son cours d'analyse algébrique et en théorie des nombres. Il souligne d'ailleurs leur importance. Il introduit également du vocabulaire similaire pour décrire des objets contenus dans plusieurs de ses travaux: les facteurs primitifs des substitutions et des nombres premiers. Nous avons également insisté sur l'introduction par Cauchy des nombres de Bernoulli en théorie des nombres. Leur utilisation s'accompagne également de l'intervention d'outils de l'analyse. En effet, afin de montrer le lien entre les nombres de Bernoulli et le nombre de résidus et non-résidus quadratiques, Cauchy traduit une égalité en nombres entiers en une égalité entre des fonctions trigonométriques. Il utilise alors des différenciations pour faire apparaître la fonction tangente et introduire ainsi les nombres de Bernoulli à l'aide du développement en série de cette fonction. Cauchy emploie également dans d'autres mémoires de théorie des nombres des outils de l'analyse, comme le calcul intégral et les fonctions réciproques qu'il a étudiées dès 1817, afin de déterminer la valeur de la somme quadratique de Gauss notée Δ. Dans d'autres mémoires, Cauchy obtient également une détermination de Δ basée sur des considérations arithmétiques et insiste sur l'importance de ce type de démonstration. Cauchy utilise donc l'analyse dans certains de ses textes de théorie des nombres, mais semble également prôner une théorie des nombres fondée sur des preuves arithmétiques. Plusieurs de ses commentaires indiquent d'ailleurs que Cauchy projette de continuer ses recherches de théorie des nombres, en les fondant sur ce qu'il appelle les facteurs primitifs. Cette oscillation entre une volonté de lier les différentes branches des mathématiques et le souhait d'obtenir des preuves arithmétiques pour les résultats de théorie des nombres se retrouve d'ailleurs régulièrement dans d'autres publications de la première moitié du XIX^{e} siècle.[65]

Mais les travaux arithmétiques de Cauchy ont-ils d'autres points communs avec les recherches de ses contemporains ? Nous avons vu que Cauchy développe une méthode générale pour certaines formes quadratiques, mais sans lien avec la théorie des formes développée par Gauss dans la section V des *Disquisitiones Arithmeticae* et approfondie par Dirichlet. Cauchy place comme Jacobi les sommes de Gauss au cœur de ses raisonnements, mais n'obtient pas de résultats sur les résidus et lois de réciprocité comme son homologue allemand. Il est le seul à consacrer une grande partie de ses recherches arithmétiques aux égalités de la forme $4p^{\mu} = x^2 + ny^2$ et ses résultats sur les formes quadratiques ne sont pas repris dans les publications des années 1830 ou 1840. Nous venons également d'évoquer l'absence de tout commentaire de la part de Cauchy sur l'utilisation de certains nombres complexes en théorie des nombres, tandis que Gauss, Jacobi ou encore Dirichlet consacrent une partie de leurs recherches à démontrer la validité de certaines propriétés des nombres entiers pour les nombres entiers complexes. Cela laisse à penser un certain isolement des travaux arithmétiques de Cauchy.

[65] Par exemple, Libri souhaite étudier la théorie des congruences à partir des fonctions circulaires tandis que Lebesgue obtient des résultats similaires à ceux de Libri en ne se fondant que sur des arguments arithmétiques et combinatoires. Nous pouvons également penser à Gauss, qui propose six démonstrations différentes de la loi de réciprocité quadratique entre 1801 et 1818, démonstrations utilisant des arguments arithmétiques divers ou faisant intervenir des outils analytiques, comme les séries par exemple. Voir également à ce sujet (Goldstein et Schappacher 2007).

Pourtant, à côté de sa méthode générale sur les formes quadratiques, Cauchy publie dans les *Comptes rendus* de l'Académie plusieurs démonstrations de la valeur de Δ. Il répond ainsi en partie à des articles de Dirichlet et Liouville, en proposant de nouvelles méthodes pour résoudre une question déjà évoquée par Gauss en 1801. Cauchy cite aussi très régulièrement les travaux de Jacobi: ce dernier place également les propriétés des sommes de Gauss au centre de ses investigations et obtient des résultats sur les résidus et la loi de réciprocité cubique. Mais il évoque également l'utilisation de ces expressions pour obtenir des résultats sur les formes quadratiques: il ne publie pas en détails ces derniers résultats, mais les présente à ses étudiants dans les leçons qu'il donne à Königsberg en 1836–1837(Jacobi 2007). Ses arguments sont d'ailleurs en partie assez proches de ceux de Cauchy. D'autre part, à partir de perspectives différentes, Cauchy et Dirichlet obtiennent des formules semblables liant les sommes et les quantités de résidus et non-résidus quadratiques. Le second relie les résultats obtenus avec le nombre de classes de formes quadratiques tandis que le premier fait intervenir les nombres de Bernoulli...qui réapparaîtront quelques années plus tard dans les travaux de Kummer.[66]

Il existe donc des points communs entre les recherches de Cauchy et celles de Jacobi, Dirichlet et Kummer par exemple, mais ces points communs ne concernent pas les thèmes arithmétiques abordés. On retrouve des liens entre ces différents savants à travers les outils utilisés et certains résultats obtenus, mais souvent dans des perspectives différentes.

