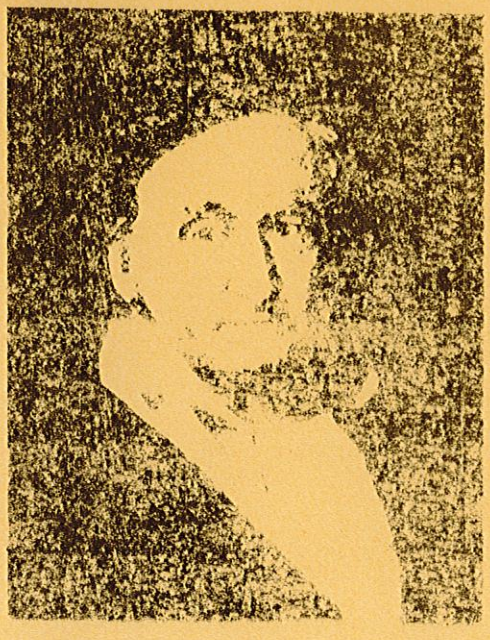


Roger Cuculière

---

histoire d'un théorème

d'arithmétique :

# LA LOI DE RECIPROCITE QUADRATIQUE

---

IREM PARIS·NORD

1980

UNIVERSITÉ PARIS 13
I.R.E.M.
99, Avenue Jean-Baptiste Clement
93430 VILLETANEUSE
Tél. 01 49 40 36 40

Roger Cuculière

---

histoire d'un théorème d'arithmétique :

# LA LOI DE RECIPROCITE QUADRATIQUE

---

IREM PARIS·NORD

1980

UNIVERSITÉ PARIS 13
I.R.E.M.
99, Avenue Jean-Baptiste Clement
93430 VILLETANEUSE
Tél. 01 49 40 36 40

UNIVERSITE PARIS-NORD. - IREM. -
Histoire d'un théorème d'arithmétique : LA LOI DE RECIPROCITE QUADRATIQUE / Roger CUCULIERE. Villetaneuse, 1980. - 71 p. dactylo. - 29 cm.

ISBN 2 86240 060 2

Dépôt légal : 2nd trimestre 1980

300 ex

7,00 F

C. S. P. - I R E M
Avenue Jean-Baptiste-Clément
93430 VILLETANEUSE
☎ 821.61.70
France

History of a theorem on arithmetics.

# The quadratic reciprocity law.

--- Summary. ---

This memo deals with Diophantine Analysis of the Second Degree, i.e. second degree equations in integers or rational numbers, and quadratic forms or congruences.

It is quite an old topic, since its origins can be found in the Pythagorician "arithmo-geometry", which used to represent integers with geometric shapes (for instance, the *square*). The most famous example of a quadratic diophantine equation is the Theorem of Pythagoras: $x^2 + y^2 = z^2$, and one immediately refers to its generalisation, still unsolved: the last Fermat's Theorem.

Some of the greatest Mathematicians studied this subject: Diophantus, Vieta, Fermat, ... In 1754, Euler set the following definition: *an integer* a *is a* quadratic residue *of an integer* b *if there exists an integer* x *such that* $x^2 \equiv a \pmod{b}$. Euler and Lagrange got many particular results about quadratic forms or residues, which are two close subjects.

Legendre gave in 1785 the quadratic reciprocity law : p *and* q *being two primes,* p *is* residue *of* q *iff* q *is residue of* p, *except when* p *and* q *can be expressed in the form* $4k + 3$: *then,* p *is residue of* q *iff* q *is* NOT *residue of* p. Legendre also defined his symbol : $\left(\frac{p}{q}\right) = 1$ or $-1$ according as p is, or is not, residue of q. Using this symbol, the law becomes:

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

But Legendre did not quite prove his law. Gauss did it, and published successively up to six proofs , fully described in our memoir. Afterwards, many mathematicians gave demonstrations, founded upon various principles. It is perhaps the theorem which has encountered the greatest number of demonstrations: several among the most important are shown here. This theorem, which Gauss considered to be fundamental, gathered many partial results, and set up an epistemological spring in the theory of numbers. Later on, it has got many generalisations, for higher degrees or other number fields. These works led to very important theories, such as classe field theory. The quadratic reciprocity law is one of the results which opened the era of modern mathematics.

# Histoire d'un théorème d'arithmétique : LA LOI DE RECIPROCITE QUADRATIQUE

# AVANT PROPOS

Il n'est plus à démontrer que la Théorie des Nombres occupe une place à part. On a pu dire en effet que, si la Mathématique est la reine des sciences, la Théorie des Nombres est la reine des Mathématiques. C'est une discipline pleine d'inattendu, où l'on ne peut juger *a priori* de la difficulté d'une question. Tel énoncé compréhensible par un élève de douze ans, comme la conjecture de Goldbach (" Tout nombre pair, sauf 2, est somme de deux nombres premiers ") peut s'avérer un problème ouvert qui résiste aux plus grands esprits. L'objet que l'on y étudie, les nombres, est (ou semble) si familier que l'on a envie de résoudre les questions qui s'y rattachent. Nombre de ces questions prennent plus l'allure de "petits problèmes" récréatifs que de pensums repoussants. En même temps, la Théorie des Nombres est l'une des grandes sources du progrès mathématique, par les outils qu'elle contraint les mathématiciens à créer pour résoudre ses problèmes. Nous en verrons ici deux exemples : formes quadratiques, idéaux .

L'Arithmétique est sans doute, avec la Géométrie Elémentaire, la plus ancienne branche des mathématiques, et du rapprochement des deux provient l'importance de l'équation du Second Degré, car le carré est la figure dominante de notre espace euclidien et le théorème de Pythagore est l'un des plus anciens moyens d'y déterminer les distances. Bien sûr, si le cube de l'hypoténuse était somme des cubes des deux autres côtés, la Théorie des Nombres n'aurait pas le même aspect, mais l'espace ambiant non plus !

Le théorème dont nous traitons ici date de la fin du dix-huitième siècle. C'est sans doute le résultat le plus original et le plus important de ce siècle en Théorie des Nombres. C'est une proposition synthétique et inattendue, qui, de plus, est d'une grande beauté. Il ne s'agit pas d'un énoncé clair par lui-même, comme la conjecture de Goldbach, que nous avons citée plus haut. Au contraire, ce théorème rassemble un grand nombre de résultats antérieurs et annonce des développements bien plus rapides. Il marque vraiment une étape, un saut épistémologique dans le développement de la science des nombres.

Aussi, tenterons-nous d'abord de décrire, les conditions qui ont présidé à la formulation de cette "loi de réciprocité". Il ne s'agira pas, bien sûr, de retracer par le menu toute l'histoire de l'analyse diophantienne du second degré et de la théorie des formes quadratiques, sujet qui remplirait plusieurs forts volumes. Nous nous bornerons à relater les étapes importantes du développement mathématique conduisant à ce théorème que Gauss a dit "fondamental". Nous rapporterons son premier énoncé par LeGendre, et le symbole dans lequel il s'exprime naturellement.

Nous nous arrêterons longuement sur les travaux de Gauss, qui n'en a pas donné moins de huit démonstrations, dont six publiées de son vivant. Nous présenterons quelques autres démonstrations et généralisations de ce théorème, qui est sans doute un de ceux pour lesquels ont été publiées le plus grand nombre de preuves : un article de l'"American Mathematical Monthly" d'avril 1963 s'intitule : " the 152-nd proof of the law of quadratic reciprocity ".

Nous signalerons enfin les développements ultérieurs de cette propriété, dont la présentation peut constituer en soi un travail plus important.

Nous ne pouvions assurément viser à être exhaustif, puisque les travaux dont nous relatons l'histoire représentent des centaines de pages : vouloir en exprimer l'intégralité, c'était se lancer dans des développements d'une égale ampleur. Mais nous croyons avoir présenté les principales phases du processus mathématique en question, avec les références précises permettant, à qui le désirerait, de reprendre plus en détail tel ou tel point.

Nous avons aussi voulu établir des filiations entre les démonstrations classiques de la loi de réciprocité et celles qui sont présentées dans des ouvrages plus récents de Théorie des Nombres. Il s'ensuit une bibliographie assez considérable mais qui, nous l'espérons, ne sera pas sans intérêt.

★

★ ★

Il est curieux de constater qu'en Mathématiques, au contraire des disciplines littéraires, on peut suivre un cursus universitaire complet

sans avoir pris un contact direct avec les classiques. De plus. l'accès à ces classiques est bien plus difficile. On peut se procurer, dansla première librairie venue, une oeuvre de Corneille ou de Diderot , ou une traduction française de Goethe ou de Shakespeare. Mais les écrits de Fermat, d'Euler, de Gauss ne se trouvent pas aussi aisément, loin s'en faut.

Il est vrai que l'étude des sciences n'est pas l'étude de leur histoire et que le cours de leur apprentissage n'a pas à reproduire le processus de leur élaboration. Il n'en est pas moins vrai que l'étude concrète de certains points du développement mathématique, et le recours direct aux penseurs qui ont apporté des contributions décisives, donnne une vision plus exacte et plus attrayante des mathématiques. Cette étude permet d'apprendre que l'ordre bourbachique d'exposition de la science acquise, sans doute légitime comme ordre d'exposition, n'est pas identique au processus de développement de la science qui se fait. Elle met en lumière les qualités d'intuition et d'initiative qu'ont dû déployer les créateurs, et les libertés qu'ils ont dû prendre avec la "rigueur" en vigueur à leur époque. Aussi, les conséquences pédagogiques de cette étude sont-elles fort bénéfiques, et il est très heureux que, de plus en plus, l'enseignement des mathématiques se nourrisse de références à l'histoire de cette science, notamment en Arithmétique. La présente contribution souhaite s'inscrire dans ce courant.

Ce travail constitue un mémoire de DEA présenté à l'Université Paris VII, sous la direction de M. Gilles Lachaud, que nous tenons à remercier ici.

Nous remercions aussi Mme Chantal Labre, qui a bien voulu assurer les traductions des textes latins de Gauss, et l'IREM de Paris-Nord, dont l'aide nous a été précieuse à plus d'un titre, et qui a bien voulu publier ce travail et le diffuser.

Paris, mai 1980 .

## § I - CARACTERE QUADRATIQUE D'UN NOMBRE :

## ORIGINES DU PROBLEME

(1) Dans un écrit de 1754-55, Euler introduit le concept de résidu quadratique : si a et b sont des entiers rationnels, on dit que a est résidu quadratique de b s'il existe un entier rationnel x tel que $x^2 - a$ soit multiple de b, c'est-à-dire $x^2 \equiv a \pmod{b}$. Dans le cas contraire, a est non-résidu de b. Trouver le caractère quadratique de a relativement à b, c'est déterminer si a est résidu ou non-résidu de b.

Dans quelle lignée cette notion s'inscrit-elle ? L'importance du second degré en algèbre est liée à l'importance du carré en géométrie. C'est aux Pythagoriciens et à leur "arithmo-géométrie" (vers 500 avant J.C.) que l'on peut faire remonter l'idée de représenter un nombre entier sous une certaine forme : nombres triangulaires, carrés, polygonaux, etc. (cf. [CO1], p.51 ; [RE], p.103).

Le mot "carré" est venu jusqu'à nous comme un témoin de ce souci, puisqu'il désigne aussi bien une figure géométrique qu'une propriété de certains nombres entiers. Le rôle particulier des sommes de deux carrés se relie au célèbre "Théorème de Pythagore" concernant le carré de l'hypoténuse (cf. [HE] p.121, [FO] p.66).

Rappelons que le triangle de côtés 3,4,5 a joué un grand rôle dans l'Antiquité, où on lui attribuait même parfois un caractère sacré. Il était connu des anciens égyptiens, chinois, hindous ([FO] p.66). Une tablette babylonienne datant de mille ans avant Pythagore donne quinze solutions entières de l'équation $x^2 + y^2 = z^2$ ([LV3], p.26). Platon a aussi donné une règle pour trouver de tels triplets. Au livre X de ses Eléments, Euclide a indiqué la solution bien connue pour les triplets "primitifs" : $x = 2uv$, $y = u^2 - v^2$, $z = u^2 + v^2$ avec $u > v$, u et v premiers entre eux (voir [DK2], p.165 ; [CO1], p.78).

(2) Diophante.

Ce mathématicien de la seconde école d'Alexandrie, qui vécut au III$^{e}$ siècle de notre ère, a consacré l'essentiel de son oeuvre à l'étude des problèmes que l'on a traduit ultérieurement par des équations en nombres entiers ou rationnels, dites "indéterminées" ou justement, "diophantiennes".

De ses livres arithmétiques, on peut citer la proposition VIII du livre II ([DI], p.53) : "partager un carré proposé en deux carrés".

Plusieurs propositions de cet ouvrage concernent la décomposition de certains nombres en sommes de deux carrés. La proposition XIX du livre III nous montre un exemple du fait que le produit de deux sommes de deux carrés est encore une somme de deux carrés : on a $5 = 1^2+2^2$, $13 = 2^2 + 3^2$, et $5 \times 13 = 65 = 1^2 + 8^2$ ([DI], p.108-109). Les nombres 5 et 13 utilisés ici sont les deux plus petits nombres premiers de la forme $4k + 1$.

D'après Sir Thomas L. Heath, Diophante savait qu'aucun nombre entier de la forme $4k - 1$ n'est somme de deux carrés. Ce résultat aurait figuré dans les "Porismes", un ouvrage dont l'ensemble a été perdu mais dont quelques extraits nous sont parvenus, sous formes de citations (cf. [HE], p.107).

(3) Diophante fut oublié en Occident durant plus de dix siècles. Il exerça une influence sur l'école des mathématiciens algébristes arabes (à travers la traduction de Ben Luga), et par leur intermédiaire, par Léonard de Pise (1180-1250), connu aussi sous le nom de Fibonacci, dont le "Livre des nombres carrés" (1225) traite encore d'équations "diophantiennes" du second degré (cf. [LP], p.XIX).

Voici par exemple la première phrase du prologue de cet ouvrage dédié à Frédéric II :

"Lorsque, ô seigneur Frédéric, prince très glorieux, maître Dominique m'amena à Pise, aux pieds de Votre Excellence, maître Jean de Palerme, m'ayant rencontré, me proposa la question, qui n'appartient pas moins à la géométrie qu'au nombre (*), de trouver un nombre carré qui, augmenté ou diminué de cinq, fait toujours un nombre carré."

---

(*) souligné par nous.

Il s'agit bien sûr de nombres rationnels. Fibonacci précise que la solution de cette question "prenait sa source dans les choses multiples qui se présentent dans les nombres carrés et entre ces nombres".

Citons également François Viète (1540-1603), qui reprit l'étude de nombreux problèmes disphantiens (cf. [DI], P.LXXIX ; [HE], p.285).

Mais il faut en arriver au XVII$^{e}$ siècle pour que l'analyse diophantienne retrouve un spécialiste éminent, en la personne de Claude Gaspar Bachet, sieur de Méziriac. Outre ses propres contributions, celui-ci édita les oeuvres de Diophante en 1621 ([DI], p.LXXXII).

## § II - FORMES QUADRATIQUES ET RESIDUS : FERMAT, EULER, LAGRANGE

### (4) Fermat (1601-1655) .

C'est cette édition de Diophante par Bachet que possédait Fermat et qui eut une grande influence sur lui. C'est dans la marge de ce "Diophante" qu'il inscrivit l'énoncé de son célèbre "Grand Théorème" . Et c'est à propos d'études diophantiennes que Fermat confie au R.P. Mersenne:"mi par diveder un gran lume" -"il me semble voir une grande lumière" (Lettre de juin 1640- [FE2], p.199).

Le plus beau théorème d'arithmétique que nous ait laissé Fermat est sans doute celui-ci :

"Tout nombre premier, qui surpasse de l'unité un multiple du quaternaire, est une seule fois la somme de deux carrés, et une seule fois l'hypotênuse d'un triangle rectangle" (Lettre à Mersenne du 25 décembre 1640- [FE2], p.213) .

Cette proposition revient plusieurs fois dans ses oeuvres ; par exemple, dans la lettre à Frenicle du 15 juin 1641 ([FE2], p.221) :

"La proposition fondamentale des triangles rectangles est que tout nombre premier, qui surpasse de l'unité un multiple de quatre, est composé de deux carrés".

On la retrouve encore dans la lettre à Digby de juin 1658

([FE2], p.403 en latin ; [FE3], p.315, pour la traduction) et dans l'observation VII sur Diophante ([FE1], p.293 , traduite dans [FE3], p.243).

Mais Fermat, conseiller au Parlement de Toulouse, ne tirait pas ses revenus de son activité mathématique et n'a jamais éprouvé la nécessité de publier ses travaux. Il n'a laissé aucun traité et son oeuvre se compose de lettres et notes éparses. Le plus souvent, il n'a rédigé aucune démonstration : tout au plus en a-t-il indiqué le principe. Le théorème en question n'échappe pas à cette remarque. Ses énoncés cités plus haut ne s'accompagnent pas de justifications : ils constituent des sortes de défis lancés aux correspondants.

On trouve cependant une indication au sujet de sa méthode de démonstration dans sa lettre à Carcavi d'août 1659 ([FE2], p.432) : parmi les écrits arithmétiques de Fermat, c'est sans doute le plus synthétique et le plus riche d'indications méthodologiques. On peut dire avec M. Jean Itard qu'il s'agit du testament de Fermat en matière de Théorie des Nombres. Et l'on peut s'en convaincre directement à la lecture de [IT1], p.41, où cette lettre est reproduite.

Cela dit, la lettre à Carcavi ne contient que l'information selon laquelle Fermat a démontré ce théorème par application de sa méthode de "descente infinie", et rien de plus. C'est Euler qui a produit la première démonstration complète ([EU 228])en s'appuyant sur les deux lemmes suivants :

- tout nombre premier $p$ de la forme $4k + 1$ divise une somme de deux carrés premiers entre eux.

- les diviseurs d'une somme de deux carrés premiers entre eux sont eux-mêmes sommes de deux carrés.

Le second lemme s'établit justement par la méthode de "descente infinie" (la démonstration en a été reprise dans [BO], p.80). C'est d'ailleurs pourquoi on peut valablement attribuer à Fermat lui-même la paternité de ce théorème.

Portons notre attention sur le premier lemme. Si $p$ , premier, divise $x^2 + y^2$ avec $x$ et $y$ premiers entre eux, $p$ ne peut diviser $x$ , ni $y$ : ils sont alors premiers avec $p$ . Disons donc, dans la terminologie actuelle, que la classe de $y$ n'est pas nulle dans le corps $Z/pZ$ : elle est par suite inversible. Autrement dit, il existe $y'$ entier tel que $yy' \equiv 1 \pmod{p}$ (L'existence de $y'$ nous est d'ailleurs assurée aussi par la relation de Bezaut). La relation $x^2 + y^2 \equiv 0 \pmod{p}$ implique alors $x^2y'^2 + y^2y'^2 \equiv 0$, d'où $(xy')^2 + 1 \equiv 0 \pmod{p}$. Posons $z = xy'$ , et nous

avons démontré l'assertion suivante : un nombre p premier divise une somme de deux carrés premiers entre eux si, et seulement si, il existe un entier z tel que q divise $z^2 + 1$ .