Revenons pour finir sur une des affirmations de Franz Lemmermeyer citées dans notre introduction: «Cauchy also studied these sums, but his lack of understanding higher reciprocity kept him from going as far as Jacobi did » (Lemmermeyer 2009, p. 171). Notre analyse confirme que Cauchy a effectivement travaillé sur les sommes de Gauss. Il a démontré des propriétés que l'on trouve aussi dans les travaux de Jacobi, mais n'obtient pas d'avancées sur les lois de réciprocité cubiques et biquadratiques. Cauchy démontre également des formules proches de celles que donne Dirichlet dans le cadre de son travail sur le nombre de classes de certaines formes quadratiques. Une lecture des textes de Cauchy focalisée sur la recherche de progrès dans les lois de réciprocité peut donc aboutir à la conclusion que Cauchy obtient ponctuellement des résultats similaires à Jacobi et Dirichlet sans aller aussi loin qu'eux. Mais l'objectif de Cauchy n'est visiblement pas d'étudier les résidus d'ordre supérieur et les lois de réciprocité; il ne semble pas non plus s'intéresser aux formes quadratiques dans le même sens que Dirichlet. Son but est d'obtenir une «foule d'équations indéterminées» de la forme $p^{\mu} = x^2 + ny^2$ à l'aide d'une méthode générale qu'il expose complètement dans son mémoire de 1840, et basée sur les propriétés particulières des sommes de Gauss. Comme nous l'avons signalé au début de notre article, les *Disquisitiones Arithmeticae* ont un rôle fondamental dans les recherches de théorie des nombres de la première moitié du XIX^{e} siècle au moins. Et notre étude montre une fois de plus que l'ouvrage de Gauss a été le point de départ de nombreux travaux, dans des perspectives très variées. Dans le cas des travaux de Cauchy étudiés ici, c'est la section sur la cyclotomie et les deux exemples présentés par Gauss qui en sont à

[66] Pour les liens entre les travaux de Cauchy, Jacobi, Dirichlet et Kummer, voir Boucard (2011b, Chap. 12).

l'origine. Lire les publications de Cauchy dans cette perspective permet de leur rendre toute leur cohérence.

Annexe A: Reconstruction de la méthode de Cauchy: un extrait

Nous avons reproduit ici les premières pages du mémoire de Cauchy où celui-ci démontre que, pour tout nombre premier impair p et tout diviseur premier n de $p-1$ de la forme $4x+3$, on peut toujours trouver des nombres entiers X et Y tels que $4p^{\frac{n-1}{2}} = X^2 + nY^2$. Avant cet extrait, Cauchy introduit les notations déjà utilisées dans le mémoire de 1829, il rappelle la notion d'indice de Gauss et une version équivalente de la définition généralisée du symbole de Legendre donnée dans (Cauchy 1829a). Nous avons indiqué tout au long du texte dans quelles parties de l'ouvrage de Cauchy sont démontrés les résultats indiqués. Certains détails de ces compléments sont donnés dans la partie principale de l'article, l'objectif étant ici de mettre en avant les difficultés rencontrées à la lecture de ce texte. Nous avons indiqué nos annotations entre crochets en caractères linéaux. Rappelons que $p = n\varpi + 1$.

Soient maintenant

$$\Theta_h = \theta + \rho^h \theta^t + \rho^{2h} \theta^{t^2} + \cdots + \rho^{(p-2)h} \theta^{t^{p-2}} \tag{8}$$

et

$$\Theta_h \Theta_k = R_{h.k} \Theta_{h+k}. \tag{9}$$

$R_{1.m}$ sera une fonction de ρ de la forme

$$R_{1.m} = a_0 + a_1\rho + a_2\rho^2 + \cdots + a_{n-1}\rho^{n-1};$$

et si l'on pose

$$k \equiv mh \pmod{n},$$

on aura, en supposant m différent de zéro et de $\frac{n}{2}$,

$$R_{h.mh} = a_0 + a_1\rho^h + a_2\rho^{2h} + \cdots + a_{n-1}\rho^{(n-1)h}$$

et

$$R_{h.k} = (-1)^{\varpi(h+k)} \sum \left(\frac{u}{p}\right)^h \left(\frac{v}{p}\right)^k, \tag{10}$$

le signe $\sum$ s'étendant à toutes les valeurs entières de u, v comprises entre les limites 1, $p-1$, et qui vérifieront l'équivalence

$$1 + u + v \equiv 0 \pmod{p}.$$

On aura d'ailleurs, en supposant h différent de zéro,

$$\Theta_h \Theta_{-h} = (-1)^{\varpi h} p, \quad R_{h,-h} = -(-1)^{\varpi h} p, \tag{11}$$

et, en supposant $h, k, h + k$ non divisibles par n,

$$R_{h,k} R_{-h,-k} = p. \tag{12}$$

On trouvera, au contraire

$$R_{h,0} R_{0,h} = -1. \tag{13}$$

Enfin l'on aura

$$a_0 + a_1 + a_2 + \cdots + a_{n-1} = p - 2 \tag{14}$$

et, en supposant n pair,

$$a_0 - a_1 + a_2 - a_3 + \cdots - a_{n-1} = -(-1)^{\frac{\varpi n}{2}}. \tag{15}$$

[Les égalités 9 à 15 sont démontrées dans la note I pour le cas particulier où $\varpi = 1$; elles n'y sont néanmoins pas toujours formulées de la même façon. Par exemple, pour la formule (10), Cauchy n'utilise pas le symbole de Legendre dans la note I. Cauchy revient sur les égalités (14) et (15), et sur d'autres propriétés des coefficients des expressions $R_{h,k}$ dans la note V.]

Par suite, si l'on suppose

$$R_{h,k} = F(\rho), \tag{16}$$

[Le fait que $R_{h,k}$ ne dépend que de ρ est également démontré dans la note I.]

on trouvera

$$F(\rho^m) = R_{mh,mk} \quad \text{et} \quad F(\rho^m) F(\rho^{-m}) = p, \tag{17}$$

[L'égalité (17) est en fait l'égalité (13) de la note I.]

si le nombre m est tel qu'aucune des équations

$$\rho^{mh} = 1, \ \rho^{mk} = 1, \ \rho^{m(h+k)} = 1 \tag{18}$$

[Les égalités (18) sont traduites en termes de divisibilité par le nombre n dans la note I.]

ne soit vérifiée. On aura, au contraire,

$$F(\rho^m) = -(-1)^{\varpi mh - \varpi mk} \tag{19}$$

si une seule des équations (18) est satisfaite, et

$$F(\rho^m) = p - 2 \tag{20}$$

si les trois équations (18) subsistent simultanément.

Soient encore h, k, l trois nombres entiers propres à vérifier la condition

$$h + k + l \equiv 0 \pmod{n}. \tag{21}$$

On aura, en supposant ces nombres tous trois différents de zéro,

$$\Theta_h \Theta_k \Theta_l = (-1)^{\varpi l} \frac{\Theta_h \Theta_k}{\Theta_{h+k}} = (-1)^{\varpi k} \frac{\Theta_h \Theta_l}{\Theta_{h+l}} = (-1)^{\varpi h} \frac{\Theta_k \Theta_l}{\Theta_{k+l}}$$

et, par conséquent,

$$(-1)^{\varpi h} R_{k,l} = (-1)^{\varpi k} R_{l,h} = (-1)^{\varpi l} R_{k,h}. \tag{22}$$

Soit maintenant s une racine primitive de

$$x^{n-1} \equiv 1 \pmod{n}, \tag{23}$$

le nombre n étant supposé premier, et faisons

$$\Theta_1 \Theta_{s^2} \Theta_{s^4} \ldots \Theta_{s^{n-3}} = \mathscr{F}(\rho) \tag{24}$$

on aura

$$\Theta_s \Theta_{s^3} \Theta_{s^5} \ldots \Theta_{s^{n-2}} = \mathscr{F}(\rho^s) \tag{25}$$

et, de plus,

$$\mathscr{F}(\rho) = \mathscr{F}(\rho^{s^2}) = \mathscr{F}(\rho^{s^4}) = \cdots = \mathscr{F}(\rho^{s^{n-3}}),$$

[Cauchy indique en note de bas de page que $1 + s^2 + s^4 + \cdots + s^{n-3} \equiv 0 \pmod{n}$: c'est donc pour cette raison que le produit ci-dessus ne dépend que de ρ.]

$$\mathscr{F}(\rho^s) = \mathscr{F}(\rho^{s^3}) = \mathscr{F}(\rho^{s^5}) = \cdots = \mathscr{F}(\rho^{s^{n-2}}).$$

Donc $\mathscr{F}(\rho)$ sera de la forme

$$\mathscr{F}(\rho) = c_0 + c_1(\rho + \rho^{s^2} + \rho^{s^4} + \cdots + \rho^{s^{n-3}}) + c_2(\rho^s + \rho^{s^3} + \cdots + \rho^{s^{n-2}}) \tag{26}$$

[Cauchy démontre que les expressions de la forme $R_{h,k,l,\ldots}$ sont symétriques par rapport aux puissances ρ^h, ρ^k, ρ^l dans la note III. Les propriétés des fonctions symétriques et alternées des racines primitives d'une équation binôme sont étudiées par Cauchy dans les notes VI et VII. Cela lui permet d'obtenir notamment la formule (26).]

ou

$$\mathscr{F}(\rho) = \frac{2c_0 - c_1 - c_2}{2} + \frac{c_1 - c_2}{2}(\rho - \rho^s + \rho^{s^2} - \rho^{s^3} + \cdots + \rho^{s^{n-3}} - \rho^{s^{n-2}})$$

et, comme on aura

$$s^{\frac{n-1}{2}} \equiv -1 \pmod{n},$$
$$\rho + \rho^s + \rho^{s^2} + \cdots + \rho^{s^{n-3}} + \rho^{s^{n-2}} = -1,$$
$$(\rho - \rho^s + \rho^{s^2} - \rho^{s^3} + \cdots + \rho^{s^{n-3}} - \rho^{s^{n-2}})^2 = (-1)^{\frac{n-1}{2}} n,$$

[Cette dernière égalité correspond à une somme de Gauss quadratique déjà démontrée par Gauss dans (Gauss 1801, Art. 356) et à la formule (14) obtenue par Cauchy dans la note I.] on trouvera

$$\mathscr{F}(\rho)\mathscr{F}(\rho^s) = \left(\frac{2c_0 - c_1 - c_2}{2}\right)^2 - (-1)^{\frac{n-1}{2}} n \left(\frac{c_1 - c_2}{2}\right)^2,$$

ou, ce qui revient au même,

$$4\mathscr{F}(\rho)\mathscr{F}(\rho^s) = (2c_0 - c_1 - c_2)^2 - (-1)^{\frac{n-1}{2}} n(c_1 - c_2)^2, \tag{27}$$

ou bien encore

$$\mathscr{F}(\rho)\mathscr{F}(\rho^s) = (c_0 - c_1)^2 + (c_0 - c_2)(c_1 - c_2) + \frac{1 - (-1)^{\frac{n-1}{2}} n}{4}(c_1 - c_2)^2. \tag{28}$$