Mais d'après la définition rappelée ci-dessus (§ I, n°1), celà signifie que -1 est résidu quadratique de p . D'après le résultat de Fermat, -1 est donc résidu quadratique des nombres premiers p de la forme $4k + 1$ .

Réciproquement, le second lemme implique que -1 est non-résidu de tout nombre premier -p de la forme $4k - 1$. D'ailleurs Fermat a indiqué, dans une lettre à Roberval d'août 1640 :

"Si un nombre est composé de deux carrés premiers entre eux, je dis qu'il ne peut être divisé par aucun nombre premier moindre de l'unité qu'un multiple du quaternaire" ([FE2], p.204) .

(5) Mais il y a plus . Non content d'avoir élucidé la question des nombres qui "sont hypoténuses" (c'est-à-dire sommes de deux carrés), Fermat a énoncé les propositions suivantes :

"Tout nombre premier, de la forme $3n + 1$, est somme d'un carré et du triple d'un autre carré".

"Tout nombre premier, de la forme $8n + 1$ ou $8n + 3$, est somme d'un carré et du double d'un autre carré" ([FE3], p.315) .

"Si d'un quarré vous ôtez 2, le reste ne peut être divisé par aucun nombre premier qui surpasse un quarré de deux" ([FE2], p.211).

Les lettres de Frenicle à Fermat font apparaître qu'il savait aussi que les nombres premiers de la forme $8n \pm 1$ sont de la forme $y^2 - 2t^2$ (voir [LA ], p.775) .

Fermat ne se confine donc pas dans l'étude des nombres de la "forme" $x^2 + y^2$ , forme qui tire son intérêt spécifique de son interprétation géométrique, mais il étudie aussi des problèmes voisins.

La remarque que nous avons faite ci-dessus au sujet de la forme $x^2 + y^2$ et de ses relations avec le résidu quadratique -1 se généralise : les autres résultats de Fermat que nous avons cités s'interprètent aussi en termes de résidus quadratiques, car le nombre premier p divise $x^2 + ay^2$ (x et y premiers entre eux) si et seulement si -a est résidu quadratique de p .

Nous en concluons ainsi : que 2 est résidu quadratique des

nombres premiers de la forme $8n \pm 1$ et non-résidu des autres, et que $-2$ est résidu quadratique des nombres premiers de la forme $8n + 1$ ou $8n + 3$, et non-résidu des autres. C'est ce qui fera dire à Gauss, dans ses "Recherches Arithmétiques", que les propositions relatives aux résidus $2$, $-2$, $3$ et $-3$ étaient connues de Fermat ([GAD], p.85, p.87).

Et l'on peut trouver aussi, dans l'oeuvre du mathématicien toulousain, d'autres propositions qui seront une source de réflexion pour ceux qui, plus tard, s'intéresseront à ces questions (cf. [KL], p.276, [LA ], p.775).

(6) Euler

Présenter complètement et de façon détaillée la contribution d'Euler à la théorie des restes quadratiques exigerait de trop longs développements.

Notons d'abord que, dans son oeuvre, apparaît pour la première fois le terme "résidu quadratique", absent des écrits de Fermat ([EU 242]).

En Théorie des Nombres, il s'est attaché à démontrer maintes propriétés énoncées par Fermat, telles que celles qui concernent les formes quadratiques. Dans un écrit de 1744, il avait donné quarante théorèmes concernant de nombreuses formes quadratiques binaires, depuis les diviseurs de $a^2 + b^2$ jusqu'à ceux de $a^2 + 30b^2$ , $2a^2 + 15b^2$, $3a^2 + 10b^2$ , $5a^2 + 6b^2$ . Mais ces résultats n'étaient pas démontrés ([EU 164]).

Comme nous l'avons vu au n°4, Euler a démontré en 1752 le théorème de Fermat concernant la forme quadratique $a^2 + b^2$ , ce qui règle le cas du résidu $-1$ ([EU 228]).

Par la suite, il a donné des démonstrations de certains des résultats de Fermat qui concernaient les formes quadratiques $a^2 + 2b^2$ et $a^2 + 3b^2$ ([EU 256], [EU 272]). Comme l'ont remarqué Lagrange ([LA ], p.776) et Gauss ([GAD], n°116, p.85), Euler n'a pas complètement élucidé la question des nombres qui sont de la forme $a^2 + 2b^2$ ou diviseurs de cette forme ; mais il est le premier à avoir démontré que tout nombre premier de la forme $8n + 1$ est de la forme $a^2 + 2b^2$ .

En 1736, Euler a découvert la démonstration du "petit théorème" de Fermat qui dit que, si le nombre premier $p$ ne divise pas l'entier $a$, alors il divise $a^{p-1} - 1$ ([EU 54]). En 1760, il a d'ailleurs généralisé ce théorème ([EU 271]) par l'introduction de la "fonction indicatrice", nommée aujourd'hui "indicateur d'Euler" $\phi(n)$, qui est égale au nombre d'entiers naturels plus petits que l'entier naturel $n$ et premiers avec lui. Le "théorème d'Euler" affirme que si $a$ est premier avec $n$, alors $n$ divise $a^{\phi(n)} - 1$ : lorsque $n = p$ premier, on retrouve le "petit théorème" de Fermat.

Et ce "petit théorème" de Fermat, si éloigné qu'il paraisse de la question des restes quadratiques, appelle en fait une autre propriété : si $p$ divise $a^{p-1} - 1$, il divise $a^{\frac{p-1}{2}} - 1$, ou il divise $a^{\frac{p-1}{2}} + 1$. Euler a montré que l'entier $a$ est résidu quadratique de $p$ si, et seulement si, $p$ divise $a^{\frac{p-1}{2}} - 1$ : c'est le "critère d'Euler" ([EU 134]), qui date de 1747. On peut trouver une démonstration de cette propriété dans [IT2], p.72.

(7) Lagrange - Euler.

Dans son étude intitulée "Recherche d'Arithmétique", publiée dans les Nouveaux Mémoires de l'Académie de Berlin (années 1773,1775) Lagrange présente des résultats nouveaux sur les diviseurs des formes quadratiques $t^2 \pm au^2$, pour des valeurs quelconques de $a$, avec démonstration ([LA], p.695). Il observe que les diviseurs, ou les non-diviseurs, de ces formes se rangent dans des progressions arithmétiques de raison $4a$. Il résout ainsi en fait le problème pratique de la détermination des nombres premiers dont $a$, ou $-a$, est résidu, pour un grand nombre de valeurs de $a$, même s'il n'aborde pas spécifiquement et explicitement la question des résidus quadratiques. Il donne les démonstrations qui manquaient à l'article d'Euler de 1744([EU164]). Réciproquement, ce mémoire de Lagrange incita Euler à reprendre l'étude des formes et des résidus quadratiques. Cela donna, en 1783, deux textes : [EU 552], [EU 610], dont le dernier contient un énoncé qui anticipe la loi de réciprocité, mais qui n'est pas démontré dans toute sa généralité.

(8) Bilan provisoire.

Arrivés à ce stade, nous constatons deux acquis : premièrement, le concept de résidu quadratique formulé par Euler, et le critère découvert par lui en relation avec son travail sur le "petit théorème" de Fermat. Deuxièmement, la multiplication des résultats particuliers concernant les diviseurs des formes quadratiques et les nombres qu'elles sont susceptibles de représenter.

Notons d'ailleurs que l'on trouve, dans les pages précédentes, l'origine des termes mathématiques "forme quadratique" et "forme linéaire". Leur usage actuel, dans le champ de l'Algèbre Linéaire, ne peut nous masquer qu'ils proviennent bien de la notion pythagoricienne de représentation d'un nombre entier par des formes arithmo-géométriques particulières.

C'est cette matière première, faite de résultats divers, qui nourrira la réflexion des successeurs : Legendre, Gauss .

## § III - LA LOI DE RECIPROCITE ET LE SYMBOLE DE LEGENDRE

(9) Comme Euler l'avait vu sans pouvoir le démontrer, les propriétés particulières déjà obtenues relativement aux résidus quadratiques appelaient un théorème général. Voici un énoncé de ce théorème :

"Si $p$ et $q$ sont deux nombres premiers impairs, $p$ est résidu de $q$ si et seulement si $q$ est résidu de $p$, sauf lorsque $p$ et $q$ sont de la forme $4k + 3$, auquel cas $p$ sera résidu de $q$ si et seulement si $q$ n'est pas résidu de $p$ ".

Legendre a nommé cette proposition "Loi de réciprocité quadratique", sans doute pour marquer que ce résultat fort général recouvrait de multiples cas particuliers, sur lesquels il avait d'abord été vérifié. Cette loi sera considérée par Gauss comme le "joyau de l'Arithmétique"(cf. [JA1], p.314) .

A qui revient le mérite de son énoncé et de sa démonstration ? Gauss dira en 1808 (article "Theorematis arithmetici...", [GA2], p.4) :

"Pro primo huius elegantissimi theorematis inventore ill. Legendre absque dubio habendus est, postquam longe antea summi geometrae Euler et Lagrange plures eius casus speciales iam per intuotiorem detexerant" (*)

(10) Adrien-Marie Legendre (1752 - 1833) ...

... est parfois sous-estimé. On peut regretter que l'Encyclopaedia Universalis, par exemple, relègue dans son "Thesaurus" ce scientifique français. Pourtant, s'il n'a su manifester l'originalité et la profondeur de vues d'un Euler ou d'un Gauss, il mérite mieux que ce demi-oubli méprisant.

Doué d'opiniâtreté et d'une grande puissance de travail, il a abordé tous les domaines mathématiques, des plus spéculatifs (Théorème des Nombres) aux plus concrets (mécanique céleste, géodésie,...). Nous lui sommes redevables de maintes découvertes, telles que l'irrationnalité de $\pi^2$ , la méthode des moindres carrés, les "polynômes de Legendre", la formule de duplication de la fonction $\Gamma$ , etc. (cf. [CO2] pp.152-155 , [OC] pp.182-187).

Sa réputation a sans doute souffert de la comparaison avec des contemporains plus talentueux. Par exemple, il s'était attaqué dès 1786 à la théorie des fonctions elliptiques, et a publié en 1825 et 1826 un traité en deux volumes consacré à ce sujet. Mais juste après cette publication, Abel et Jacobi eurent l'idée d'inverser ces fonctions, ce qui lui avait échappé, et qui devait donner à cette question un nouvel essor. Legendre ajouta alors un troisième volume à son ouvrage, donnant par là une grande publicité à la découverte des deux jeunes chercheurs étrangers.

---

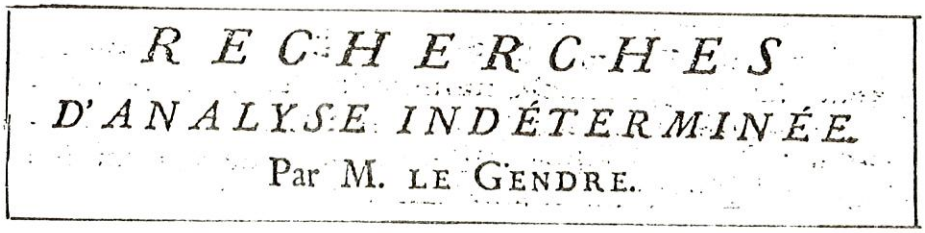
(*) "Le célèbre Legendre doit être considéré comme le premier qui ait découvert ce très élégant théorème après que, longtemps auparavant, les grands géomètres Euler et Lagrange en aient élucidé par induction plusieurs cas particuliers".

Ajoutons que Legendre fut un écrivain scientifique prolixe qui fit beaucoup pourla diffusion des connaissances mathématiques. On connaît le succès de ses "Eléments de géométrie" qui contiennent des idées originales et manifestent un réel talent pédagogique : ils eurent vingt éditions.

Dans le domaine qui nous occupe, il a publié en 1798 (AN VI de la République) un "Essai sur la théorie des nombres". C'était le premier traité jamais consacré à cette discipline, la première initiative visant à rassembler des résultats dispersés dans divers travaux de Diophante, Viète, Bachet, Fermat, Euler, Lagrange, et Legendre lui-même. Cet ouvrage eut une grande influence sur la culture mathématique de l'époque et connut un franc succès. Il fut réédité en 1808 puis en 1816. En 1830, l'auteur lui donna sa forme définitive, en deux volumes, sous le titre de "Théorie des Nombres". Chacune de ces rééditions a été remaniée et améliorée par rapport à la précédente.

(11) Le mémoire de 1785.

La première formulation et la première démonstration de la loi de réciprocité se trouve dansle mémoire de 1785 :


RECHERCHES
D'ANALYSE INDÉTERMINÉE.
Par M. LE GENDRE.

([LG1], p. 465.)

Conformément à son titre, ce travail concerne surtout les équations diophantiennes.

Il couvre 88 pages, plus 7 pages de tables numériques, et se divise en quatre articles, qui contiennent :

« 1.° Une méthode pour réſoudre en nombres entiers l'équation

$$Ay = ax^n + bx^{n-1} + cx^{n-2} + \text{\&c.}$$

2.° Une méthode fondée ſur l'analyſe indéterminée, pour trouver les diviſeurs des équations numériques.

3.° Un théorème pour juger de la poſſibilité ou de l'impoſſibilité d'une équation indéterminée du ſecond degré.

4.° Divers théorèmes relatifs aux nombres premiers. »

([LG1], p.465.)

A vrai dire, l'auteur ne parle pas de résidus quadratiques, mais des diviseurs premiers c de la "formule" $t^2 - du^2$, u et t étant premiers entre-eux, et c ne divisant pas d : comme nous l'avons vu (§ I, n°5), c'est bien la même chose. Dans son article I, il démontre que l'on a " $d^{\frac{c-1}{2}} = 1$ " (qu'il faut lire : $d^{\frac{c-1}{2}} \equiv 1 \pmod{c}$) si c divise $t^2 - du^2$ et " $d^{\frac{c-1}{2}} = -1$ " dans le cas contraire. C'est le "critère d'Euler".

L'article III ([LG1], p.507) est consacré à ce que l'on appelle encore de nos jours le théorème de Legendre ([LG1], p.513) :

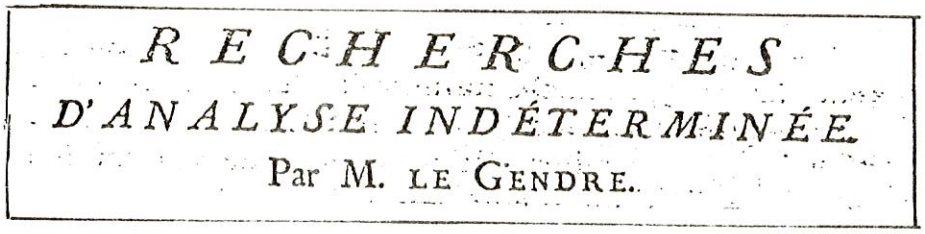
« *Étant propoſé l'équation* $ax^2 + by^2 = cz^2$, *dans laquelle* a, b, c *ſont poſitifs, premiers entr'eux, & dégagés de tout facteur carré, cette équation ſera réſoluble ſi on peut trouver trois entiers,* $\lambda, \mu, \nu$, *tels que les trois quantités* $\frac{a\lambda^2 + b}{c}$, $\frac{c\mu^2 - b}{a}$, $\frac{c\nu^2 - a}{b}$ *ſoient des entiers.* »

Ajoutons que Legendre fut un écrivain scientifique prolixe qui fit beaucoup pourla diffusion des connaissances mathématiques. On connaît le succès de ses "Eléments de géométrie" qui contiennent des idées originales et manifestent un réel talent pédagogique : ils eurent vingt éditions.

Dans le domaine qui nous occupe, il a publié en 1798 (AN VI de la République) un "Essai sur la théorie des nombres". C'était le premier traité jamais consacré à cette discipline, la première initiative visant à rassembler des résultats dispersés dans divers travaux de Diophante, Viète, Bachet, Fermat, Euler, Lagrange, et Legendre lui-même. Cet ouvrage eut une grande influence sur la culture mathématique de l'époque et connut un franc succès. Il fut réédité en 1808 puis en 1816. En 1830, l'auteur lui donna sa forme définitive, en deux volumes, sous le titre de "Théorie des Nombres". Chacune de ces rééditions a été remaniée et améliorée par rapport à la précédente.

(11) Le mémoire de 1785.

La première formulation et la première démonstration de la loi de réciprocité se trouve dansle mémoire de 1785 :


RECHERCHES
D'ANALYSE INDÉTERMINÉE.
Par M. LE GENDRE.

([LG1], p. 165.)

Conformément à son titre, ce travail concerne surtout les équations diophantiennes.

Il couvre 88 pages, plus 7 pages de tables numériques, et se divise en quatre articles, qui contiennent :

« 1.° Une méthode pour résoudre en nombres entiers l'équation

$$Ay = ax^n + bx^{n-1} + cx^{n-2} + \text{\&c.}$$

2.° Une méthode fondée sur l'analyse indéterminée, pour trouver les diviseurs des équations numériques.

3.° Un théorème pour juger de la possibilité ou de l'impossibilité d'une équation indéterminée du second degré.

4.° Divers théorèmes relatifs aux nombres premiers. »

([LG1], p.465.)

A vrai dire, l'auteur ne parle pas de résidus quadratiques, mais des diviseurs premiers c de la "formule" $t^2 - du^2$, u et t étant premiers entre-eux, et c ne divisant pas d : comme nous l'avons vu (§ I, n°5), c'est bien la même chose. Dans son article I, il démontre que l'on a " $d^{\frac{c-1}{2}} = 1$ " (qu'il faut lire : $d^{\frac{c-1}{2}} \equiv 1 \pmod{c}$) si c divise $t^2 - du^2$ et " $d^{\frac{c-1}{2}} = -1$ " dans le cas contraire. C'est le "critère d'Euler".

L'article III ([LG1], p.507) est consacré à ce que l'on appelle encore de nos jours le théorème de Legendre ([LG1], p.513) :

« *Étant proposé l'équation* $ax^2 + by^2 = cz^2$, *dans laquelle* a, b, c *sont positifs, premiers entr'eux, & dégagés de tout facteur carré, cette équation sera résoluble si on peut trouver trois entiers,* $\lambda$, $\mu$, $\nu$, *tels que les trois quantités* $\frac{a\lambda^2 + b}{c}$, $\frac{c\mu^2 - b}{a}$, $\frac{c\nu^2 - a}{b}$ *soient des entiers.* »

Et c'est enfin l'article IV qui présente la loi de réciprocité. L'auteur note A, a, α, A' etc. les nombres premiers de la forme 4k + 1 et B, b, β, B', ceux de la forme 4k - 1 . Avec ces notations, la loi est exprimée en huit théorèmes :

« THÉORÈME I.

Si $b^{\frac{a-1}{2}} = 1$, il s'enſuit $a^{\frac{b-1}{2}} = 1$.

THÉORÈME II.

Si $a^{\frac{b-1}{2}} = -1$, il s'enſuit $b^{\frac{a-1}{2}} = -1$.

THÉORÈME III.

Si $a^{\frac{A-1}{2}} = 1$, il s'enſuit $A^{\frac{a-1}{2}} = 1$.