Lorsque n est de la forme $4x + 3$, l'équation (27) ou (28) se réduit à

$$4\mathscr{F}(\rho)\mathscr{F}(\rho^s) = (2c_0 - c_1 - c_2)^2 + n(c_1 - c_2)^2 \tag{29}$$

ou bien à

$$\mathscr{F}(\rho)\mathscr{F}(\rho^s) = (c_0 - c_1)^2 + (c_0 - c_2)(c_1 - c_2) + \frac{n+1}{4}(c_1 - c_2)^2. \tag{30}$$

Au contraire, lorsque n est de la forme $4x + 1$, alors, $\frac{n-1}{2}$ étant pair, la formule (24) donne simplement

$$\mathscr{F}(\rho) = p^{\frac{n-1}{4}}$$

[Cette formule est démontrée dans la note III, dans laquelle Cauchy utilise implicitement des résultats démontrés dans les notes VI et VII.] et ρ disparaît de l'équation (26), qui se trouve réduite à la forme

$$\mathscr{F}(\rho) = c_0.$$

Revenons au cas où n est de la forme $4x + 3$. Comme on aura

$$\mathscr{F}(\rho)\mathscr{F}(\rho^s) = p^{\frac{n-1}{2}},$$

[Cette égalité est démontrée dans la note III, dans laquelle Cauchy utilise implicitement des résultats démontrés dans les notes VI et VII.] l'équation (29) donnera

$$4p^{\frac{n-1}{2}} = (2c_0 - c_1 - c_2)^2 + n(c_1 - c_2)^2.$$

Donc on résoudra l'équation

$$4p^{\frac{n-1}{2}} = X^2 + nY^2 \tag{31}$$

en prenant

$$X = 2c_0 - c_1 - c_2, \quad Y = c_1 - c_2.$$

Annexe B

See Table 1.

Annexe C

See Table 2.

Table 1 Liste des travaux arithmétiques de Cauchy publiés ou présentés à l'Académie des sciences (1829–1840)

Liste des publications et présentations à l'Académie de Cauchy en théorie des nombres (1829–1840)					
Année	Titre	Référence		Savants cités par Cauchy	Nb. pages
1829	Mémoire sur la théorie des nombres	BF	12, pp. 205–221	Gauss, Poinsot, Jacobi	20
1829	Sur diverses propositions relatives à l'algèbre et à la théorie des nombres	Ex.	45-46^{e} livraisons	Euler, Lagrange, Gauss, Legendre, Libri, Poinsot, Binet	99
1829	Sur la résolution des équivalences dont les modules se réduisent à des nombres premiers	Ex.	46-47^{e} livraisons	Gauss, Libri	44
1829	Détermination des racines primitives dans la théorie des nombres	PV	14 septembre 1829 (9, p. 312)		
1829	Théorie générale des puissances qui comprend comme cas particuliers tout ce que l'on sait sur la théorie des résidus quadratiques et biquadratiques, etc	PV	14 septembre 1829 (9, p. 312)		
1829	Mémoire sur la théorie des nombres	PV[1]	9 novembre 1829 (9, p. 350)		
1830	Détermination des racines primitives dans la théorie des nombres	PV	25 janvier 1830 (9, p. 393)		
1830	Détermination des racines primitives dans la théorie des nombres	PV	31 mai 1830 (9, p. 449)		
1830	Mémoire sur la théorie des nombres	PV	31 mai 1830 (9, p. 449)		
1830	Détermination des racines primitives	PV	5 juillet 1830 (9, p. 470)		
1830		PV[2]	12 juillet 1830 (9, p. 473)		
1831	Sur la théorie des nombres	BF	15, pp. 137–139	X	4
1839	Sur la théorie des nombres et en particulier sur les formes quadratiques des nombres premiers	CRAS	14 octobre 1839 (9, pp. 473–474)	Libri, Gauss, Jacobi	3
1839	Sur la théorie des nombres et en particulier sur les formes quadratiques des puissances d'un nombre premier, ou du quadruple de ces puissances	CRAS	28 octobre 1839 (9, pp. 519–526)	Lagrange, Gauss, Poinsot	8

Table 1 continued

Liste des publications et présentations à l'Académie de Cauchy en théorie des nombres (1829–1840)

Année	Titre	Référence		Savants cités par Cauchy	Nb. pages
1840	Théorèmes relatifs aux formes quadratiques des nombres premiers et de leurs puissances	CRAS	13 janvier 1840 (10, pp. 51–61)	Gauss, Jacobi	12
1840	Observations nouvelles sur les formes quadratiques des nombres premiers et de leurs puissances	CRAS	20 janvier 1840 (10, pp. 85–100)	Jacobi	18
1840	Suite des observations sur les formes quadratiques de certaines puissances des nombres premiers. Théorèmes relatifs aux exposants de ces puissances	CRAS	3 février 1840 (10, pp. 181–190)	X	11
1840	Discussion des formes quadratiques sous lesquelles se présentent certaines puissances des nombres premiers. Réduction des exposants de ces puissances	CRAS	10 février 1840 (10, pp. 229–243)	Jacobi	17
1840	Théorèmes divers sur les résidus et les non-résidus quadratiques	CRAS	16 mars 1840 (10, pp. 437–452)	Gauss, Liouville, Dirichlet	18
1840	Méthode simple et nouvelle pour la détermination complète des sommes alternées, formées avec les racines primitives des équations binômes	CRAS	6 avril 1840 (10, pp. 560–572)	Gauss, Dirichlet, Lebesgue, Poisson	15
1840	Sur la sommation de certaines puissances d'une racine primitive d'une équation binôme, et en particulier des puissances qui offrent pour exposants les résidus cubiques inférieurs au module donné	CRAS	13 avril 1840 (10, pp. 594–606)	Gauss, Jacobi, Libri, Lebesgue	15
1840	Sur quelques séries dignes de remarque, qui se présentent dans la théorie des nombres	CRAS	11 mai 1840 (10, pp. 719–731)	Dirichlet, Liouville	12
1840	Mémoire sur la théorie des nombres	Mém. Ac.	17, pp. 249–768	Gauss, Poinsot, Legendre, Euler, Dirichlet, Jacobi	446
1840	Méthode simple et nouvelle pour la détermination complète des sommes alternées formées avec les racines primitives des équations binomes	JMPA[3]	5, pp. 154–168	Gauss, Dirichlet, Lebesgue, Poisson	15