THÉORÈME IV.

Si $a^{\frac{A-1}{2}} = -1$, il s'enſuit $A^{\frac{a-1}{2}} = -1$.

THÉORÈME V.

Si $a^{\frac{b-1}{2}} = 1$, il s'enſuit $b^{\frac{a-1}{2}} = 1$.

THÉORÈME VI.

Si $b^{\frac{a-1}{2}} = -1$, il s'enſuit $a^{\frac{b-1}{2}} = -1$.

THÉORÈME VII.

Si $b^{\frac{B-1}{2}} = 1$, il s'enſuit $B^{\frac{b-1}{2}} = -1$.

THÉORÈME VIII.

Si $b^{\frac{B-1}{2}} = -1$, il s'enſuit $B^{\frac{b-1}{2}} = 1$. »

Après quoi, Legendre précise :

« Ces Théorèmes ainſi détaillés, ſont encore d'une grande généralité, mais on auroit pu les comprendre tous dans l'énoncé ſuivant.

$\epsilon$ & $\partial$ étant deux nombres premiers, les expreſſions $\epsilon^{\frac{\partial-1}{2}}$, $\partial^{\frac{\epsilon-1}{2}}$ ne ſeront de différens ſignes que lorſque $\epsilon$ & $\partial$ ſeront tous deux de la forme $4n-1$ ; dans tous les autres cas, ces expreſſions auront toujours le même ſigne. »

La démonstration est assez longue, et commence ainsi :

« L'équation $Ax^2 + ay^2 = bz^2$ eſt impoſſible, & plus généralement l'équation $(4m+1)x^2 + (4n+1)y^2 = (4p-1)z^2$ : car le premier membre eſt toujours de l'une des formes $4n+1$ & $4n+2$, tandis que le ſecond ne peut être que de celles-ci $4n$ ou $4n-1$. Or, par le théorème de l'*article III*, nous ſavons que l'équation $Ax^2 + ay^2 = bz^2$ ſeroit réſoluble ſi on pouvoit ſatisfaire à la fois aux trois conditions

$$a^{\frac{A-1}{2}} b^{\frac{A-1}{2}} = 1, \quad A^{\frac{a-1}{2}} b^{\frac{a-1}{2}} = 1,$$

$$A^{\frac{b-1}{2}} a^{\frac{b-1}{2}} = -1 \ldots\ldots (2);$$

il faut donc que ces conditions ſoient incompatibles entr'elles.

Soit $A = 1$, la première condition aura lieu d'elle-même, & les deux autres ſeront

$$b^{\frac{a-1}{2}} = 1, \quad a^{\frac{b-1}{2}} = -1.$$

Donc, puiſqu'elles ne peuvent avoir lieu en même-temps,

1.° Si $b^{\frac{a-1}{2}} = 1$, on aura $a^{\frac{b-1}{2}} = 1$.

2.° Si $a^{\frac{b-1}{2}} = -1$, on aura $b^{\frac{a-1}{2}} = -1$.

D'ailleurs on voit que cette ſeconde propoſition eſt une ſuite de la première. »

On obtient donc les théorème I et II, et il n'y a rien à redire. Mais lorsque l'auteur veut aborder le théorème III, il est contraint de recourir à un nombre premier $b$ (i.e. de la forme $4k - 1$) diviseur de $x^2 + Ay^2$, c'est-à-dire dont $-A$ soit résidu. Or, rien ne lui permet d'affirmer qu'il existe effectivement un tel nombre $b$. De même, pour obtenir les théorèmes V et VI, il est amené à supposer qu'existe un nombre premier $A$ non-résidu de deux nombres premiers $a$ et $b$. Pour lui, cette existence est ainsi assurée : il lui suffit de prendre un entier $g$, non résidu de $a$ et de $b$, et de la forme $4k + 1$ : il existe un tel $g$. Dès lors, tout nombre premier $A$, appartenant à la progression arithmétique $\{g + 4abn/n \in N\}$, fera l'affaire. Mais voilà : y-a-t-il des nombres premiers dans cette progression ? Legendre pense qu'il y en a, et même une infinité.

Il est intéressant à ce propos de citer la remarque finale de ce mémoire ([LG1], p.552) :

« *Remarque.* Il ſeroit peut-être néceſſaire de démontrer rigoureuſement une choſe que nous avons ſuppoſée dans pluſieurs endroits de cet article, ſavoir, qu'il y a une infinité de nombres premiers compris dans toute progreſſion arithmétique, dont le premier terme & la raiſon ſont premiers entr'eux, ou, ce qui revient au même, dans la formule $2mx + \mu$, lorſque $2m$ & $\mu$ n'ont point de commun diviſeur. Cette propoſition eſt aſſez difficile à démontrer, cependant on peut s'aſſurer qu'elle eſt vraie, en comparant la progreſſion arithmétique dont il s'agit, à la progreſſion ordinaire 1, 3, 5, 7, &c. Si on prend un grand nombre de termes de ces progreſſions, le même dans les deux, & qu'on les diſpoſe, par exemple, de manière que le plus grand terme ſoit égal & à la même place de part & d'autre; on verra qu'en omettant de chaque côté les multiples de 3, 5, 7, &c. juſqu'à un certain nombre premier $p$, il doit reſter des deux côtés le même nombre de termes, ou même il en reſtera moins dans la progreſſion 1, 3, 5, 7, &c. Mais comme dans celle-ci, il reſte néceſſairement des nombres premiers, il en doit reſter auſſi dans l'autre. Je me contente d'indiquer ce moyen de démonſtration qu'il ſeroit trop long de détailler, d'autant plus que ce Mémoire paſſe déjà les bornes ordinaires. »

On peut regretter que cette longue et pénétrante étude se termine par ce que l'on pourrait appeler vulgairement "le coup de Fermat" ("Hanc marginis exignitas non caperet" - "la marge est trop étroite" : [FE1], p.291 ; [FE3], p.241). Si l'on en juge par certains passages, l'existence d'une infinité de nombres premiers dans la progression arithmétique ne faisait vraiement pas de doute, et Legendre pensait vraisemblablement que la démonstration ne serait pas malaisée. Par la suite, il a beaucoup travaillé cette question, a trouvé des résultats empiriques et formulé des conjectures intéressantes, mais il n'a pas réussi à conclure. C'est Lejeune-Dirichlet qui est parvenu à démontrer ce théorème en 1857, d'une manière tout à fait différente des tentatives de Legendre (cf. [LD1], p.313, article traduit en français dans le "Journal de Liouville" série I, tome IV, p.393).

(12) Gauss, critique de Legendre

Dans ses "Recherches Arithmétiques" (1801), Gauss rappelle et critique la démonstration de Legendre, en faisant observer que l'existence des nombres premiers auxiliaires utilisés n'est pas assurée ([GAD] N°151, pp.115-116 ; N°296, pp.359-361 ; N°297, pp.361-363 ; Additions, p.490). Gauss se demande aussi, s'il n'y aurait pas une pétition de principe dans la démonstration de Legendre, et si les suppositions arbitraires qui y sont posées peuvent vraiment se prouver sans faire intervenir la loi de réciprocité elle-même. Kummer a répondu à cette question en 1859 : il a indiqué que ces suppositions peuvent se déduire du théorème de Dirichlet. (cf. [SM], p.57, [KU], p.20). Comme dit HJS Smith : "It would follow from this, that the demonstration of Legendre (...) must be regarded as rigorously exact" (*).

---

(*) "Il s'ensuit que la démonstration de Legendre doit être considérée comme rigoureusement exacte" .

(13) Le symbole de Legendre.

Dans son "Essai sur la théorie des Nombres", de 1798 Legendre définit le symbole qui portera son nom (*) ([LG5], p.197, N°135) :

« *Comme les quantités analogues à* $N^{\frac{c-1}{2}}$ *se rencontreront fréquemment dans le cours de nos recherches, nous emploîrons le caractère abrégé* $\left(\frac{N}{c}\right)$ *pour exprimer le reste que donne* $N^{\frac{c-1}{2}}$ *divisée par* c; *reste qui, suivant ce qu'on vient de voir, ne peut être que* $+1$ *ou* $-1$.

Lorsque $\left(\frac{N}{c}\right) = +1$, on dit que N est un *résidu carré* de $c$, parce qu'alors $N^{\frac{c-1}{2}}$ divisé par $c$, laisse le reste $+1$, ce qui est la condition nécessaire pour que $c$ soit diviseur de $x^2 - N$; au contraire, lorsque $\left(\frac{N}{c}\right) = -1$, on dit que N est un *non-résidu carré* de $c$. »

Il précise que N est un nombre quelconque et c un nombre premier impair. La première propriété de ce symbole est celle qui en fait un caractère : $\left(\frac{MN}{c}\right) = \left(\frac{M}{c}\right)\left(\frac{N}{c}\right)$ .

---

(*) C'est bien à 1798 que remonte l'introduction de ce symbole, et non à 1808 comme l'affirment Morris Kline ([MK], p.811) et Collette ([CO2], p.154) .

Avec ce symbole, la loi de réciprocité prend la forme suivante :

« Quels que soient les nombres premiers $m$ et $n$, s'ils ne sont pas « tous deux de la forme $4x+3$, on aura toujours $\left(\frac{n}{m}\right)=\left(\frac{m}{n}\right)$, et « s'ils sont tous deux de la forme $4x+3$, on aura $\left(\frac{n}{m}\right)=-\left(\frac{m}{n}\right)$. « Ces deux cas généraux sont compris dans la formule

$$\left(\frac{n}{m}\right)=(-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}\cdot\left(\frac{m}{n}\right).\ »$$ ([LGS], p.230.)

Ce qui s'écrit aussi : $\left(\frac{n}{m}\right)\left(\frac{m}{n}\right)=(-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}$ . (*)

Mais la démonstration ne présente pas d'amélioration par rapport à celle de 1785. Des considérations sur les nombres premiers contenus dans certaines progressions arithmétiques témoignent des efforts que fait l'auteur pour compléter sa démonstration. Vains efforts, comme l'on sait.

Nous avons vu au § II que les résultats de Fermat-Euler-Lagrange relatifs aux formes quadratiques $x^2 + y^2$ et $x^2 - 2y^2$ élucident complètement la question du caractère quadratique de -1 et 2 :

p étant premier impair, on a $\left(\frac{-1}{p}\right) = 1$ si $p = 4k + 1$ et $\left(\frac{-1}{p}\right) = -1$ si $p = 4k - 1$ ; on a $\left(\frac{2}{p}\right) = 1$ si $p = 8k + 1$ ou $8k + 7$, et $\left(\frac{2}{p}\right) = -1$ si $p = 8k + 3$ ou $8k + 5$. Ce qui peut (si l'on veut) se traduire ainsi :

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \quad ; \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

---

(*) On peut donc observer une erreur dans la notice "Legendre" de l'"Encyclopaedia Universalis" .

(14) Premières applications.

Dans son mémoire de 1785, Legendre s'empresse de montrer que la loi de réciprocité permet de retrouver les propositions de Lagrange et Euler concernant les diviseurs des formes quadratiques.

Si nous cherchons par exemple les diviseurs premiers $p$ de $x^2 + 5y^2$, cela revient à chercher les $p$ dont $-5$ est résidu, c'est-à-dire tels que $\left(\frac{-5}{p}\right) = 1$, ou encore $\left(\frac{5}{p}\right) = (-1)^{\frac{p-1}{2}}$. D'après la loi de réciprocité, on a $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = (-1)^{\frac{(p-1)(5-1)}{4}} = 1$.

Et notre problème devient : trouver les nombres premiers impairs $p$ tels que $\left(\frac{p}{5}\right) = (-1)^{\frac{p-1}{2}}$. Il faut alors distinguer deux cas : si $p$ est de la forme $4k + 1$, nous devons avoir $\left(\frac{p}{5}\right) = 1$, d'où $p \equiv 1$ (mod. 5) ou $p \equiv 4$ (mod. 5), puisque 1 et 4 sont les résidus quadratiques non nuls de 5. Les diviseurs $p$ convenables sont de la forme $20k + 1$ ou $20k + 9$ ; si $p$ est de la forme $4k - 1$, il faut que $\left(\frac{p}{5}\right) = -1$, d'où $p \equiv 2$ ou $p \equiv 3$ (mod. 5) : résultat, $p = 20k + 7$ ou $p = 20k + 3$.

Dans sa "Théorie des Nombres", Legendre présente l'aspect algorithmique de sa loi et de son symbole, la loi permettant de calculer $\left(\frac{a}{p}\right)$ même pour des valeurs considérables de $a$ et $p$. Si nous cherchons par exemple à déterminer $\left(\frac{888}{1999}\right)$, nous écrivons :

$$\left(\frac{888}{1999}\right) = \left(\frac{2}{1999}\right)\left(\frac{4}{1999}\right)\left(\frac{3}{1999}\right)\left(\frac{37}{1999}\right).$$

On a $\left(\frac{4}{1999}\right) = 1$ parce que 4 est un carré, et $\left(\frac{2}{1999}\right) = 1$ parce que $1999 \equiv 7$ (mod. 8). Pour calculer $\left(\frac{3}{1999}\right)$ et $\left(\frac{37}{1999}\right)$, on utilise la loi de réciprocité :

on écrit que $\left(\frac{3}{1999}\right) = (-1)^{\frac{1998 \times 2}{4}} \left(\frac{1999}{3}\right) = -\left(\frac{1999}{3}\right)$. Et l'on applique alors une propriété que Legendre n'énonce pas, mais utilise, sans doute parce qu'elle lui paraît évidente : c'est que $a \equiv a'$ (mod. $p$) implique $\left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right)$. Le reste de 1999 par 3 étant

1, on a : $\left(\frac{1999}{3}\right) = \left(\frac{1}{3}\right) = 1$ .

On traite de même $\left(\frac{37}{1999}\right)$ , que l'on trouve égal à 1 .

Le regroupement de tous ces résultats nous donne $\left(\frac{888}{1999}\right) = -1$ : 888 n'est pas résidu quadratique de 1999 .

(15) Généralisation de Jacobi.

Pour faciliter l'exposé de la suite, nous citerons ici par anticipation la généralisation du symbole de Legendre, que Jacobi a présentée dans une note à l'Académie de Berlin en Octobre 1837 ([SM], p.58 ; [JA2], p.262 ; J. de Crelle, tome 30, p.166). Si $a$ désigne un entier rationnel quelconque et $P$ un nombre impair plus grand que 1 , premier avec $a$ , si $P = p_1 p_2 \ldots p_n$ est la décomposition de $P$ en produit de facteurs premiers (égaux ou inégaux), Jacobi pose :

$$\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\ldots\left(\frac{a}{p_n}\right) .$$

Il est clair que, si $a$ est résidu quadratique de $P$ , il est résidu de $p_1, p_2, \ldots, p_n$ , de sorte que l'on a : $\left(\frac{a}{p_1}\right) = \left(\frac{a}{p_2}\right) = \ldots = \left(\frac{a}{p_n}\right) = 1$ , et $\left(\frac{a}{P}\right) = 1$ . Mais évidemment, cette condition nécessaire n'est pas suffisante puisque $\left(\frac{a}{P}\right)$ est égal à 1 dès qu'un nombre pair des $\left(\frac{a}{p_i}\right)$ est égal à -1 . C'est dire que $\left(\frac{a}{P}\right) = 1$ est une condition nécessaire, mais non suffisante, pour que $a$ soit résidu quadratique de $P$ .

Ce symbole vérifie encore les propriétés suivantes :

$\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}$ , $\left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}$ et surtout

$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{1}{4}(P-1)(Q-1)}$ pour $P$ et $Q$ impairs, plus grands que 1, premiers entre eux . Et, bien sûr, $\left(\frac{a}{P}\right)\left(\frac{a'}{P}\right)$ lorsque $a \equiv a' \pmod{P}$ ; ainsi que : $\left(\frac{a}{P}\right)\left(\frac{b}{P}\right) = \left(\frac{ab}{P}\right)$ , $\left(\frac{a}{P}\right)\left(\frac{a}{Q}\right) = \left(\frac{a}{PQ}\right)$.

Ce symbole est d'abord utile pour faciliter la recherche pratique de la valeur du symbole de Legendre, avec lequel il se confond lorsque P est premier. Pour reprendre l'exemple du paragraphe précédent, on a : $\left(\frac{888}{1999}\right) = \left(\frac{2}{1999}\right)\left(\frac{4}{1999}\right)\left(\frac{111}{1999}\right) = \left(\frac{111}{1999}\right)$ $= (-1)^{\frac{110 \times 1998}{4}} \left(\frac{1999}{111}\right) = -\left(\frac{1999}{111}\right) = -\left(\frac{1}{111}\right) = -1$ . Si l'on veut calculer $\left(\frac{a}{p}\right)$ , il n'est plus nécessaire de décomposer l'entier a en produit de facteurs premiers, mais seulement de le mettre sous la forme : $a = 2^n (2m + 1)$ .

C'est cette considération qui a inspiré le programme que l'on trouvera ci-après, et qui permet de déterminer $\left(\frac{a}{p}\right)$ à l'aide d'une calculatrice de proche programmable.

Notons qu'Eisenstein a publié en 1844 un bref article présentant un procédé de calcul de $\left(\frac{a}{b}\right)$ , qui paraît de prime abord fort séduisant par son caractère régulier et automatique ([EI1]; [SI], p.329) . Mais cet algorithme se révèle, à l'usage, trop long d'exécution lorsque a et b sont voisins l'un de l'autre, ou lorsque l'on tombe sur deux nombres voisins au cours du calcul. V.A. Lebesgue(*) s'est livré à une étude comparative de plusieurs algorithmes ([LB]) et conclut que le plus efficace est celui qui s'appuie sur les principes décrits ci-dessus.

(16) Un algorithme pour calculer $\left(\frac{P}{Q}\right)$.

On peut tirer des considérations précédentes un algorithme permettant de déterminer $\left(\frac{P}{Q}\right)$ , où P et Q sont des entiers rationnels premiers entre-eux, Q étant positif impair.

Principe de la méthode :

1 - On pose $\left(\frac{P}{Q}\right) = (-1)^S$ et on comptabilise S dans une mémoire. Dans le cas où $P < o$ , on change P en -P et on applique la formule : $\left(\frac{P}{Q}\right) = (-1)^{(Q-1)/2} \left(\frac{P}{Q}\right)$ , c'est-à-dire qu'on ajoute

(*) Victor-Amédée Lebesgue (1791 - 1875) : mathématicien français, auteur de nombreuses publications concernant la Théorie des Nombres. Son souvenir souffre peut être de l'homonymie avec Henri Lebesgue (1875 - 1951).

$\frac{Q - 1}{2}$ dans la mémoire S . On se ramène ainsi au cas où $P > 0$.

2 - On remplace ensuite l'entier P par son reste par Q : on se ramène au cas où $0 < P < Q$ .

3 - On met ensuite P sous la forme $P = 2^n(2m + 1)$. On détermine n et, s'il est impair :

4 - on applique la formule : $\left(\frac{2}{Q}\right) = (-1)^{(Q^2 - 1)/8}$ : on ajoute $\frac{Q^2 - 1}{8}$ dans la mémoire S .