Table 1 continued

Liste des publications et présentations à l'Académie de Cauchy en théorie des nombres (1829–1840)

Année	Titre	Référence		Savants cités par Cauchy	Nb. pages
1840	Sur la sommation de certaines puissances d'une racine primitive d'une équation binôme, et en particulier des puissances qui offrent pour exposants les résidus cubiques inférieurs au module donné	JMPA[4]	5, pp. 169–183	Gauss, Jacobi, Libri, Lebesgue	15

[1] Réception d'un mémoire par l'Académie

[2] "Cauchy entretient l'Académie de divers Mémoires qu'il avait, dit-il, présentés en 1829 et 1830, et dans lesquels il a donné plusieurs méthodes propres à la Détermination des racines primitives et quelques propositions relatives a la Théorie des nombres"

[3] Reproduction de la note insérée dans les CRAS (6 avril 1840)

[4] Reproduction de la note insérée dans les CRAS (13 avril 1840)

Voici la signification des différentes abréviations utilisées dans ce tableau

BF *Bulletin des sciences mathématiques, astronomiques, physiques et chimiques*, souvent appelé *Bulletin de Férussac*

CRAS: *Comptes rendus hebdomadaires des séances de l'Académie des sciences*

Ex.: *Exercices de mathématiques* (périodique publié régulièrement de 1826 à 1830, dont l'unique rédacteur est Cauchy (Belhoste 1985, p. 93).)

JMPA: *Journal de mathématiques pures et appliquées*, souvent appelé *Journal de Liouville*

Mém. Ac.: *Mémoires de l'Académie royale des sciences de l'Institut de France*

PV: *Procès verbaux des séances de l'Académie*. Ces entrées ne correspondent donc pas à des publications de Cauchy mais à des interventions lors de séances de l'Académie des sciences

Table 2 Structure du *Mémoire sur la théorie des nombres* de Cauchy (1840)

	Titre du paragraphe/de la note	Pages	Nb. For.	Références explicites à la partie principale du mémoire
§I		pp. 6–21	59	
§II	Applications nouvelles des formules établies dans le premier paragraphe	pp. 21–42	78	
§III	Suite du même sujet	pp. 43–68	81	
§IV	Suite du même sujet	pp. 68–83	33	
Note I	Propriétés fondamentales des fonctions $\Theta_h, \Theta_k, \ldots$	pp. 84–94	14	Certaines formules correspondent à des égalités des paragraphes I et III
Note II	Sur diverses formules obtenues dans le deuxième paragraphe	pp. 94–110		Références aux formules du paragraphe II
Note III	Sur la multiplication des fonctions $\Theta_h, \Theta_k, \ldots$	pp. 110–163	110	Cauchy note que beaucoup de formules données dans la partie principale découlent des résultats sur les produits des Θ_h
Note IV	Sur les résidus quadratiques	pp. 163–180	40	
Note V	Détermination des fonctions $R_{h,k}$, ...et des coefficients qu'elles renferment	pp. 180–221	99	
Note VI	Sur la somme des racines primitives d'une équation binôme et sur les fonctions symétriques de ces racines	pp. 222–239	31	
Note VII	Sur les sommes alternées des racines primitives des équations binômes, et sur les fonctions alternées de ces racines	pp. 239–264	63	
Note VIII	Propriétés des nombres qui, dans une somme alternée des racines primitives d'une équation binôme, servent d'exposants aux diverses puissances de l'une de ces racines	pp. 265–292	40	
Note IX	Théorèmes divers relatifs aux sommes alternées des racines primitives des équations binômes	pp. 293–308	35	
Note X	Sur les fonctions réciproques, et sur les moyens qu'elles fournissent d'évaluer les sommes alternées des racines primitives d'une équation binôme	pp. 308–333	67	
Note XI	Méthode simple et nouvelle pour la détermination complète des sommes alternées, formées avec les racines primitives des équations binômes	pp. 334–359	46	
Note XII	Formules diverses qui se déduisent des principes établis dans la note précédente	pp. 359–390	94	

Table 2 continued

	Titre du paragraphe/de la note	Pages	Nb. For.	Références explicites à la partie principale du mémoire
Note XIII	Sur les formes quadratiques de certaines puissances des nombres premiers, ou du quadruple de ces puissances	pp. 390–437	97	
Note XIV	Observations relatives aux formes quadratiques sous les quelles se présentent certaines puissances des nombres premiers, et réduction des exposants de ces puissances	pp. 437–449	24	

Les données ci-dessus sont issues de la reproduction du mémoire dans les *Œuvres complètes* de Cauchy. Dans la colonne intitulée «Nb. For.», nous avons indiqué le nombre de formules numérotées données par Cauchy dans chaque paragraphe ou note

References

Belhoste, B. 1985. *Cauchy, un mathématicien légitimiste au XIXe siècle*. Paris: Berlin.