5 - On remplace alors P par $2m + 1$, et on est ramené au calcul de $\left(\frac{P}{Q}\right)$ avec $0 < P < Q$ , P et Q impairs premiers entre-eux. C'est le moment d'appliquer la loi de réciprocité, donc de remplacer P par Q et Q par P , quitte à incrémenter S de $\frac{(P - 1)(Q - 1)}{4}$ . Et l'on repart à l'étape 2, avec une valeur de Q strictement inférieure à ce qu'elle était. On s'arrête lorsque $P = 1$, et alors :

6 - on calcule $(-1)^S$ .

Comme seule importe la valeur de $(-1)^S$ , c'est à la parité de S que l'on s'intéresse. A chaque étape du calcul, on peut remplacer S par son reste par 2 , pour éviter de manipuler de trop grands nombres.

Réalisation sur calculatrice de poche HP 29 C

Les six labels (LBL1, LBL2, ... LBL6) correspondent aux six étapes ci-dessus décrites, et S est comptabilisé dans le registre-mémoire $R_3$ .

feuille illisible



| | |
|---|---|
| gLBL 1 | |
| 0 | $P \leftarrow R_1$ |
| STO 3 | $Q \leftarrow R_2$ |
| R ↓ | $0 \leftarrow R_3$ |
| STO 2 | Stockage de P dans le registre $R_1$, de Q dans le registre $R_2$, mise à 0 du registre $R_3$ |
| R ↓ | |
| STO 1 | |

| | |
|---|---|
| g x > 0 ? | |
| GTO 2 | Si P > 0, aller au label 2 |
| CHS | |
| STO 1 | Si P < 0, |
| RCL 2 | remplacement de P |
| 1 | par -P |
| - | |
| 4 | Addition, |
| ÷ | dans $R_3$, de |
| g FRAC | $\frac{Q-1}{2}$ (mod. 2) |
| 2 | |
| x | |
| STO + 3 | |

| | |
|---|---|
| g LBL 2 | |
| Q | |
| STO 0 | Calcul du |
| RCL L | reste de P |
| RCL 1 | par Q. et |
| RCL 2 | remplacement |
| ÷ | de P par ce |
| F INT | reste |
| RCL 2 | |
| x | |
| - | |
| STO 1 | |

| | |
|---|---|
| g LBL 3 | Calcul de n tel |
| RCL 1 | que $P = 2^n(2m+1)$, |
| Σ | dans $R_0$. Remplace- |
| ÷ | ment de P par |
| ENTER ↑ | 2m + 1. |
| f INT | |
| f x≠y ? | |
| GTO 4 | |
| STO 1 | |
| ISZ | |
| GTO 3 | |

| | |
|---|---|
| g LBL 4 | |
| RCL 0 | |
| 2 | |
| ÷ | |
| g FRAC | |
| g x = 0? | |
| GTO 5 | si n pair, aller au label 5 |
| RCL 2 | |
| 8 | si n est impair, |
| ÷ | addition, dans |
| FRAC | $R_3$ de $\frac{Q^2-1}{8}$ |
| 8 | (mod 2) |
| x | |
| 1 | |
| - | |
| 8 | |
| ÷ | |
| STO + 3 | |

| | |
|---|---|
| g LBL 5 | |
| RCL 1 | |
| RCL 1 | |
| 1 | |
| - | |
| gx = 0 ? | |
| GTO | Si P = 1 aller |
| 4 | au label 6 |
| ÷ | Si P > 1, |
| g FRAC | application de |
| RCL 2 | la loi de ré- |
| STO 1 | ciprocité et |
| 1 | retour à l'é- |
| - | tape n° 2 |
| x | |
| STO +3 | |
| x ↔ y | |
| STO 2 | |
| GTO 2 | |

| | |
|---|---|
| g LBL 6 | |
| 1 | |
| RCL | |
| 2 | Calculer $(-1)^S$ |
| g FRAC | |
| 4 | |
| : | |
| x | |
| - | |
| g RTN | |

Ce programme s'exécute en tapant : P ↑ Q GSB 1 . On constate que beaucoup d'instructions sont consacrées à remplacer les nombres ajoutés dans $R_3$ par des nombres de même parité, mais plus petits. Une machine permettant d'obtenir le reste d'une division euclidienne à l'aide d'une simple touche (telle que MOD sur la HP 41C) fournirait un programme plus court. Celui-ci convient pour des nombres P et Q inférieurs à $8.10^8$. On peut l'utiliser notamment pour taiter les exemples donnés par Legendre et Gauss :

$$\left(\frac{601}{1013}\right) = -1 \qquad ([LG2], \text{ p.245}),$$

$$\left(\frac{-1459}{22\ 366\ 891}\right) = 1 \qquad ([LG2], \text{ p.246}),$$

$$\left(\frac{-1365}{5\ 428\ 681}\right) = 1 \qquad ([GAD], \text{ p.414}).$$

La machine donne le résultat en 20 s (environ) pour les deux premiers exemples et en 15 s pour le troisième.

## § IV - LES " RECHERCHES ARITHMETIQUES " de GAUSS

### (17) Gauss et les "Disquisitiones Arithmeticae"

Il n'est certes pas utile de présenter ici Carl Friedrich Gauss (1777 - 1855) que l'on a désigné comme "le prince des mathématiciens" pour bien marquer le rôle hors de pair qu'il a joué à la tête de toutes les mathématiques, pendant le premier tiers du dix-neuvième siècle.

En 1795, âgé de 18 ans, il se lance dans l'étude de la Théorie des Nombres, dans des conditions qu'il décrit lui-même en ces termes :

"Occupé dans ce temps d'une autre matière, je tombai par hasard sur une vérité importante de l'Arithmétique". (C'était le "critère d'Euler"). "Comme elle me sembla très-belle par elle-même et que je la soupçonnais liée à d'autres plus importantes, j'employai toute la contention d'esprit dont j'étais susceptible, à découvrir les

principes sur lesquels elle s'appuyait, et à en trouver une démonstration rigoureuse ; le succès ayant répondu à mes voeux, je me sentis tellement entraîné par l'attrait de ces questions, qu'il me fut impossible de les abandonner (...)" ([GAD], p.xiii).

Et c'est ainsi que sont nées les "Disquisitiones Arithmeticae" ("Recherches Arithmétiques") parues seulement en 1801 par suite de difficultés d'édition.

Gauss raconte aussi ([GAD], p. xiii) qu'il s'est engagé dans ces recherches sans aucune connaissance des travaux des autres mathématiciens, anciens ou modernes. C'est pourquoi cet ouvrage, contrairement à la "Théorie des Nombres" de Legendre, prend les choses au début, consacrant par exemple les deux premières sections aux congruences du premier degré en particulier, ce qui aura déjà l'intérêt de fixer les notations (cf.[CC]).

Il traite ensuite des résidus des puissances, et consacre toute la quatrième section aux résidus quadratiques. Et là, il donna enfin une démonstration complète de la loi de réciprocité.

(18) La première démonstration de Gauss : "homogène", mais "illisible".

Cette première démonstration couvre les articles 131 à 145, pages 96 à 108 de l'édition française des "Disquisitions" ([GAD]). D'après les notes manuscrites de l'auteur, il a découvert la loi de réciprocité en mars 1795, et la ([GA1], p.476) démonstration en avril 1796. Exactement, le 8 avril 1796, juste avant son dix-neuvième anniversaire. Il lui attribuera une place à part pour son "homogénéité" :

(*) "Sed annes hae demonstrationes (...) e principiis heterogeneis derivatae sunt, prima forsam excepta" ([GA2], p.4).

Qu'est-ce à dire ? Que Gauss a d'abord étudié de nombreux cas particuliers : les articles 108 à 124 sont consacrés à l'étude des résidus -1, 2, -2, 3, -3, 5, -5, 7 et -7. De ces observations, il a conclu "par induction" à une loi générale. Par induction, c'est-à-dire en généralisant les observations portant sur ces divers cas. Cette proposition générale, il ne l'appelle d'ailleurs pas "loi de réciprocité

(*) "Mais toutes ces démonstrations (...) sont dérivées de principes trop hétérogènes, sauf peut être la première" .

quadratique", mais "théorème général" ou "fondamental", et il l'énonce ainsi :

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

Et pour démontrer ce théorème, il ne recourt à aucune considération qui puisse paraître éloignée de son objet : puisque l'on traite de nombres entiers, il le démontrera par récurrence, par cette méthode qui s'applique essentiellement aux entiers naturels. C'est en cela que consiste l'homogénéité de sa démonstration, par opposition à des démonstrations ultérieures qui, nous le verrons, utilisent des nombres complexes, des fonctions trigonométriques, etc.

De plus, les notions mises en oeuvre dans cette démonstration sont uniquement celles qui interviennent dans l'énoncé du théorème, comme le dit Lejeune-Dirichlet dans un article de 1857 ([LD3]) :

"Cette démonstration est la seule, que je sache, où l'on emprunte toutes les considérations à la doctrine des congruences du second degré, à laquelle appartient essentiellement ce théorème ; tandis que les principes fondamentaux des autres démonstrations semblent être plus ou moins étrangers à cette doctrine".

Pourtant, cette démonstration a mauvaise réputation : M. Ellison la dit "illisible" ([DD1], p.176) et H.J.S. Smith (*) la qualifie ainsi : "repulsive to any but the most laborious students" ([SM], p.59), c'est-à-dire "rebutante pour quiconque, sauf pour les étudiants les plus studieux". Gauss lui-même a écrit qu'elle "avance au moyen de calculs trop laborieux". (cf. infra, § V, n°21). Une étude directe montre que ces jugements sont fondés. Mais quelle en est la cause ? On peut lire la réponse dans un article de Lejeune-Dirichlet de 1857 ([LD3]), qui attribue la difficulté de cette démonstration à une "circonstance accidentelle" :

---

(*) Henry John Smith (1826-1883) : mathématicien anglais, auteur d'un "Rapport sur la théorie des nombres" présenté à l'Association Britannique pour l'avancement des sciences, en six parties, de 1859 à 1865. C'est un bilan très riche et précis des progrès de cette discipline mathématique au 19e siècle. Jordan a salué ce rapport comme "le monument le plus complet (...) qui ait jamais été élevé à la Théorie des Nombres" (1883).

"pour représenter certaines relations qui reviennent à chaque instant dans cette manière de procéder, on n'a employé aucun signe approprié au calcul, ce qui a mais dans la nécessité de distinguer huit cas différents, dont chacun se partage encore en plusieurs subdivisions. En introduisant le signe dont Legendre a le premier fait usage, avec la signification plus générale que Jacobi lui a donnée depuis (...), celle-ci se trouve réduite (...)."

En effet, Gauss n'utilise jamais le symbole de Legendre, d'abord parce qu'il a engagé ses recherches sans connaître les publications du mathématicien français et par la suite, sans doute, parce qu'il n'a pas daigné y faire un emprunt. Il se borne à noter " a R p " l'affirmation " a est résidu quadratique de p " et " a N p " l'affirmation contraire. C'est une notation plus proche du langage parlé, mais bien moins opératoire que le symbole de Legendre. Dans son étude, Dirichlet montre bien tout le profit que l'on peut tirer de ce symbole.

(19) L'étude de Dirichlet.

Dirichlet rappelle les propriétés du symbole de Legendre-Jacobi (voir ci-dessus, n°s 13 et 15), et la première démonstration de Gauss se présente ainsi : on constate d'abord que $\left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = -1$, ce qui montre que 3 et 5 satisfont à la loi de réciprocité :

$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\,\frac{q-1}{2}}$. On suppose cette loi vérifiée pour tous les nombres premiers impairs strictement inférieurs à un certain nombre premier impair $q$. On aura alors :

$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\,\frac{Q-1}{2}}$ pour toutes les paires d'entiers impairs $P$ et $Q$ premiers entre-eux, et ayant leurs diviseurs premiers tous $< q$. Et l'on démontre que la loi de réciprocité est encore vérifiée pour $q$ (et pour un autre nombre premier impair $p < q$), en distinguant seulement trois cas.

Premier cas : $\left(\frac{p}{q}\right) = 1$. Il existe alors deux entiers $e$ et $f$ tels que $e^2 - p = q\,f$. On peut prendre $e$ positif, pair, inférieur à $q$.

Dès lors, $f$ est impair, positif, inférieur à $q$ .

Si $p$ ne divise pas $f$ , la relation $e^2 - p = q f$ implique $\left(\frac{p}{f}\right) = 1$ et $\left(\frac{qf}{p}\right) = 1$ . Et d'après l'hypothèse de récurrence, on a :

$\left(\frac{p}{f}\right)\left(\frac{f}{p}\right) = (-1)^{\frac{1}{4}(p-1)(f-1)}$ parce que $p < q$ et $f < q$ , et ceci entraîne : $\left(\frac{f}{p}\right) = (-1)^{\frac{1}{4}(p-1)(f-1)}$ .

Par suite, $\left(\frac{q}{p}\right) = \left(\frac{qf}{p}\right)\left(\frac{f}{p}\right) = (-1)^{\frac{1}{4}(p-1)(f-1)}$ . Il n'est pas difficile de montrer enfin que les entiers $\frac{1}{4}(p-1)(q-1)$ et $\frac{1}{4}(p-1)(f-1)$ ont même parité, ce qui achève la démonstration.

Si $p$ divise $f$ , le raisonnement se déroule de même, à ceci près qu'il utilise la propriété : $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ .

Deuxième cas : $\left(\frac{p}{q}\right) = -1$ et $q \equiv 3 \pmod 4$. On écrit alors $\left(\frac{-p}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{p}{q}\right) = 1$ , ce qui indique que $-p$ est résidu quadratique de $q$ , et qu'il existe donc des entiers $e$ et $f$ tels que $e^2 + p = q f$ . Le reste de la démonstration diffère peu du premier cas.

Troisième cas : $\left(\frac{p}{q}\right) = -1$ et $q \equiv 1 \pmod 4$. Ici, est nécessaire en lemme que Gauss énonce au n°125 des "Disquisitiones" ([GAD], p.91), et démonstre sur le champ : "tout nombre premier de la forme $4n + 1$, soit positif, soit négatif, est non-résidu de quelques nombres premiers, et même de nombres premiers plus petits que lui."

Il faut entendre, bien sûr, que ces nombres premiers sont impairs.

Soit donc un nombre premier $p'$ plus petit que $q$, et tel que $\left(\frac{q}{p'}\right) = -1$ . Il est clair qu'alors on a $\left(\frac{p'}{q}\right) = -1$ car si l'on supposait $\left(\frac{p'}{q}\right) = 1$, on retomberait dans le "premiers cas" envisagé ci-

dessus, et l'on concluerait $\left(\frac{q}{p'}\right) = \left(\frac{p'}{q}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = +1$, ce qui n'est pas. En conséquence, on a : $\left(\frac{pp'}{q}\right) = \left(\frac{p}{q}\right)\left(\frac{p'}{q}\right) = 1$, et il existe $e$ et $f$ tels que $e^2 - pp' = qf$. La suite se traite comme dans le "premier cas", en distinguant trois "sous-cas", selon la divisibilité de $f$ par $p$ ou $p'$. Et la loi de réciprocité est ainsi complètement établie.

Cette démonstration a été exposée par H.J.S. Smith dans son "Rapport sur la Théorie des Nombres" ([SM], p.59), par G.B. Mathews, dans sa "Number theory" parue en 1892 ([MA], p.45), et par B.A. Venkov ([VE], p.72). Elle a encore été perfectionnée par L. Carlitz qui, dans un article de 1960 ([CR]), en donne une version fort rapide.

Il est curieux de constater que les principes de la première démonstration de Gauss ont été repris récemment, dans le cadre de la K-théorie, pour démontrer que le groupe $K_2\mathbb{Q}$ est isomorphe à la somme directe $A_2 \oplus A_3 \oplus A_5 \oplus \ldots$, où $A_2$ est le groupe $\{1, -1\}$ et où $A_p$ est le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$ pour $p$ premier impair (cf. [MI], p.101).

(20) La seconde démonstration de Gauss.

Nous avons vu que Gauss s'était lancé dans la rédaction de ses "Recherches Arithmétiques" sans qu'il ait rien connu des travaux des autres mathématiciens sur ce sujet. Mais ensuite, il a étudié leurs publications, ce qu'attestent les nombreuses références contenues dans cet ouvrage. Et voici sa réaction :

" ... animé d'une nouvelle ardeur, je m'efforçai en suivant leurs pas, de cultiver plus avant le champ de l'Arithmétique, et telle a été l'origine des Sections V, VI et VII".

Et en effet, si la première démonstration dont nous venons de parler était un tour de force, les sections V et VII constituent un apport fondamental et original, qui fait faire un bond en avant aux mathématiques. En particulier, la section V a pour objet la classification des formes quadratiques binaires à coefficients entiers rationnels.

Gauss considère comme équivalentes deux formes qui se déduisent l'une de l'autre par une transformation linéaire de déterminant $\pm 1$ et s'intéresse aux classes de cette équivalence, qu'il représente par des formes réduites. Selon les déterminants et les nombres qu'elles sont susceptibles de représenter ces classes de formes se répartissent en genres.

Toute cette théorie est construite avec une grande minutie, et une profusion de définitions et de théorèmes que nous ne saurions reproduire ici. On peut en trouver un exposé accessible dans [SM], pp.169 sq, [MA], pp.57 sp, [VE], pp.99 sp.

Signalons que Lejeune-Dirichlet a repris ces question dans son article de 1839 : "Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres". ([LD1], p.411) article dans lequel il retrouve, par ses méthodes analytiques, plusieurs résultats de Gauss et en établit de nouveaux.

Dans le cadre de cette Section, la loi de réciprocité apparaît comme un petit corollaire. En effet, le déterminant de la forme $ax^2 + 2by + cy^2$ est $b^2 - ac$. Dire que $p$ est résidu quadratique de $q$, c'est dire qu'il existe $b$ et $c$ tels que $p = b^2 - qc$, donc une forme quadratique $qx^2 + 2bxy + cy^2$ de déterminant $p$. Le lien étant ainsi fait entre les deux notions, les théorèmes généraux de la Section V suffisent à établir la loi : c'est l'objet de l'article 262, p.296 (voir aussi [SM], p.252, [MA], p.176).

Ajoutons que la théorie de Gauss des formes quadratiques a été fort développée depuis et a donné lieu à maints problèmes dont certains ne sont encore pas résolus aujourd'hui (cf. [DD1], p.181 et [DK3]).

## § V - DEUX DEMONSTRATIONS "NATURELLES" de GAUSS

### (21) Le mémoire de janvier 1808.

Gauss ne se satisfait pas de ses deux premières démonstrations d'un théorème qui continue à s'imposer à sa réflexion. En janvier 1808, il publie un mémoire intitulé "Theorematis arithmetici-demonstratio

nova" ("démonstration nouvelle d'un théorème arithmétique"), (|GA2|, p.1) que nous croyons inédit en français.

En voici l'article 1, qui comporte d'intéressantes réflexions sur la théorie des nombres :

" Les questions d'arithmétique supérieure présentent souvent un singulier phénomène, qui advient beaucoup plus rarement dans l'analyse, et contribue beaucoup à en augmenter le charme.