Belhoste, B. 1991. *Augustin-Louis Cauchy*. New York: Springer.

Belhoste, B., and J. Lützen. 1984. Joseph Liouville et le Collège de France. *Revue d'histoire des sciences* 37(3–4): 255–304.

Biot, J.-B. 1842. Comptes rendus hebdomadaires des séances de l' Académie des sciences, publiés par MM. les secrétaires perpétuels, commençant au 3 août 1836. *Journal des Savants*, 641–661.

Boucard, J. 2011a. Louis Poinsot et la théorie de l'ordre: un chaînon manquant entre Gauss et Galois? *Revue d'histoire des mathématiques* 17(1): 41–138.

Boucard, J. 2011b. *Un "rapprochement curieux de l'algèbre et de la théorie des nombres": études sur l'utilisation des congruences de 1801 à 1850*, thèse de doctorat, Université Paris 6, Paris.

Brian, E., and C. Demeulenaere Douyère. 1996. *Histoire et mémoire de l'Académie des sciences. Guide de recherches*. Paris: Lavoisier.

Cauchy, A.-L. 1813. Recherches sur les nombres. *Journal de l'École polytechnique* IX(16): 99–123. Repr. in *Œuvres complètes*, éd. Académie des sciences, 2è sér., t. 1. Paris: Gauthier-Villars, 1882–1974: 39–63.

Cauchy, A.-L. 1815a. Mémoire sur le nombre de valeurs qu'une fonction peut acquérir lorsqu'on y permute de toutes les manières possibles les quantités qu'elles renferment. *Journal de l'École polytechnique* X(17): 1–28. Repr. in *Œuvres complètes*, ed. Académie des sciences, 2^{e} sér., t. 1, p. 64–90, Paris: Gauthier-Villars, 1882–1974.

Cauchy, A.-L. 1815b. Mémoire sur les fonctions qui ne peuvent obtenir que deux valeurs égales et de signes contraires par suite des transpositions opérées entre les variables qu'elles renferment. *Journal de l'École polytechnique* X(17): 29–97. Repr. in *Œuvres complètes*, ed. Académie des sciences, 2^{e} sér., t. 1, Paris: Gauthier-Villars, 1882–1974: 91–169

Cauchy, A.-L. 1818. Démonstration du théorème général de Fermat sur les nombres polygones. *Mémoires de la classe des sciences mathématiques et physiques de l'Institut de France* 14: 177–220. Repr. in *Œuvres complètes*, éd. Académie des sciences, $2^{é}$ sér., t. 6. Paris: Gauthier-Villars, 1882–1974: 320–353.

Cauchy, A.-L. 1829a. Mémoire sur la théorie des nombres. *Bulletin des sciences mathématiques, physiques et chimiques* XII: 205–221. Repr. in *Œuvres complètes*, éd. Académie des sciences, 2^{e} sér., t. 2. Paris: Gauthier-Villars, 1882–1974: 88–107.

Cauchy, A.-L. 1829b. Sur diverses propositions relatives à l'algèbre et à la théorie des nombres. *Exercices de mathématiques* 4: 217–252. Repr. in *Œuvres complètes*, éd. Académie des sciences, 2^{e} sér., t. 9. Paris: Gauthier-Villars, 1882–1974: 259–297.

Cauchy, A.-L. 1829c. Sur la résolution des équivalences dont les modules se réduisent à des nombres premiers. *Exercices de mathématiques* 4: 253–292. Repr. in *Œuvres complètes*, éd. Académie des sciences, 2^{e} sér., t. 9. Paris: Gauthier-Villars, 1882–1974: 298–341.

Cauchy, A.-L. 1831. Mémoire sur la théorie des nombres. *Bulletin des sciences mathématiques, physiques et chimiques* 15: 137–139.

Cauchy, A.-L. 1839a. Sur la théorie des nombres, et en particulier sur les formes quadratiques des nombres premiers. *Comptes rendus hebdomadaires des séances de l'Académie des sciences* 9: 473–474. Repr. in *Œuvres complètes*, éd. Académie des sciences, $1^{ère}$ sér., t. 4. Paris: Gauthier-Villars, 1882–1974: 506–513.

Cauchy, A.-L. 1839b. Sur la théorie des nombres, et en particulier sur les formes quadratiques des puissances d'un nombre premier ou du quadruple de ces puissances. *Comptes rendus hebdomadaires des séances de l'Académie des sciences* 9: 519–525. Repr. in *Œuvres complètes*, éd. Académie des sciences, $1^{ère}$ sér., t. 4. Paris: Gauthier-Villars 1882–1974: 506–513.

Cauchy, A.-L. 1840a. Mémoire sur la théorie des nombres. *Mémoires de l'Académie royale des sciences de l'Institut de France* 17: 249–768. Repr. in *Œuvres complètes*, éd. Académie des sciences, $1^{ère}$ sér., t. 3. Paris: Gauthier-Villars, 1882–1974: 5–450.

Cauchy, A.-L. 1840b. Méthode simple et nouvelle pour la détermination complète des sommes alternées, formées avec les racines primitives des équations binômes. *Comptes rendus hebdomadaires des sèances de l'Académie des sciences* 10: 560–572. Repr. in *Œuvres complètes*, éd. Académie des sciences, $1^{ère}$ sér., t. 5. Paris: Gauthier-Villars, 1882–1974: 152–166.

Cauchy, A.-L. 1840c. Sur la sommation de certaines puissances d'une racine primitive d'une équation binôme, et en particulier, des puissances qui offrent pour exposants les résidus cubiques inférieurs au module donné. *Comptes rendus hebdomadaires des séances de l'Académie des sciences* 10: 594–606.

Repr. in *Œuvres complètes*, éd. Académie des sciences, 1ère sér., t. 5. Paris: Gauthier-Villars, 1882–1974: 166–180.

Cauchy, A.-L. 1840d. Sur les fonctions alternées et sur diverses formules d'analyse. *Comptes rendus hebdomadaires des séances de l'Académie des sciences* 10: 178–181. Repr. in *Œuvres complètes*, éd. Académie des sciences, 1ère sér., t. 5. Paris: Gauthier-Villars, 1882–1974: 81–85.

Cauchy, A.-L. 1840e. Théorèmes relatifs aux formes quadratiques des nombres premiers et de leurs puissances. *Comptes rendus hebdomadaires des séances de l'Académie des sciences* 10: 51–61. Repr. in *Œuvres complètes*, éd. Académie des sciences, 1ère sér., t. 5. Paris: Gauthier-Villars, 1882–1974: 52–64.

Cauchy, A.-L. 1846. Mémoire sur les arrangements que l'on peut former avec des lettres données et sur les permutations ou substitutions à l'aide desquelles on passe d'un arrangement à un autre. *Exercices d'analyse et de physique mathématique* 3: 151–252. Repr. in *Œuvres complètes*, éd. Académie des sciences, 2e sér., t. 13. Paris: Gauthier-Villars, 1882–1974: 171–282.

Cox, D.A. 1989. *Primes of the form* $x^2 + ny^2$. New York: Wiley.

Crosland, M. 1992. *Science under Control: The French Academy of Sciences, 1795–1914*. Cambridge: Cambridge University Press.

Dahan Dalmedico, A. 1979. *Les recherches algébriques de Cauchy*, Thèse de 3é cycle. Université Paris 13, Paris.

Dahan Dalmedico, A. 1980. Les travaux de Cauchy sur les: substitutions. Étude de son approche du concept de groupe. *Archive for History of Exact Sciences* 23(4): 279–319.

Dahan Dalmedico, A. 1997. L'étoile "imaginaire" a-t-elle immuablement brillé ? le nombre complexe et ses différentes interprétations dans l'oeuvre de Cauchy. Dans *Le nombre, une hydre à n visages*, édité par D. Flament, Paris: Maison des Sciences de l'Homme, 29–50.

Dhombres, J., and C. Gilain. 1992. Bibliographie concernant Cauchy (1974 à aujourd'hui). *Revue d'histoire des sciences* 45(1): 129–134.

Dirichlet, J.P.G.L. 1832. Démonstration d'une propriété analogue à la loi de réciprocité qui existe entre deux nombres premiers quelconques. *Journal für die reine und angewandte Mathematik* 9: 379–389.

Dirichlet, J.P.G.L. 1838. Sur l'usage des séries infinies dans la théorie des nombres. *Journal für die reine und angewandte Mathematik* 18: 259–274.

Domingues, C. J. 2008. Lacroix and the Calculus . Bâle: Birkhäuser.

Edwards, H.M. 1977. *Fermat's Last Theorem. A Genetic Introduction to Algebraic Number Theory*, vol. 50, New York: Springer.

Ehrhard, E. C. L'identité sociale d'un mathématicien et enseignant: Sylvestre-François Lacroix (1765–1843). *Histoire de l'éducation*, 123:5–43.

Euler, L. 1774. Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia. *Novi Commentarii academiae scientiarum Petropolitanae* 18: 85–135.

Flament, D. 2003. *Histoire des nombres complexes. Entre algèbre et géométrie*. Paris: CNRS.

Galois, E. 1830. Sur la théorie des nombres. *Bulletin des sciences mathématiques, physiques et chimiques* 13: 428–435.

Gauss, C.F. 1801. *Disquisitiones Arithmeticae*, Leipzig: Fleischer. Traduction française par A. C. M. Poullet-Delisle, *Recherches arithmétiques*, Paris: Courcier, 1807.

Gauss, C.F. 1808. Theorematis arithmetici demonstratio nova, *Commentationes Societatis Regiae Scientiarum Gottingensis recentiores (Commentationes mathematicae)* 16: 69–74. Repr. in Werke, vol. II, Höhere Arithmetik, ed. *Königliche Gesellschaft der Wissenschaften zu Göttingen*, Göttingen: Universitäts-Druckerei 1863: 3–8.

Gauss, C.F. 1811. Summatio quarundam serierum singularium. *Commentationes societatis regiae scientiarum Gottingensis recentiores*, vol. 1. Repr. in Werke, vol. II, Höhere Arithmetik, ed. *Königliche Gesellschaft der Wissenschaften zu Göttingen*, Göttingen: Universitäts-Druckerei 1863: 11–45.

Gauss, C.F. 1818. Theorematis fundamentalis in doctrina de residuis quadraticis demonstrationes et ampliationes novae. *Commentationes societatis regiae scientiarum Gottingensis recentiores* 4: 3–20. Repr. in Werke, vol. II, Höhere Arithmetik, ed. *Königliche Gesellschaft der Wissenschaften zu Göttingen*, Göttingen: Universitäts-Druckerei 1863: 49–64.