Car on ne peut, dans les recherches analytiques, atteindre des vérités neuves sans s'être d'abord assuré des principes sur lesquels elles s'appuient et qui doivent en quelque sorte nous frayer une voie jusqu'à elles : au contraire, en arithmétique, c'est très souvent par induction, sous l'effet d'un hasard heureux et inattendu, que jaillissent des vérités nouvelles et très élégantes, dont les démonstrations sont si profondément cachées et entourées de si épaisses ténèbres qu'elles se raillent de tous nos efforts et dérobent leur approche aux plus fins examens. En outre, l'enchaînement entre les vérités mathématiques est si grand et si étonnant, en dépit de leur apparente hétérogénéité, que souvent quand nous cherchons tout à fait autre chose, nous parvenons très heureusement, par une tout autre voie que nous ne nous y attendions, à la démonstration tellement souhaitée et cherchée en vain au cours de longues méditations antérieures. La plupart du temps, les vérités de cet ordre sont telles que l'on peut les atteindre par des chemins tout à fait divers, et que les voies les plus courtes ne sont pas toujours celles qui s'offrent de prime abord. C'est pourquoi l'on devra juger à coup sûr d'un grand prix le fait de parvenir à découvrir une démonstration très simple et naturelle pour une vérité longtemps débattue en vain, puis démontrée, mais au moyen de détours trop obscurs". ([GA2], p.3).

Et l'article 2 apporte quelques lueurs sur le travail que Gauss a consacré à démontrer la loi de réciprocité :

" Parmi les questions dont nous avons parlé à l'article précédent, un théorème tient une place prépondérante : c'est celui qui concerne presque toute la théorie des résidus quadratiques, et qui est appelé théorème fondamental dans les Recherches arithmétiques (Section IV). Le célèbre Legendre doit être considéré comme le premier qui ait découvert ce très élégant théorème après que, longtemps auparavant, les grands géomètres Euler et Lagrange en aient élucidé par induction plusieurs cas particuliers.

Je ne m'attarderai pas ici à énumérer les efforts de ces hommes autour de cette démonstration ; je laisse cela à ceux qui prennent plaisir au simple rappel des ouvrages. Qu'il me soit seulement permis d'ajouter, pour étayer leurs dires, que ce qui est cité à l'article précédent revient à mes efforts. J'étais arrivé à ce théorème par mes propres forces en 1795, alors que j'étais tout à fait ignorant de ce qui avait été déjà trouvé en arithmétique supérieure, et que j'étais totalement coupé de toute aide livresque ; mais ce théorème me tortura pendant une année entières, échappa à tous mes efforts, jusqu'à ce qu'enfin je rencontrasse la démonstration qui est rapportée dans la Section IV de l'ouvrage cité plus haut. Ensuite, trois autres démonstrations, qui s'appuyaient sur des principes tout à fait différents, s'offrirent à moi ; j'en ai rapporté une dans la Section V, et je ferai le public juge des autres, qui ne lui sont pas inférieures en élégance, en une autre occasion. Mais toutes ces démonstrations, si elles semblent ne rien laisser à désirer sur le plan de la rigueur, sont dérivées de principes trop hétérogènes, sauf peut être la première, et même celle-ci, qui avance au moyen de calculs trop laborieux, est étouffée par un trop grand nombre d'opérations. C'est pourquoi je n'hésite pas à dire qu'une démonstration naturelle a jusqu'ici manqué : aux gens compétents de décider si la démonstration qu'il m'a été donné de découvrir récemment, et qu'exposent les pages suivantes, mérite d'être honorée de ce nom" ([GA2], p.4).

(22) Le lemme de Gauss

Ces "pages suivantes" présentent d'abord la démonstration d'une proposition comme encore de nos jours sous le nom de "lemme de Gauss", qu'il énonce ainsi :

" Soit p un nombre premier positif ; soit q un entier quelconque non divisible par p ; soit A l'ensemble des nombres (complexus numerorum) 1, 2, 3, .... $\frac{1}{2}$ (p-1) et B l'ensemble des nombres $\frac{1}{2}$ (p+1), $\frac{1}{2}$ (p+3), $\frac{1}{2}$ (p+5), ... p-1 . Prenons les restes positifs des produits par q des nombres de A , qui sont manifestement tous distincts, et qui appartiennent, soit à A , soit à B. Alors, si l'on suppose que m restes appartiennent à B, q est résidu ou non-résidu quadratique de p selon que m est pair ou impair". (*)

(*) Il est sous-entendu que p n'est pas égal à 2.

En d'autres termes, si l'on considère les restes des divisions par $p$ des nombres $q, 2q, 3q, \ldots \frac{p-1}{2} q$ et si, parmi ces restes, il y en a $\underline{m}$ qui sont supérieurs à $\frac{p}{2}$, alors on a : $\left(\frac{q}{p}\right) = (-1)^m$.

Pour démontrer ce lemme, notons que l'ensemble $A$ jouit de la propriété suivante :

(P) Tout entier $\underline{a}$ non multiple de $\underline{p}$ est congru, modulo $p$, à un élément de l'ensemble $A$ ou à son opposé.

En effet, au lieu de considérer la division euclidienne de $\underline{a}$ par $\underline{p}$, avec son reste $\underline{\text{positif}}$, compris entre 1 et p-1, on peut déterminer le "reste minimal" de $\underline{a}$ par $\underline{p}$, lequel est compris entre $-\frac{p-1}{2}$ et $\frac{p-1}{2}$. Le reste euclidien habituel est plus grand que $\frac{p}{2}$ $\underline{\text{ssi}}$ le reste minimal est négatif.

Un ensemble $A$ qui vérifie la propriété (P) décrite ci-dessus est appelée un $\underline{\text{demi-système de résidus modulo } p}$.

Par suite, l'on a, pour tout élément $k$ de $A$, $kq \equiv \alpha_k r_k$ avec $r_k \in A$ et $\alpha_k = \pm 1$. Plus précisément, on a $\alpha_k = 1$ si le reste de la division de $kq$ par $p$ est élément de $A$ et $\alpha_k = -1$ dans le cas contraire. On vérifie aisément que si $k$ et $h$ sont deux éléments $\underline{\text{distincts}}$ de $A$, alors $r_k \neq r_k$, de sorte que l'ensemble $\{r_1, r_2, \ldots r_{(p-1)/2}\}$ n'est autre que l'ensemble $A$ lui-même. Le produit de toutes les congruences $kq \equiv \alpha_k r_k$ donne alors :

$$q^{\frac{p-1}{2}} \prod_{k=1}^{(p-1)/2} k \equiv \prod_{k=1}^{(p-1)/2} \alpha_k \cdot \prod_{k=1}^{(p-1)/2} r_k \pmod{p},$$

Soit : $q^{(p-1)/2} \left(\frac{p-1}{2}\right)! \equiv (-1)^m \left(\frac{p-1}{2}\right)! \pmod{p}$,

d'où le lemme énoncé ci-dessus.

La détermination de $\left(\frac{q}{p}\right)$ est ainsi ramenée au calcul du nombre $m$, c'est-à-dire à un problème de $\underline{\text{dénombrement}}$.

Il est d'ailleurs curieux d'observer que Gauss, qui ne

daigne jamais utiliser le symbole de Legendre, introduit dans cet article une notation provisoire qui n'est pas sans le rappeler, puisqu'il pose : $(q , p) = m$ (et non $(q , p) = (-1)^m$) .

(23) La Troisième Démonstration

Gauss introduit ensuite la notation $[x]$ pour représenter la partie entière d'une "quantité quelconque x ". Le quotient de la division euclidienne de $\lambda q$ par $p$ est $\left[ \frac{\lambda q}{p} \right]$ , et le reste : $\lambda q - p \left[ \frac{\lambda q}{p} \right]$. Ce reste sera supérieur à $\frac{p}{2}$ ssi l'on a $\frac{\lambda q}{p} - \left[ \frac{\lambda q}{p} \right] > \frac{1}{2}$ .

Or, on remarque que, pour tout réel $x$ , on a $[2x] - 2[x] = 0$ si $x$ vérifie : $0 \leqslant x - [x] < \frac{1}{2}$ , et $[2x] - 2[x] = 1$ lorsque $\frac{1}{2} \leqslant x - [x] < 1$ . Ainsi, lorsque $\lambda$ est un entier qui varie entre 1 et $\frac{p-1}{2}$ , les valeurs de $\lambda$ pour lesquelles on a $\frac{\lambda q}{p} - \left[ \frac{\lambda q}{p} \right] > \frac{1}{2}$ , et dont nous cherchons le nombre $m$ , vérifient aussi : $\left[ \frac{2\lambda q}{p} \right] - 2 \left[ \frac{\lambda q}{p} \right] = 1$ ; les autres donnent : $\left[ \frac{2\lambda q}{p} \right] - 2 \left[ \frac{\lambda q}{p} \right] = 0$ . Il en découle que :

$$m = \sum_{\lambda = 1}^{(p-1)/2} \left( \left[ \frac{2\lambda q}{p} \right] - 2 \left[ \frac{\lambda q}{p} \right] \right)$$ , ce que notre auteur écrit ainsi :

$$m = \left[ \frac{2q}{p} \right] + \left[ \frac{4q}{p} \right] + \left[ \frac{6q}{p} \right] + \ldots + \left[ \frac{(p-1)q}{p} \right] - 2 \left[ \frac{2q}{p} \right] - 2 \left[ \frac{3q}{p} \right] - \ldots - 2 \left[ \frac{\frac{1}{2}(p-1)q}{p} \right]$$

Il transforme ensuite la première partie de cette somme par application de l'égalité : $[x] + [h - x] = h - 1$ , vraie pour $h$ entier et $x$ réel non-entier ; ce qui donne par exemple :

$$\left[ \frac{(p-1)q}{p} \right] = \left[ q - \frac{q}{p} \right] = q - 1 - \left[ \frac{q}{p} \right] , \left[ \frac{(p-3)q}{p} \right] = q - 1 - \left[ \frac{3q}{p} \right] , \text{ etc.}$$

Cela lui donne deux expressions de $m$ , que le lecteur établira sans peine, selon que $p$ est de la forme $4n + 1$ ou $4n + 3$ . Remarquons simplement, pour aller plus vite, que seule nous intéresse la parité de $m$ , et que l'on peut toujours écrire : $m \equiv \left[ \frac{2q}{p} \right] + \left[ \frac{4q}{p} \right] + \ldots + \left[ \frac{(p-1)q}{p} \right]$ ,

d'où, lorsque q est impair :

$$m \equiv -\left[\frac{q}{p}\right] + \left[\frac{2q}{p}\right] - \left[\frac{3q}{p}\right] + \ldots \pm \left[\frac{\frac{1}{2}(p-1)\,q}{p}\right] \equiv \sum_{\lambda=1}^{(p-1)/2} \left[\frac{\lambda q}{p}\right] \text{ mod. } 2$$

Dès lors, la loi de réciprocité n'est pas loin. Notre auteur établit encore une propriété de la fonction partie-entière :

"Soit x une quantité positive non entière, telle qu'aucun des multiples : x, 2x, ... nx ne soit entier posant $[n\,x] = h$, il est facile de conclure que parmi les multiples de la quantité réciproque :

$\frac{1}{x}, \frac{2}{x}, \ldots \frac{h}{x}$, on ne trouve pas non plus d'entier. Alors, je dis que :

$$\left.\begin{array}{l} [x] + [2x] + [3x] + \ldots + [nx] \\ + \left[\frac{1}{x}\right] + \left[\frac{2}{x}\right] + \left[\frac{3}{x}\right] + \ldots + \left[\frac{h}{x}\right] \end{array}\right\} = n\,h \text{ ".}$$

Corollaire : si k et p sont des nombres impairs premiers entre eux, on a :

$$\left.\begin{array}{l} \left[\frac{q}{p}\right] + \left[\frac{2q}{p}\right] + \left[\frac{3q}{p}\right] + \ldots + \left[\frac{1/2(p-1)\,q}{p}\right] \\ + \left[\frac{p}{q}\right] + \left[\frac{2p}{q}\right] + \left[\frac{3p}{q}\right] + \ldots + \left[\frac{1/2(q-1)\,p}{q}\right] \end{array}\right\} = \frac{1}{4}(q-1)(p-1).$$

Et enfin, si l'on suppose q et p premiers impairs, si l'on pose, avec la notation de Gauss, $(q,p) = m$ et $(p,q) = n$, ce dernier corollaire nous dit que : $m + n \equiv \frac{1}{4}(q-1)(p-1) \pmod 2$. Puisque l'on sait, par le lemme de Gauss, que $\left(\frac{q}{p}\right) = (-1)^m$ et $\left(\frac{p}{q}\right) = (-1)^n$, la loi de réciprocité est établie.

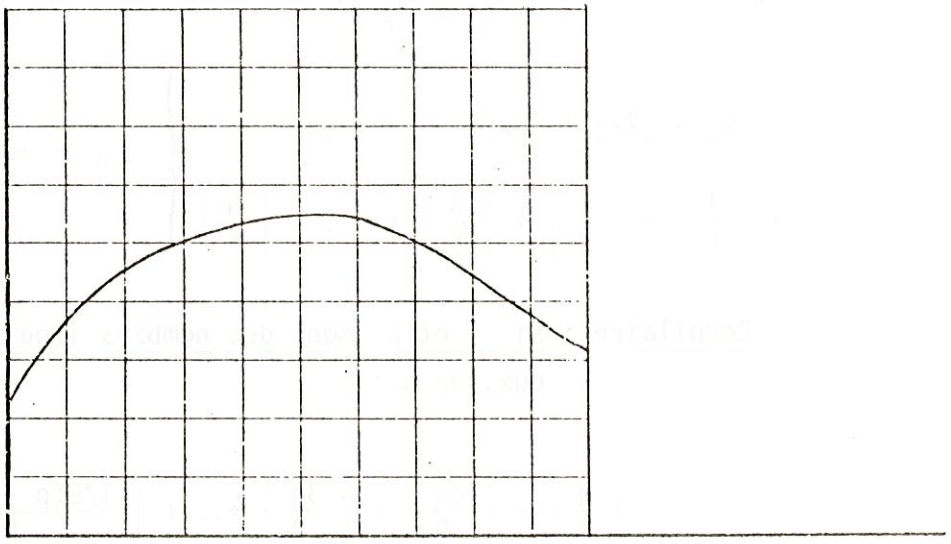
Ajoutons que le lemme de Gauss et la première expression de m trouvée ci-dessus permettent de retrouver aisément la valeur de $\left(\frac{2}{p}\right)$.

(24) L'interprétation géométrique d'Eisenstein.

Dans un article de juillet 1844 ([EI2]), Eisenstein améliore la troisième démonstration de Gauss. En reprenant les notations du n°23, disons qu'il redémontre d'abord la relation :

$m \equiv \sum_{\lambda = 1}^{(p-1)/2} \left[ \frac{\lambda q}{p} \right]$ (mod. 2) . Il considère ensuite un plan euclidien muni d'un système de coordonnées rectangulaires, et dans ce plan une courbe d'équation $y = \phi(x)$ (figure 1).

*1.*



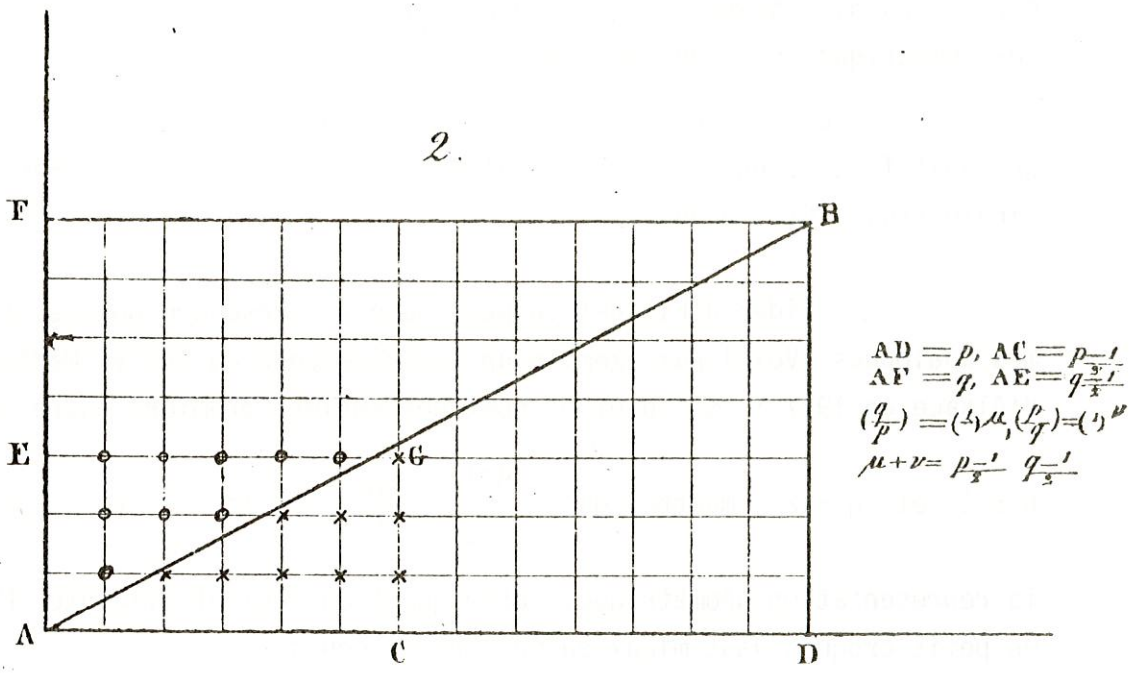
Le nombre des "points entiers", c'est-à-dire à coordonnées entières, situés entre cette courbe et l'axe des abscisses est :

$$[\ \phi(1)\ ] + [\ \phi(2)\ ] + [\ \phi(3)] + \ldots$$

On comprend dans cette somme les points appartenant à la courbe, mais on exclut les points situés sur les axes.

Pour revenir à notre sujet, considérons sur la figure 2 les points tels que $AD = FB = p$ , $AF = DB = q$ , $AC = EG = \frac{1}{2}(p - 1)$ ,

$$AE = CG = \frac{1}{2}(q - 1) .$$




La droite AB a pour équation $y = \frac{q}{p} x$ et la somme $\sum_{\lambda=1}^{(p-1)/2} \left[ \frac{\lambda q}{p} \right]$ désigne le nombre des points entiers compris entre AB et AD , non compris ceux de AD , jusqu'à l'ordonnée CG incluse (ce sont les points marqués x sur la figure) . Mais on peut raisonner de même en écrivant $x = \frac{p}{q} y$ l'équation de la droite AB et en échangeant les rôles des axes de coordonnées. Le nombre des points marqués ∘ sur la figure est : $\sum_{\lambda=1}^{(q-1)/2} \left[ \frac{\lambda p}{q} \right]$ . Mais ces points, pris tous ensemble, donnent le système de tous les points entiers du rectangle AEGC, non compris ceux de AE et ceux de AC . Leur nombre total est visiblement $\frac{p - 1}{2} \cdot \frac{q - 1}{2}$ .

Nous avons ainsi une justification géométrique du dernier "corollaire" de la démonstration de Gauss.

Ajoutons qu'Eisenstein termine son article par une "Remarque" concernant des dénombrements de "points entiers" (Gitterpuncte) dans certaines régions du plan limitées par des courbes remarquables, telles que cercles ou hyperboles, ce qui ouvre toute une série de question arithmético-géométriques du plus haut intérêt.

Cet article a été traduit en anglais en 1857 par Cayley, avec un additif qui donne les démonstrations qui manquaient à la "Remarque" finale (voir [CY], p.39).

L'idée d'Eisenstein peut servir à résoudre nombre de problèmes analogues. Voici par exemple un exercice posé au Rallye Mathématique d'Alsace en 1977 : "Si $p$ et $q$ sont des entiers premiers entre eux avec $p \geqslant 1$ et $q \geqslant 2$, montrer que $\sum_{\lambda=1}^{q-1} \left[ \frac{\lambda p}{q} \right] = \frac{1}{2} (p - 1) (q - 1)$". Avec la représentation géométrique, cette question devient évidente. Moralité : un petit croquis vaut mieux qu'un long discours.

(25) Dans sa "Théorie des Nombres" ([LG3], pp.57 sq.) Legendre a reproduit assez fidèlement la troisième démonstration de Gauss, qu'il dit "d'autant plus remarquable qu'elle repose sur les principes les plus élémentaires". Ce texte de Legendre est repris dans [CL], p.51. La démonstration en question est exposée aussi dans [MA], p.38 .

On peut considérer que les promesses de simplicité, formulées par Gauss dans le préambule de son mémoire, ont été tenues. C'est pourquoi plusieurs ouvrages de Théorie des Nombres présentent la loi de réciprocité quadratique à l'aide de la troisième démonstration de Gauss, avec diverses nuances : [AP], p.185 ; [SI], p.321 ; [RO], p.203 . D'autres utilisent la représentation géométrique d'Eisenstein, qui rend plus naturel et plus évident l'un des maillons importants de la troisième démonstration de Gauss : par exemple , [NA], p.141 ; [HW], p.76 ; [BU], p.203 ; [DR], p.104 .

(26) La cinquième démonstration de Gauss.

Publiée en 1817 ([GA2], p.48), cette cinquième démonstration s'appuie elle aussi sur le lemme de Gauss, mais présente un autre procédé d'estimation de la parité des nombres appelés ci-dessus m et n (n°s 22 et 23), sans utiliser la fonction "partie entière".

Voici le théorème qui est la clé de cette démonstration :

"Soient p et q deux entiers positifs impairs premiers entre eux, et m le nombre des restes minimaux positifs des nombres

$$q,\ 2q,\ 3q,\ \ldots\ \frac{1}{2}(p-1)\,q\ ,$$

selon le module p, qui sont supérieurs à $\frac{1}{2}p$ ; et soit n le nombre des restes minimaux positifs des nombres

$$p,\ 2p,\ 3p,\ \ldots\ \frac{1}{2}(q-1)\,p\ ,$$

selon le module q, qui sont supérieurs à $\frac{1}{2}q$. Alors, parmi les trois nombres m, n, $\frac{1}{4}(p-1)(q-1)$, ou bien tous sont pairs, ou bien un est pair et les deux autres impairs".

Il est clair que, par le lemme de Gauss, la loi de réciprocité découle immédiatement de ce théorème. La démonstration de Gauss est assez longue, et nécessite de répartir en seize classes les ensembles de nombres en question.

Frobenius en a donné une interprétation très lumineuse ([FR], p.628). Il part d'un énoncé du lemme de Gauss légèrement différent de celui que nous avons donné au n° 22, et que voici. Au lieu des restes euclidiens positifs habituels, on utilise les restes minimaux, positifs ou négatifs, dont nous avons parlé au n° 22 : pour tout entier x tel que $1 \leqslant x \leqslant \frac{p-1}{2}$, il existe deux entiers y et $r_x$ uniques tels que $qx = py + r_x$, avec $-\frac{p}{2} < r_x < \frac{p}{2}$. Dès lors, m est le nombre des $r_x$ négatifs. Il est clair qu'alors le quotient y vérifie : $0 < y < \frac{q}{2}$, et que m est le nombre des couples d'entiers (x,y) tels que : $0 < x < \frac{p}{2}$, $0 < y < \frac{q}{2}$, $-\frac{p}{2} < qx - py < 0$. De même, n est le nombre de couples d'entiers (x,y) tles que : $0 < x < \frac{p}{2}$, $0 < y < \frac{q}{2}$, $0 < qx - py < \frac{q}{2}$.

Appelons $s$ le nombre des couples d'entiers $(x,y)$ tels que : $0 < x < \frac{p}{2}$ , $0 < y < \frac{q}{2}$ , $qx - py < -\frac{p}{2}$ et $t$ le nombre des couples d'entiers $(x,y)$ tels que : $0 < x < \frac{p}{2}$ , $0 < y < \frac{q}{2}$ , $qx - py < \frac{q}{2}$ . Ces deux ensembles comptent le même nombre d'éléments car les relations : $x' = \frac{p+1}{2} - x$ , $y' = \frac{q+1}{2} - y$ définissent entre eux une correspondance bijective. Donc : $s = t$ .

Par ailleurs, la somme $m + n + s + t$ représente le nombre total des couples d'entiers $(x,y)$ tels que $0 < x < \frac{p}{2}$ et $0 < y < \frac{q}{2}$ . C'est le nombre des "points entiers" du rectangle AEGC de la représentation d'Eisenstein (cf. n° 24), car on peut interpréter les entiers $x$ et $y$ comme les coordonnées de ces points : La "correspondance bijective" dont nous venons de parler se "lit" alors comme une symétrie par rapport au centre de ce rectangle.

On a donc : $m + n + s + t = \frac{p-1}{2} \cdot \frac{q-1}{2}$ et, puisque $s = t$ , $m + n \equiv \frac{p-1}{2} \frac{q-1}{2} \pmod 2$, ce qu'il fallait démontrer.

Cette démonstration, plus simple encore que la troisième, est utilisée par divers auteurs désireux d'établir la loi de réciprocité selon des voies élémentaires. Voir par exemple : [LV3], p.103, [WE2], p.58, [LV2], p.69 , et [IT2], p.76 , qui développe de façon particulièrement détaillée le point de vue géométrique.

## § VI - SOMMES de GAUSS

### (27) Le mémoire d'août 1808

En août 1808, Gauss communique à la Société Scientifique de Göttingen un mémoire intitulé :

" Summatio quarumdam serierum singularium " ("somme de certaines séries particulières") qui est publiée en 1811 ([GA2], p.10). Ce texte a

pour but principal de démontrer un résultat qui était déjà annoncé dans les "Recherches Arithmétiques", article 356, p.465, dans le cadre de la Section VII, consacrée aux "équations qui déterminent la division du cercle" - nous dirions : à la cyclotomie . Mais il s'agissait alors d'une "observation" sans démonstration. Voici ce que devient ce théorème dans le mémoire d'août 1808 :

" Supposant que n est un nombre premier impair, on désigne par a les résidus quadratiques de n compris entre 1 et n-1 inclusivement, et par b les non-résidus situés entre les mêmes limites, on note $\omega$ l'arc $360°/n$, et k un entier déterminé quelconque non divisible par n , et l'on a :

I . pour toute valeur de p de la forme $4n + 1$ ,

$$\Sigma \cos a k \omega = -\frac{1}{2} \pm \frac{1}{2}\sqrt{n}$$

$$\Sigma \cos b k \omega = -\frac{1}{2} \mp \frac{1}{2}\sqrt{n} \quad , \text{ d'où}$$

$$\Sigma \cos a k \omega - \Sigma \cos b k \omega = \pm \sqrt{n}$$

$$\Sigma \sin a k \omega = 0$$

$$\Sigma \sin b k \omega = 0 .$$

II . pour toute valeur de p de la forme $4m + 3$ ,

$$\Sigma \cos a k \omega = -\frac{1}{2}$$

$$\Sigma \cos b k \omega = -\frac{1}{2}$$

$$\Sigma \sin a k \omega = \pm \frac{1}{2}\sqrt{n}$$

$$\Sigma \sin b k \omega = \mp \frac{1}{2}\sqrt{n}$$

$$\Sigma \sin a k \omega - \Sigma \sin b k \omega = \pm \sqrt{n} . "$$

Il faut entendre que, dans ces $\Sigma$ , ce sont a et b qui varient, décrivant respectivement l'ensemble des résidus quadratiques et des non-résidus compris entre 1 et n-1 . L'auteur précise que ces sommations sont rigoureusement établies, mais qu'il est difficile de déter-

miner le signe du radical qui intervient dans certaines de ces formules.

Dans la suite de l'article, il remarque que : $\Sigma \cos a\, k\, \omega = \cos k\, \omega + \cos 4\, k\, \omega + \ldots + (\frac{1}{2}(n-1))^2 k\, \omega =$ $\cos (\frac{1}{2}(n+1))^2\, k\, \omega + \ldots + \cos(n-1)^2\, k\, \omega$ , de sorte qu'en posant :

$T = 1 + \cos k\, \omega + \cos 4\, k\, \omega + \ldots + \cos (n-1)^2\, k\, \omega$

et $U = \sin k\, \omega + \sin 4\, k\, \omega + \ldots + \sin(n-1)^2\, k\, \omega$ , on obtient :

$1 + 2\, \Sigma \cos a\, k\, \omega = T$ , $2\, \Sigma \sin a\, k\, \omega = U$ , et que le problème revient alors à évaluer $T$ et $U$ . Ce double problème se réduit à un seul par l'usage des nombres complexes. Si l'on nomme $r$ le complexe $\cos k\, \omega + \sin k\, \omega$ , qui est une racine $n$-ième de l'unité, il vient :

$$T + i\, U = 1 + r + r^4 + \ldots + r^{(n-1)^2} .$$

Ce nombre complexe, que Gauss note $W$ , est appelé de nos jours somme de Gauss quadratique et noté $G(k;n)$ ([AP], p.177, p.306). Il n'est d'ailleurs pas nécessaire, dans le cas général, de supposer $n$ premier.

(28) Calcul des sommes de Gauss quadratiques.

Pour calculer cette somme, il existe plusieurs procédés. Dans le texte de 1808, Gauss introduit l'expression :

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

où $m$ et $\mu$ sont des entiers naturels et $x$ une variable, qu'il n'éprouve pas le besoin de définir précisément. Il démontre que cette fonction est entière et rationnelle, c'est-à-dire est un polynôme (nul si $m < \mu$). Puis il considère la "progression" :

$$f(n,m) = 1 - (m,1) + (m,2) - (m,3) + \ldots ,$$

qui n'est pas une "série", mais une somme finie, un polynôme, puisque son dernier terme non nul est : $(-1)^m\, (m,m) = (-1)^m$ . Il démontre par récurrence que $f(x,m)$ est nul si $m$ est impair, et que l'on a pour $m$ pair :

$$f(x,m) = (1 - x)\ (1 - x^3)\ (1 - x^5)\ \ldots\ (1 - x^{m-1})\ .$$

Notons qu'ici, Gauss insère une remarque qui montre le lien de ce travail avec ses recherches sur les séries infinies, les fonctions analytiques, la fonction thêta : lorsque $m$ est un entier négatif, $f(x,m)$ prend bien la forme d'une telle série. Et nous voyons apparaître l'identité :

$$1 + x + x^3 + x^6 + x^{10} + \ldots = \frac{1-x^2}{1-x}\ \frac{1-x^6}{1-x^3}\ \frac{1-x^6}{1-x^5}\ \frac{1-x^8}{1-x^7}\ \ldots$$

qui n'a rien à voir avec notre propos, mais sur laquelle Gauss promet de revenir en d'autres occasions.

Le lien entre la "série" $f(x,m)$ et la "somme de Gauss" $G(k;n)$ apparaît lorsque l'on fait $x = r$ et $m = n - 1$, car alors il vient :

$$f(r, n-1) = 1 + r^{-1} + r^{-3} + r^{-6} + \ldots + r^{-\frac{1}{2}(n-1)n}$$

$$= (1 - r)\ (1 - r^3)\ (1 - r^5)\ \ldots\ (1 - r)^{n-2}\ ,$$

si $n$ est impair et si $r$ est une "racine propre" de l'unité ($r = \cos\frac{2k\pi}{n} + i \sin\frac{2k\pi}{n}$, avec $k$ et $n$ premiers entre eux). Nous dirions aujourd'hui une "racine primitive". On peut remplacer $r$ par $r^{-2}$, qui est encore une racine primitive n-ième de l'unité, ce qui donne :

$$1 + r^2 + r^6 + \ldots + r^{(n-1)n} = (1 - r^{-2})\ (1 - r^{-6})\ldots(1-r^{-2(n-2)}).$$

Et en multipliant les deux membres de cette égalité par le produit

$r\ r^3\ r^5\ \ldots\ r^{n-2} = r^{\frac{1}{4}(n-1)^2}$, on obtient :

$$W = G(n;k) = 1 + r + r^4 + \ldots + r^{(n-1)^2} = (r-r^{-1})\ (r^3-r^{-3})\ \ldots\ (r^{n-2} - r^{-n+2})\ .$$

Mais on remarque que : $r-r^{-1} = r^{-n+1} - r^{n-1}$, $r^3 - r^{-3} = r^{-n+3} - r^{n-3}$, etc. ce qui implique une nouvelle expression de $W$ :

$$W = (-1)^{\frac{1}{2}(n-1)} (r^2 - r^{-2}) (r^4 - r^{-4}) \dots (r^{(n-1)} - r^{-n+1}) .$$

Et par suite, $W^2 = (-1)^{\frac{1}{2}(n-1)} (r - r^{-1}) (r^2 - r^{-2}) (r^3 - r^{-3}) \dots (r^{n-1} r^{-n+1})$

$$= (-1)^{\frac{1}{2}(n-1)} r^{\frac{1}{2}n(n-1)} (1 - r^{-2}) (1 - r^{-4}) \dots (1 - r^{-2(n-1)}) .$$

Or, les complexes $r^{-2}$ , $r^{-4}$ ,... $r^{-2(n-1)}$ sont les racines n-ièmes de l'unité autres que $1$ , parce que $r$ est une racine primitive et que $n$ est impair. Il en découle que : $(x - r^{-2}) (x - r^{-4}) \dots$

$$(x - r^{-2(n-1)}) = x^{n-1} + x^{n-2} + \dots + x^2 + x + 1,$$

d'où : $(1 - r^{-2}) (1 - r^{-4}) \dots (1 - r^{-2(n-1)}) = n$ .

En conclusion, on a $W^2 = \pm n$ , avec le signe $+$ si $n$ est de la forme $4k + 1$ et $-$ si $n$ est de la forme $4k + 3$ . On retrouve bien les formules annoncées ci-dessus, mais avec la même imprécision sur le signe si l'on veut obtenir $W$ , et non plus seulement $W^2$ .

Gauss montre que l'on peut lever cette imprécision dans le cas où $k = 1$ , car alors on a : $r - r^{-1} = 2 i \sin \omega$ , $r^3 - r^{-3} = 2i\sin 3\omega$ etc., avec $\omega = \frac{2\pi}{n}$ , d'où :

$$W = (2 i)^{\frac{1}{2}(n-1)} \sin \omega \sin 3\omega \dots \sin(n - 2)\omega .$$

Il suffit de compter le nombre de facteurs négatifs de ce produit pour avoir le signe cherché. On trouve : $W = \sqrt{n}$ si $n$ est de la forme $4k + 1$, et $W = i \sqrt{n}$ si $n$ est de la forme $4k + 3$ . Nous avons ainsi obtenu $G(1;n)$, toujours égal à : $i^{(n-1)^2/4} \sqrt{n}$ .

Pour en revenir au cas général, avec $n$ premier impair, $\omega = \frac{2\pi}{n}$ et $r = \cos k \omega + i \sin k \omega$ , rappelons que l'on a , avec les notations introduites au début du présent article : $G(k;n) = W = 1 + 2 \Sigma r^a$ , le $\Sigma$ étant étendu à tous les $a$ résidus quadratiques de $n$ . Or, la somme de toutes les $n$ racines n-ièmes de l'unité est nulle, c'est-à-dire

que : $1 + \Sigma\, r^a + \Sigma\, r^b = 0$ . Il en résulte que $W = \Sigma\, r^a - \Sigma\, r^b$ . On pose alors $R = \cos\omega + i \sin\omega$ , d'où $W = \Sigma\, R^{ka} - \Sigma\, R^{kb}$ . Si $k$ est résidu quadratique de $n$ , tous les produits $ka$ sont résidus et tous les $kb$ sont non résidus. On en déduit dans ce cas : $G(k;n) = G(1;n)$ . Mais si $k$ est non-résidu, les $ka$ sont non-résidus et les $kb$ sont résidus ; et alors, il vient $G(k;n) = - G(1;n)$ . D'où l'utilité du symbole de Legendre, qui permet d'écrire : $G(k;n) = \left(\frac{k}{n}\right) G(1;n)$ , pour tout $n$ premier impair et $k$ non multiple de $n$ .

Dans ce mémoire, Gauss détermine aussi la somme $G(1;n)$ pour $n$ pair, en utilisant une autre "série" notée $F(x,m)$ . Nous ne nous arrêterons pas sur ce point ; on pourra trouver par exemple les formules, établies par une autre méthode, dans [AP], p.195 . Ces "sommes de Gauss" vérifient enfin une relation que l'on appelle aussi à juste titre "loi de réciprocité" :

$$\boxed{G(m;n)\, G(n;m) = G(1;mn)} \quad ,$$

pour $m$ et $n$ premiers entre eux. Cette propriété se démontre simplement, par le calcul (cf. [MA], p.208 , [AP], p.177) .

(29) Par la suite, plusieurs mathématiciens ont cherché aussi à évaluer ces "sommes de Gauss" et en particulier leur signe.

Lejeune-Dirichlet a utilisé pour cette question, avec autant de succès que pour d'autres, sa méthode consistant à appliquer l'Analyse à la Théorie des Nombres. Son article de 1835 "sur l'usage des intégrales définies dans la sommation des séries finies ou infinies" ([LD1], p.257 : J. de Crelle, t.17 , p.57 ; [MA], p.205) part du calcul de l'intégrale $\int_a^b \frac{\sin(2k+1)\,\theta}{\sin\theta}\, f(\theta)\, d\theta$ et de sa limite lorsque l'entier $k$ tend vers $+\infty$ , $f$ étant une fonction continue ; il utilise aussi les intégrales de Fresnel $\int_{-\infty}^{+\infty} \cos(x^2)\, dx$ et $\int_{-\infty}^{+\infty} \sin(x^2)\, dx$ , dont la commune valeur est $\sqrt{\frac{\pi}{2}}$ . Après des calculs assez longs, il obtient le ré-

sultat voulu, ainsi qu'un procédé de sommation de séries. Il est revenu sur cette question et sur bien d'autres dans sa grande étude de 1839-1840 "Recherches sur diverses applications de l'Analyse infinitésimale à la Théorie des Nombres" ([LD1], p.411; J. de Crelle, tomes 19 et 21). Cauchy et V.A. Lebesgue ont aussi obtenu ce résultat à l'aide de calculs faisant intervenir la fonction thêta et les fonctions elliptiques (cf. [SM], pp.63-64).