Gauss, C.F. 1828. Theoria residuorum biquadraticorum, commentatio prima. *Commentationes societatis regiae scientiarum Gottingensis recentiores* 6: 27–56. Repr. in Werke, vol. II, Höhere Arithmetik, ed. *Königliche Gesellschaft der Wissenschaften zu Göttingen*, Göttingen: Universitäts-Druckerei 1863: 65–92.

Gauss, C.F. 1832. Theoria residuorum biquadraticorum, Comentatio: secunda. *Commentationes societatis regiae scientiarum Gottingensis recentiores* 7: 89–148. Repr. in Werke, vol. II, Höhere Arith-

metik, ed. *Königliche Gesellschaft der Wissenschaften zu Göttingen*, Göttingen: Universitäts-Druckerei 1863: 93–150.

Gilain, C. 1989. Cauchy et le cours d'analyse de l'École polytechnique. *Bulletin de la Société des amis de la bibliothèque de l'École polytechnique* 5: 3–46.

Goldstein, C., and N. Schappacher. 2007. A Book in Search of a Discipline (1801–1860), dans *The Shaping of Arithmetic after C. F. Gauss's Disquisitiones Arithmeticae*, édité par C. Goldstein, N. Schappacher et J. Schwermer. 3–65, Berlin: Springer.

Ireland, K., and M. Rosen. 1990. *A Classical Introduction to Modern Number Theory*, 2^e éd. New York: Springer.

Jacobi, C.G.J. 1827. De residuis cubiscis commentatio numerosa. *Journal für die reine und angewandte Mathematik* 2: 66–69.

Jacobi, C.G.J. 1837. Über die Kreistheilung und ihre Anwendung auf die Zahlentheorie. *Monatsbericht der Akademie der Wissenschaften zu Berlin*, p. 127–136. Traduction française par E. Laguerre-Werly. Sur la division du cercle et son application a la théorie des nombres. *Nouvelles annales de mathématiques*, $1^{ère}$ série, tome 15, 1856: 337–352.

Jacobi, C.G.J. 1839. *Canon arithmeticus sive tabulae quibus exhibentur pro singulis numeris primis vel primorum potestatibus infra 1000 numeri an datos indices et indices ad datos numerus pertinentes.* Berlin: Typis Academicis.

Jacobi, C.G.J. 1881–1891. *Briefe Jacobi's an Gauss. dans Gesammelte Werke*, vol. 7, Berlin: Reimer, 389–406.

Jacobi, C.G.J. 2007. *Vorlesungen über Zahlentheorie-Wintersemester 1836/37, Königsberg*. Augsburg: Dr. Erwin Rauner Verlag.

Kummer, E.E. 1847, Beweis des Fermat'schen Satzes der Unmöglichkeit von $x^\lambda + y^\lambda = z^\lambda$ für eine unendliche Anzahl Primzahlen λ, *Monatsberichte der Königlichen Preußischen Akademie der Wissenschaften zu* Berlin, 132–141, 305–319.

Lacroix, S.-F. 1800. *Traité des différences et des séries, faisant suite au traité du calcul différentiel et du calcul intégral*. Paris: Duprat.

Lacroix, S.-F. 1804. *Complément des élémens d'algèbre*, 3^e éd. Paris: Courcier.

Lagrange, J.-L. 1772–1773. Réflexions sur la résolution algébrique des équations. *Nouveaux mémoires de l'Académie royale des sciences et belles-lettres de Berlin*. 134–215 (1770); 138–253 (1771). Repr. in *Œuvres de Lagrange*, éd. J.-A. Serret, t. 3, Paris: Gauthier-Villars, 1869, 205–421.

Lagrange, J.-L. 1808. *Traité de la résolution des équations numériques de tous les degrés, avec des notes sur plusieurs points de la théorie des équations algébriques*, 2^e éd. Paris: Courcier.

Lamandé, P. 2004. La conception des nombres en France vers 1800: l'œuvre didactique de S.F. Lacroix. *Revue d'historie des mathématiques* 10: 45–106.

Lebesgue, V.-A. 1831. Note sur les résidus des puissances. *Bulletin des sciences mathématiques, physiques et chimiques* 15: 158–159.

Legendre, A.-M. 1808. *Essai sur la théorie des nombres*, 2^e éd. Paris: Courcier.

Lemmermeyer, F. 2000. *Reciprocity Laws: From Euler to Eisenstein*. Berlin: Springer.

Lemmermeyer, F. 2009. Jacobi and Kummer's Ideal Numbers. *Abhandlungen aus dem mathematischen Seminar der Universität Hamburg* 79(2): 165–187.

Libri, G. 1830. Sur les racines primitives des nombres premiers. *Bulletin des sciences mathématiques, physiques et chimiques* 13: 272–273.

Nielsen, N. 1923. *Traité élémentaire des nombres de Bernoulli*. Paris: Gauthier-Villars.

Peiffer, J. 1978. *Les premiers exposés globaux de la théorie des fonctions de Cauchy*, thèse de doctorat. EHESS, Paris.

Poinsot, L. 1818. Extrait de quelques recherches nouvelles sur l'algèbre et la théorie des nombres. *Mémoires de la classe des sciences mathématiques et physiques de l'Institut de France* 14: 381–392.

Poinsot, L. 1820. Mémoire sur l'application de l'algèbre à la théorie des nombres. *Journal de l'École polytechnique* 11: 342–410.

Staudt, G. K. C. von 1840. Beweis eines Lehrsatzes, die Bernoullischen Zahlen betreffend. *Journal für die reine und angewandte Mathematik* 21: 372–374.

Wussing, H. 1984. *The Genesis of the Abstract Group Concept*. Cambridge (MA): MIT Press.