Il faut noter que, dès les "Recherches Arithmétiques" (|GAD| VII n°335 p.429), Gauss avait indiqué que les principes de l'étude des fonctions circulaires exposée à la section VII pouvaient s'appliquer aussi aux "fonctions transcendantes (...) qui dépendent de l'intégrale $\int \frac{dx}{\sqrt{1-x^4}}$ ".

En 1889, Kronecker a déduit les sommes de Gauss d'un calcul de résidus, que l'on peut trouver dans [MA], p.202, ou plus récemment dans [AP], p.196 , avec une simplification due à Mordell ([MO]).

On peut aussi lire les démonstrations de Schur et de Mertens dans [LU], p.207, p.213 .

Et le calcul des sommes de Gauss peut encore se déduire de la transformée de Fourier de la fonction thêta (cf. [GO], p.72 ; [LN], p.90).

Signalons enfin que les sommes de Gauss ont connu des généralisations. Nous avons, pour $p$ premier et $m$ entier rationnel :

$$G(m;p) = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) e^{2km i\pi/p}$$

. C'est sous cette forme que Eisenstein cite les "formules de Mr. Gauss" ([EI3], p.41). Ceci découle de la relation vue plus haut (n°28) : $W = \Sigma\, r^a - \Sigma\, r^b$ .

Dirichlet a introduit des fonctions appelées aujourd'hui <u>caractères</u>, qui possèdent deux propriétés importantes du <u>caractère</u> de Legendre $m \longmapsto \left(\frac{m}{p}\right)$ : un caractère modulo $p$ est une application $\chi$ de $\mathbb{Z}$ dans $\mathbb{C}$ qui jouit des propriétés suivantes :

a) Elle est <u>complètement multiplicative</u> (on a : $\chi(ab) = \chi(a)\,\chi(b)$ pour tous entiers $a$ et $b$).

b) Elle est <u>périodique</u>, de période $p$ .

c) On a $\chi(a) = o$ si, et seulement si, $p$ divise $a$ .

La périodicité permet de définir ce caractère sur l'ensemble $\mathbb{Z}/p\mathbb{Z}$ . La restriction de $\chi$ au groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$ est un morphisme de ce groupe dans le groupe multiplicatif $\mathbb{C}^*$ .

Plus généralement, un caractère d'un groupe abélien fini $G$ sera un morphisme de $G$ dans le groupe multiplicatif $\mathbb{C}^*$ .

On peut aussi définir un caractère modulo $m$ non premier en conservant les propriétés a) et b) ci-dessus et en supposant que $\chi(a) = o$ <u>ssi</u> : $m \wedge a > 1$ .

Une somme de Gauss associée à un caractère $\chi$ modulo $p$ sera alors une somme de la forme :

$$G(m\ ,\ \chi) \ = \ \sum_{k=1}^{p-1} \chi(k)\ e^{2kmi\pi/p} \quad .$$

Et l'on peut concevoir encore d'autres généralisations (cf. [DO], p.10 ; [AP], p.165 ; [WE1], p.39).

(30) <u>Quatrième démonstration de la loi de réciprocité quadratique.</u>

On aura compris que les sommes de Gauss présentent un grand intérêt par elles-mêmes et que le texte " Summatio serierum singularium " n'a pas pour unique but la démonstration de la loi de réciprocité. Pourtant, cette démonstration -la quatrième de Gauss- vient "en prime", de la façon suivante : Si $p$ et $q$ sont des nombres premiers impairs distincts, la loi de réciprocité des sommes de Gauss s'écrit :

$$G(p\ ;\ q)\ G(q\ ;\ p) = G(1\ ;\ pq) \ .$$

Mais nous avons vu que $G(p\ ;\ q) = \left(\frac{p}{q}\right) G(1\ ;\ q)$ et que $G(q\ ;\ p) = \left(\frac{q}{p}\right) G(1\ ;\ p)$, d'où : $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \dfrac{G(1\ ;\ pq)}{G(1\ ;\ p)\ G(1\ ;\ q)}$ .

La valeur de $G(1\ ;\ n)$ a été calculée plus haut pour tout $n$ impair : $G(1\ ;\ n) = i^{(n-1)2/4}\ \sqrt{n}$ . Il vient donc :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = i^{\frac{1}{4}\left((pq-1)^2-(p-1)^2-(q-1)^2\right)} \quad .$$

La conclusion découle du fait que l'exposant de $i$ s'écrit

aussi $(p^2 - 1)\ \frac{q^2 - 1}{4} - 2\ \frac{(p - 1)(q - 1)}{4}$ .

A vrai dire, le texte de Gauss contient une proposition d'allure plus générale, qu'il énonce ainsi :

" Dénotant a, b, c etc. des nombres entiers premiers impairs inégaux, dont le produit est = n , supposons que, parmi eux, m soient de la forme $4\mu + 3$, les autres de la forme $4\mu + 1$ : alors le nombre des entiers a, b, c etc. dont $\frac{n}{a}$ , $\frac{n}{b}$ , $\frac{n}{c}$ etc. sont respectivement non-résidus sera pair si m est de la forme $4\mu$ ou $4\mu + 1$ et impair si m est de la forme $4\mu + 2$ ou $4\mu + 3$ ". ([GA2], p.42).

Un exemple illustre cet énoncé un peu obscur : Si a = 3 , b = 5 , c = 7 , d = 11 , alors m = 3 . On a, avec la notation de Gauss : 5.7.11 R3 ; 3.7.11 R5 ; 3.5.11 R7 ; 3.5.7 N11 . Seul , $\frac{n}{d}$ est non résidu de d .

Ce théorème, que Gauss dit "très élégant", se démontre comme ci-dessus (cf. [MA], p.214).

L'auteur précise ensuite :

" Le très célèbre théorème fondamental au sujet des résidus quadratiques n'est autre qu'un cas particulier du théorème précédemment exposé. En effet, en limitant le nombre des entiers a, b, c etc. à deux, il apparaît que si l'un d'eux seulement est de la forme $4\mu + 3$ ou si aucun d'eux n'est de cette forme, on doit avoir simultanément, ou bien aRb et bRa, ou bien aNb et bNa ; au contraire si les deux sont de la forme $4\mu + 3$, l'un d'eux devra être non résidu de l'autre et celui-ci résidu de celui-là. Voici donc la quatrième démonstration de ce très important (*) théorème, dont nous avons rapporté la première et la deuxième démonstration dans les Recherches Arithmétiques, et la troisième récemment dans un commentaie particulier : nous en exposerons plus tard deux autres reposant sur des principes tout à fait différents. Il est vraiment très étonnant que ce très beau (venustissimus) théorème, qui d'abord avait déjoué si constamment tous les efforts, ait pu ensuite être élucidé par des voies qui sont aux antipodes les unes des autres ". ([GA2], p.42).

(31) La sixième démonstration

Ces deux démonstrations que Gauss promet ici, il les a

---

(*) gravissimus

présentées en février 1817 dans un commentaire intitulé " Theorematis fundamentalis in doctrina de residuis quadraticis - demonstrationes et ampliationes novae " (*) ([GA2], p.47). Il s'agit donc de la cinquième et de la sixième . Nous avons présenté plus haut la cinquième (§ V, n°26).

La sixième ([GA2], p.55) s'apparente à la quatrième, que nous venons d'exposer, mais elle est débarassée de tout recours à l'analyse. En voici le principe, que nous énoncerons rapidement à l'aide des notations les plus efficaces possibles, au risque de modifier quelque peu la rédaction de Gauss.

Soit l'expression $\xi_k = \sum_{s=o}^{s=p-2} (-1)^s \, x^{kx^s}$ , où $p$ est un nombre premier impair, $k$ un entier non divisible par $p$ , $x$ une déterminée et $\alpha$ une racine primitive modulo $p$ , c'est-à-dire un entier dont la classe mod. $p$ est un générateur du groupe multiplicatif $(\mathbb{Z}/p\,\mathbb{Z})^*$ . Soit $q$ un nombre premier impair autre que $p$ . Gauss démontre successivement :

a) que $\xi_1^2 - (-1)^{\frac{p-1}{2}} p$ est divisible par $\frac{1 - x^p}{1 - x}$ ;

b) que $(\xi_1)^q - \xi_q$ est divisible par $q$ (**) ;

c) enfin, que $\xi_q - \left(\frac{q}{p}\right) \xi_1$ est divisible par $1 - x^p$ .

La proposition a) implique que $\xi_1^{q-1} - (-1)^{\frac{p-1}{2}\frac{q-1}{2}} p^{\frac{q-1}{2}}$ est divisible par $\frac{1 - x^p}{1 - x}$ . Ce résultat, combiné à la proposition c), suffit à prouver que : $\xi_1 (\xi_1^q - \xi_q) - (-1)^{(p-1)/2} p\left[(-1)^{(p-1)(q-1)/4} p^{(p-1)/2} - \left(\frac{q}{p}\right)\right]$ est aussi divisible par $\frac{1 - x^p}{1 - x}$ . Gauss déduit alors de la proposition b) que le contenu du crochet est multiple de $q$ et comme l'on sait (critère d'Euler) que $p^{(q-1)/2} \equiv \left(\frac{p}{q}\right)$ (mod. $q$), la loi de réciprocité est démontrée une fois encore .

---

(*) "Démonstrations et développements nouveaux du théorème fondamental de la doctrine des résidus quadratiques" .

(**) En renvoyant à l'article 51 des Recherches Arithmétiques, où il montrait que $(a + b + \ldots)^q \equiv a^q + b^q + \ldots$ (mod. $q$).

(32) Gauss et les nombres algébriques : septième et huitième démonstrations.

On aura remarqué qu'interviennent, dans les deux démonstrations précédentes, les racines de l'unité et les polynômes $x^n - 1$. Dans la sixième démonstration, Gauss utilise la divisibilité dans l'anneau des polynômes $\mathbb{Z}[X]$. Mais on sent déjà, en lisant cette démonstration qu'il serait plus commode de pouvoir soulever des questions de divisibilité à propos de nombres qui ne seraient plus seulement entiers rationnels, mais qui pourraient comporter des racines n-ièmes imaginaires de l'unité, bref de travailler dans des extensions cyclotomiques de $\mathbb{Q}$ et dans leurs anneaux d'entiers. C'est une des raisons du grand essor de la théorie des nombres algébriques du 19e siècle, avec notamment les "nombres idéaux" de Kummer, destinés à pallier les inconvénients de ces nouveaux nombres relativement à la décomposition en facteurs premiers (cf. [DD1], p.178, p.191 ou [WE1], p.39).

Pour sa part, Gauss y a pris une part éminente. Les considérations de la section VII des Recherches Arithmétiques, que nous avons déjà mentionnée, ont été développées par lui dans des écrits non publiés de son vivant, dont certains ont été rassemblés dans le tome II de ses oeuvres ([GA2], p.212). Sur cette base, il a encore donné deux démonstrations supplémentaires de la loi de réciprocité, par des procédés algébriques ([GA2], pp.234,235). Bien que classées septième et huitième, elles datent de septembre 1796. Ces textes devaient former le second volume des "Recherches Arithmétiques", qui jamais ne vit le jour.

(33) Démonstrations "purement algébriques" de la loi.

Jacobi, Eisenstein et Cauchy ont donné des versions différentes de la sixième démonstration de Gauss.

On peut lire la démonstration de Jacobi dans la "Théorie des Nombres" de Legendre ([LG3], p.391).

Celle de Cauchy a été publiée dans le "Bulletin des Sciences" de M. de Férussac 1829, puis dans son grand mémoire de 1840 sur la théorie des nombres ([CA1], [CA2]).

Celle d'Eisenstein 1844 s'intitule justement "La loi de

réciprocité tirée des formules de Mr. Gauss sans avoir déterminé préalablement le signe du radical". ([EI3]).

Nombre d'ouvrages récents présentent des démonstrations de la loi qui utilisent des sommes de Gauss, calculées non plus dans $\mathbb{C}$, mais dans des corps qui sont des extensions du corps fini $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ par des racines q-ièmes de l'unité. Il n'y a plus alors, évidemment, de problème de signe. Mais cela nécessite un arsenal mathématique un peu plus sophistiqué. On peut citer à ce propos les ouvrages suivants : [BC], p.377 ; [RI], p.43 ; [SA], p.93 ; [SE], p.16 ; [WA], p.252 .

## § VII - AUTRES DEMONSTRATIONS ET GENERALISATIONS

(34) Durant le dix-neuvième siècle, de nombreux mathématiciens ont proposé des démonstrations de la loi de réciprocité, qui étaient le plus souvent des exposés améliorés de celles de Gauss, comme nous l'avons vu, ou bien qui reposaient sur une combinaison d'éléments appartenant à deux démonstrations différentes de celles de Gauss.

Citons par exemple un article d'Eisenstein de 1845 ([EI4]). L'auteur part des considérations exposées ci-dessus (§ V, n°22) au sujet du demi-système de résidus mod. p : $\{1, 2, \ldots \frac{p-1}{2}\} = A$ . Nous avons dit alors que l'on a, pour tout $k \in A$, et tout $q$ non multiple de $p$ : $kq \equiv \alpha_k r_k \pmod{p}$ avec $\alpha_k = \pm 1$ et $r_k \in A$ ,

et nous avons montré que $q^{(p-1)/2} \equiv \prod_{k=1}^{(p-1)/2} \alpha_k \pmod{p}$. C'est le lemme de Gauss.

L'idée d'Eisenstein est de partir de la relation :

$\sin \frac{2kq\pi}{p} = \alpha_k \sin \frac{2r_k\pi}{p}$ , vraie à cause de la parité du sinus,

d'où il tire l'expression suivante :

$$\left(\frac{q}{p}\right) = \prod_{k=1}^{(p-1)/2} \frac{\sin \frac{2kq\pi}{p}}{\sin \frac{2k\pi}{p}}$$

en vertu de la remarque selon laquelle l'ensemble des $r_k$ est l'ensemble des $k$, c'est-à-dire $A$.

Une fois obtenue cette remarquable expression de $\left(\frac{q}{p}\right)$, il n'a pas même besoin d'énoncer le lemme de Gauss, qui s'y trouve exprimé. La réciprocité s'obtient à l'aide de l'identité trigonométrique :

$$\frac{\sin q x}{\sin x} = (-4)^{(q-1)/2} \prod_{h=1}^{(q-1)/2} \left(\sin^2 x - \sin^2 \frac{2h\pi}{q}\right),$$

laquelle, a priori, ne serait guère suspecte d'avoir quelque rapport avec la loi de réciprocité quadratique !

On peut trouver cette démonstration exposée dans [SE], p.19. Indiquons qu'elle a fait l'objet d'une partie d'un problème posé au concours d'entrée de l'ENS-Ulm en 1978 (voir [DO], p.8). Ce problème étudiait aussi les sommes de Gauss par application d'intéressantes considérations d'algèbre linéaire et en montrant le lien avec le déterminant de Vandermonde des racines p-ièmes de l'unité.

Dans le même ordre d'idées, un article de J. Liouville de 1847 ([LI]) part de l'identité :

$$p = (-1)^{(p-1)/2} (r - r^{-1})^2 (r^2 - r^{-2})^2 \ldots (r^{(p-1)/2} - r^{-(p-1)/2})^2,$$

où $p$ est un nombre premier impair et $r$ une racine p-ième de l'unité (*). On y reconnaît le carré de la somme de Gauss, notée plus haut $W$ (§ VI, n°27), mais cela importe peu. Liouville élève les deux membres de cette inégalité à la puissance $\frac{q-1}{2}$, "en omettant les multiples de $q$", c'est-à-dire en introduisant une considération qui appartient à la sixième démonstration de Gauss. Il obtient ainsi :

$$\left(\frac{p}{q}\right) = (-1)^{(p-1)/2 \cdot (q-1)/2} \prod_{\alpha=1}^{(p-1)/2} \frac{r^{\alpha q} - r^{-\alpha q}}{r^{\alpha} - r^{-\alpha}}.$$

Le rapprochement avec la démonstration d'Eisenstein que nous venons de rappeler s'impose alors, car on reconnaît dans ce produit la valeur de $\left(\frac{q}{p}\right)$ donnée par Eisenstein. Liouville nous précise que cela

---

(*) Cette racine doit être primitive, bien que Liouville ne l'indique pas.

découle du "lemme de M. Gauss", mais que l'on pourrait se passer aussi de l'intervention de ce lemme : c'est ce que faisait aussi Eisenstein . Signalons que l'on peut aussi lire cette démonstration dans [LV2], p.92.

(35) Citons encore deux preuves élémentaires, dans le goût de la troisième et de la cinquième de Gauss.

L'une est due au pasteur Zeller et date de 1872. Elle s'appuie sur le lemme suivant : "Soit $m$ le nombre des restes minimaux nétatifs des produits $q, 2q, \ldots \frac{p-1}{2} q$ , divisés par $p$ ; soit $n$ le nombre des restes minimaux négatifs des produits $p, 2p, \ldots \frac{q-1}{2} p$ , divisés par $q$ . Les deux entiers $p$ et $q$ étant premiers impairs, la somme $m + r$ ne peut être impaire que si $p$ et $q$ sont tous deux de la forme $4k + 3$ ". Ce lemme est démontré par une suite d'inégalités. On peut lire cette démonstration reproduite dans [CH], p.122 et [NI], p.207 .

L'autre est présentée dans un article de Kronecker (Journal de Crelle n°96, 1884, p.348). Comme toujours, $p$ et $q$ sont des nombres premiers impairs distincts, et $h$ et $k$ sont des entiers respectivement compris entre 1 et $\frac{p-1}{2}$ , 1 et $\frac{q-1}{2}$ . On démontre d'abord que le signe du reste minimal de $hq$ par $p$ est celui du produit :

$$\prod_{k=1}^{(q-1)/2} \left( \frac{h}{p} - \frac{k}{q} \right) \left( \frac{h}{p} + \frac{k}{q} - \frac{1}{2} \right) .$$

Par suite, le signe de $\left( \frac{p}{q} \right)$ est celui du double produit :

$$\prod_{h=1}^{(p-1)/2} \prod_{k=1}^{(q-1)/2} \left( \frac{h}{p} - \frac{k}{q} \right) \left( \frac{h}{p} + \frac{k}{q} - \frac{1}{2} \right) .$$

On échange ensuite $q$ et $p$ , et la loi en découle.

Cette démonstration a été reprise dans [CH], p.127 , et [TA], p.474 .

(36) Les 45 premières démonstrations.

On pourrait citer de la sorte maintes publications, dif-

férant les unes des autres par des nuances, qui souvent s'inspirent peu ou prou de telle ou telle démonstration de Gauss. Ainsi, la loi de réciprocité est un des théorèmes mathématiques pour lesquels ont été publiées le plus grand nombre de démonstrations. Elle partage cette particularité avec, par exemple, le théorème de Pythagore ou le théorème fondamental de l'algèbre, de d'Alembert-Gauss.

Voici la liste des 45 premières démonstrations, d'après Bachmann ([BA], tome 1, p.203-204). Nous avons pu, dans les lignes qui précèdent, en exposer un certain nombre. L'ouvrage de Bachmann lui-même (pp.180 à 318) en rapporte plusieurs.

## Chronologische Tabelle der Beweise des Reziprozitätsgesetzes(*)

| | |
|---|---|
| 1. Gaufs, 1. Beweis, *Disqu. Ar. art.* 135 ff., 1801 (1796). | Induktion. |
| 2. „ , 2. „ , „ „ „ 257 ff., 1801. | Quadr. Formen. |
| 3. „ , 7. u. 8. Beweis, *W.* 2, p. 233 (1801) | höh. Kongruenzen. |
| 4. „ , 3. Beweis, *Comm. Gott.* 16, 1808; *W.* 2, p. 1, | Gaufs. Lemma. |
| 5. „ , 4. „ , *Comm. Gott. rec.* 1, 1809; *W.* 2, p. 9. | Kreisteilung. |
| 6. „ , 5. „ , ebend, 4. 1818; *W.* 2, p. 47. | Gaufs. Lemma. |
| 7. „ , 6. „ , an derselben Stelle. | Kreisteilung. |
| 8. Cauchy, *Bull. de Férussac* 12, 1829, p. 205. | desgl. |
| 9. Jacobi, Journ. f. Math. 30, p. 172, vgl. 35, p. 273. | desgl. |
| 10. Eisenstein, Journ. f. Math. 27, 1844, p. 322. | desgl. (arithm.) |
| 11. „ , „ „ „ 28, 1844, p. 41. | desgl. |
| 12. „ , „ „ „ 28, 1844, p. 246. | G. Lemma, (geom.) |
| 13. „ , „ „ „ 29, 1845, p. 177. | Kreist. $\left(\frac{\sin pv}{\sin v}\right)$. |
| 14. Liouville, *Journ. de Math.* 12, 1847, p. 95. | Kreist. |
| 15. Lebesgue, ebendas. p. 457. | desgl. (arithm.) |
| 16. Schaar, *Bulletin Belgique*, 14 I, 1847, p. 79. | G. Lemma. |
| 17. Genocchi, *Ac. R. Belg., mém. couronnés*, 25, 1853 (52). | desgl. |
| 18. Lebesgue, *Par. Comptes R.* 51, 1860, p. 9. | höh. Kongr. |
| 19. Kummer, zwei Beweise, *Abh. Berl. Ak.* 1861. | Quadr. Formen. |
| 20. Stern, *Gött. Nachr.* 1870, p. 237. | G. Lemma. |
| 21. Zeller, *Berl. Monatsber.* 1872, p. 846. | desgl. |
| 22. Zolotareff, *Nouv. Ann. de Math.* (2) 11, 1872, p. 354. | Permutationen. |
| 23. Kronecker, *Berl. Monatsber.* 1876, p. 301. | Induktion. |
| 24. Bouniakowsky, *Bull. St. Pét.* 22, 1876. | variirtes G. L. |
| 25. Schering, *Gött. Nachr.* 1879, p. 217. | G. Lemma. |
| *P. C. R.* 88, p. 1073. | |
| 26. Petersen, *Amer. Journ.* 2, 1879, p. 217, | var. G. L. |
| *Zeuthen, Tidskr.* 1879, p. 86. | |
| 27. Voigt, *Ztschr. f. Math. u. Phys.* 26, 1881, p. 134. | G. Lemma. |
| 28. Busche, *Dissertation, Göttingen* 1883. | desgl., Hilfssatz. |
| 29. Kronecker, *Berl. Sitzgsber.* 1884, p. 645. | G. Lemma. |
| 30. Gegenbauer, *Wiener Ber.* 1884, p. 1026; 1885, p. 876. | desgl. |
| 31. Kronecker, *Berl. Sitzgsber.* 1885, p. 117. | desgl. |
| 32. „ , „ „ 1885, p. 383, 1045. | desgl. |
| 33. Hermes, *Arch. f. Math. u. Phys.* (2) 5, 1887, p. 190. | Induktion. |
| 34. Lerch, *Teixeira Journ.* 8, 1887, p. 137. | G. Lemma. |
| 35. Busche, *J. f. Math.* 103, 1888, p. 118. | var. G. Lemma. |
| 36. „ , „ „ „ 106, 1890, p. 65. | G. Lemma. |
| 37. Lucas, *Bull. St. Pét., nouv. sér.* 1, 1890. | desgl. |
| *Assoc. franç., Limoges*, 19, 1890, p. 147. | |
| 38. Franklin, *Mess. of Math.* (2) 19, 1890, p. 176. | desgl. |
| 39. Fields, *Amer. Journ.* 13, 1891, p. 189. | desgl. |
| 40. Gegenbauer, *Wiener Ber.* 100, 1891, p. 855. | desgl. |
| 41. Schmidt, *J. f. Math.* 111, 1893, p. 107, drei Beweise, | |
| erster Beweis: | desgl. |
| zweiter Beweis: | desgl. (versteckt). |
| dritter Beweis: | Induktion. |
| 42. Gegenbauer, *Wiener Ber.* 103, 1894, p. 285. | G. Lemma. |
| 43. A. S. Bang, *N. Tidsskr. for Math.* 5 B, 1894, p. 92. | Induktion. |
| 44. Busche, *Hamburger Mitt. III*, 6, 1896, p. 233. | var. G. L. (geom.). |
| 45. Lange, drei Beweise, *Leipz. Ber.* 48, 1896, p. 629. | G. Lemma. |
| „ „ 49, 1897, p. 607. | |

(*) TABLEAU CHRONOLOGIQUE DES DEMONSTRATIONS DE LA LOI DE RECIPROCITE QUADRATIQUE

| | | |
|---|---|---|
| Induktion | - | Induction |
| Quach-Formen | - | Formes quadratiques |
| Höheren Kongruenzen | - | Congruences de degré supérieur |
| Gauss Lemma | - | Lemme de Gauss |
| Kreisteilung | - | Cyclotomie |
| Desglichen | - | Idem |
| Variirtes | - | Variante |
| Hilfssatz | - | Théorème auxiliaire |
| Versteckt | - | Dissimulé |

(37) L'idée de Zolotareff.

Parmi ces démonstrations, celle de Zolotareff (numéro 22 de la liste) nous semble mériter une mention spéciale car elle se base sur une remarque originale.

On considère $p$ premier impair et $k$ non multiple de $p$ . La suite des restes euclidiens des nombres $k, 2k, 3k, \ldots (p-1)k$ par $p$ définit une permutation de l'ensemble $\{1, 2, \ldots p-1\}$ . Alors, la signature de cette permutation est justement $\left(\frac{k}{p}\right)$ . La démonstration de ce résultat peut être trouvée dans [ZO] ou dans [DO], p.26 .

Pour en déduire la loi de réciprocité, Zolotareff utilise la permutation suivante des entiers naturels de 1 à $qp-1$ :

$$\begin{pmatrix} 1, 2, \ldots p-1, p, p+1, \ldots 2p-1, 2p, \ldots (q-1)p, (q-1)p+1, \ldots (q-1)p+(p-1) \\ q, 2q, \ldots (p-1)q, 1, 1+q, \ldots 1+(p-1)q, 2, \ldots q-1, (q-1)+q, \ldots (q-1)+(p-1)q \end{pmatrix}$$

et il démontre que la signature de cette permutation est égale à : $(-1)^{\frac{p-1}{2}\,\frac{q-1}{2}}$ .

Il obtient le résultat recherché en exprimant cette permutation comme produit d'autres permutations dont les signatures, de par son lemme initial, sont égales à $\left(\frac{p}{q}\right)$ et $\left(\frac{q}{p}\right)$ .

L'intérêt de la chose n'est assurément pas d'ajouter une démonstration supplémentaire à un théorème qui n'en avait pas besoin. Il est de mettre en lumière un lien inattendu entre la théorie des résidus quadratiques et celle des permutations.

(38) Cas des modules non premiers.

Bien sûr, les mathématiciens ne se sont pas bornés à ajouter des lignes à la liste de M. Bachmann : ils n'ont pas seulement voulu redémontrer une $n+1$-ième fois un théorème si clairement établi, mais ils ont cherché des généralisations.

La première généralisation qui vient à l'esprit concerne le caractère quadratique d'un entier selon un module non-premier. Gauss a résolu cette question dans ses Recherches Arithmétiques ([GAD], n°100, p.73 et n°140, p.108). L'existence de "racines primitives" modulo $p^\alpha$ par $p$ premier impair, nous dirions aujourd'hui le fait que le groupe multiplicatif des unités de l'anneau $\mathbb{Z}/p^\alpha\mathbb{Z}$ est cyclique, donne le résultat suivant : si $p$ ne divise pas l'entier $a$, celui-ci est résidu de $p^\alpha$ ssi il est résidu de $p$. Et pour $p = 2$, ce n'est pas plus compliqué.

Mais nous avons vu que Jacobi a défini une généralisation du symbole de Legendre, qui vérifie aussi une loi de réciprocité (cf. supra, § III, n°15). Ce symbole $\left(\frac{P}{Q}\right)$ ne fournit plus qu'une condition nécessaire pour que $P$ soit résidu de $Q$, mais là ne gît pas tout son intérêt. Le plus curieux est qu'il vérifie encore les lemmes de Gauss et de Zolotareff, ainsi que l'ont montré respectivement Schering ([SC]) et Frobenius ([FR]).

En d'autres termes, si $P$ et $Q$ sont des entiers naturels impairs premiers entre eux, et si, parmi les restes euclidiens positifs (resp. minimaux) de $Q, 2Q \ldots \frac{P-1}{2}Q$ par $P$, il y en a $m$ qui sont supérieurs à $\frac{P}{2}$ (resp. négatifs), alors on a :

$$\left(\frac{Q}{P}\right) = (-1)^m .$$

Pour une démonstrations, on peut se reporter à [CT], p.36. Dès lors, la troisième et la cinquième démonstrations de Gauss s'appliquent à ce symbole, car on pourra observer qu'elles n'utilisent que le caractère relativement premier de P et Q. Et la loi de réciprocité est démontrée. Mais il y a plus. Le lemme de Gauss pourrait servir à définir le symbole $\left(\frac{P}{Q}\right)$, et l'on pourrait ainsi retrouver les propriétés de ce symbole. C'est ainsi qu'avait procédé Schering. Sur ce point, voir [TA], p.476 et [RS], p.163.

De plus, le lemme de Zolotareff se généralise ainsi : les hypothèses posées sur $P$ et $Q$ impliquent que l'application $x \longmapsto Qx$, de $\mathbb{Z}/P\mathbb{Z}$ vers lui-même, est une permutation de cet ensemble. Alors, la signature de cette permutation est $\left(\frac{Q}{P}\right)$ (voir [CT] ou [RS]). Mais cette propriété pourrait elle aussi servir de définition du symbole de Legendre-Jacobi. Cette définition peut intervenir dans des situations plus géné-

rales. Ainsi, M. Cartier définit le symbole $\left(\begin{smallmatrix} u \\ \\ G \end{smallmatrix}\right)$ comme la signature de l'automorphisme $u$ du groupe abélien $G$ ([CT]), ce qui permet de trouver des résultats dans des corps de nombres algébriques.

## § VIII - CONCLUSION : UNITE et GENERALITE

### (39) Gauss et l'unité des mathématiques

Nous avons pu lire à plusieurs reprises dans les pages précédentes des jugements concernant "l'homogénéité" ou "l'hétérogénéité" de telle ou telle démonstration.

On peut trouver trace d'un souci analogue, par exemple, dans les "Recherches Arithmétiques", n°50, p.35 : Gauss cite une démonstration du "petit théorème" de Fermat, fondée sur les propriétés arithmétiques des coefficients binômiaux $C_p^k$ pour $p$ premier, et il dit que "le développement de la puissance d'un binôme semble étranger à la théorie des nombres".

Dirichlet, dans la citation reproduite plus haut, (§ IV, n°17), précise bien que la première démonstration de Gauss est la seule qui ne sorte pas du domaine des congruences du second degré, excluant ainsi même la troisième etla cinquième, pourtant purement arithmétiques. C'est que ces démonstrations se fondent sur le lemme de Gauss, lui-même basé sur le critère d'Euler, qui est une "congruence de degré supérieur" (supérieur à deux), comme l'on disait naguère.

En même temps, Gauss n'a pas craint de proposer des démonstrations "hétérogènes", fondées sur des principes apparemment éloignés de l'objet de la loi de réciprocité. Il a ainsi mis en lumière avec force sur cet exemple l'unité des mathématiques et a ouvert la voie aux conceptions modernes en la matière. Déjà, l'introduction de la Section VII des "Recherches Arithmétiques" contient de précieuses indications à ce sujet ([GAD], n°335, p.429) . Gauss annonce que cette section est consacrée aux fonctions circulaires qui interviennent "à chaque instant dans des recherches qui y semblent tout-à-fait étrangères". Et il avertit :

"Le lecteur pourrait s'étonner de rencontrer une semblable recherche dans un ouvrage consacré à une doctrine qui paraît au premier abord absolument hétérogène ; mais l'exposition fera voir bien clairement quelle est la liaison de ce sujet et de l'Arithmétique transcendante".

Or, cette section d'un livre d'Arithmétique contient un théorème apparemment géométrique de la plus grande importance, un progrès dans une question qui n'avait pas avancé depuis les Anciens : la possibilité de partager le cercle en 17 parties égales avec la règle et le compas. Un bel exemple de lien entre des parties des mathématiques jugées "hétérogènes"!

Nous avons déjà vu plusieurs fois Gauss attirer l'attention de ses lecteurs sur de tels rapprochements : § V, n°21 et § VI, n°30 . Citons également l'introduction de son mémoire de 1817 :

"Le théorème fondamental au sujet des résidus quadratiques, que l'on met au rang des plus belles vérités de l'arithmétique supérieure, est facile à découvrir par induction, mais bien plus difficile à démontrer. Dans ce domaine, il arrive souvent que les démonstrations de vérités très simples, qui s'offrent de façon quasi-spontanée à l'esprit du chercheur, par le moyen de l'induction, se cachent très profondément et ne puissent être amenées à la lumière qu'après bien des tentatives inutiles, et par hasard, par une autre voie que celle que l'on se proposait d'utiliser pour les atteindre. Ensuite il arrive souvent, dès que l'on a trouvé une démonstration, que plusieurs apparaissent à partir de là menant au même but, les unes brièvement et plus directement, les autres pour ainsi dire de biais, en s'appuyant sur des principes très différents, de sorte que l'on n'aurait soupçonné aucun lien entre eux et le sujet à l'étude. Un lien étonnant de ce genre entre des vérités assez obscures n'apporte pas seulement un charme particulier à ces recherches, mais mérité par là même d'être aussi étudié et élucidé avec zèle, car il n'est pas rare que la science elle-même en reçoive de nouveaux développements.

Ainsi, quoique le théorème arithmétique en question puisse être considéré comme pleinement établi par les efforts antérieurs qui ont fourni quatre démonstrations différentes les unes des autres, je reprends le même sujet, toutefois de façon nouvelle, et je lui adjoins deux autres démonstrations, qui apportent sur ce point, à coup sûr, une nouvelle lumière. La première de ces deux démonstrations a quelque affinité avec la troisième, parce qu'elle part du même lemme ; mais après elle suit

un chemin différent, au point qu'elle peut à bon droit être considérée comme une démonstration nouvelle, qui paraîtra, sinon supérieure, du moins égale en harmonie à cette troisième. Au contraire, la sixième démonstration s'appuie sur un principe subtil, tout à fait différent, et offre un nouvel exemple de l'étonnant enchaînement qui existe entre des vérités arithmétiques au premier abord très éloignées les unes des autres".

Nous avons déjà rapporté les démonstrations dont Gauss introduit l'exposé par ces lignes : la cinquième (§ V, n°26) et la sixième (§ VI, n°31). Dans cette introduction, comme dans d'autres textes déjà cités, l'auteur présente ces "enchaînements entre vérités éloignées" comme fruit du hasard. Dans la suite du développement mathématique, on sait que de telles exceptions deviendront la règle.

(40) Lois de réciprocité générales.

A la lecture de l'énorme travail que Gauss a consacré à la loi de réciprocité, on est en droit de se demander pourquoi il a ainsi multiplié les démonstrations d'une propriété qui pouvait sembler suffisamment assurée. Ses textes, que nous avons longuement cités (§ V, n°21 et § VIII,n°39), contiennent déjà une réponse à cette question. Mais la suite de l'introduction de 1817 donne une information du plus haut intérêt :

"Il y a eu encore une autre raison, qui m'a conduit à publier de préférence aujourd'hui des démonstrations nouvelles, déjà promises depuis neuf ans. C'est que depuis 1805 j'avais commencé à étudier de près la théorie des résidus cubiques et biquadratiques, sujet beaucoup plus difficile, et que je rencontrai la même fortune, qu'autrefois dans la théorie des résidus quadratiques. En effet, ces théorèmes, qui épuisent absolument ces questions, et dans lesquels apparaît une étonnante analogie avec les théorèmes concernant les résidus quadratiques, ont été trouvés immédiatement par induction, dès qu'on les étudia selon la démarche adéquate : mais tous les efforts pour s'en rendre maîtres par des démonstrations parfaites en tous points, demeurèrent longtemps vains. C'est cela qui m'incitait à m'adonner avec tant de soin à l'étude, afin d'ajouter d'autres et d'autres démonstrations à celles déjà connues concernant les résidus quadratiques, soutenu par l'espoir que, de ces méthodes nombreuses et diverses, l'une ou l'autre pourrait apporter quelque élément propre à éclairer le problème. Cet espoir ne fut absolument pas vain, et finalement d'heureux

succès ont couronné ce travail infatigable. Bientôt, il me sera permis de produire à la lumière publique le fruit de mes veilles : mais avant d'achever ce travail ardu, je suis revenu une fois encore à la théorie des résidus quadratiques, j'ai décidé d'achever tout ce qui reste à faire à ce sujet et de dire adieu, en quelque sorte, à cette partie de l'Arithmétique supérieure" ([GA2], p.50) .

Dans ses travaux, Gauss était donc mû par un désir de généralisation : il voulait établir des lois de réciprocité pour des congruences de degrés supérieurs . En 1828 et 1832, il a publié deux mémoires consacrés aux résidus biquadratiques ([GA2], pp.65, 93). C'est à ce propos qu'il devait considérer les nombres de la forme $x + iy$ , avec $x$ et $y$ entiers rationnels, nombres que l'on appellera ipso facto entiers de Gauss.

Jacobi, Eisenstein et Dirichlet ont obtenu les premiers résultats importants. Par exemple Eisenstein, dans un article déjà cité ([EI4], cf. supra, § VII, n°34), après avoir établi la loi de réciprocité quadratique à l'aide de fonctions trigonométriques "circulaires", s'attaque aux résidus biquadratiques à l'aide des fonctions elliptiques "ou plutôt cette espèce de fonctions elliptiques qui se rapportent à la lemniscate", c'est-à-dire justement celles dont parlait Gauss à la section VII des "Recherches Arithmétiques" (cf. supra, § VI, n°29 ; cf. [DD2], p.58).

L'étude des lois de réciprocités générales dans divers anneaux d'entiers algébriques s'est révélée un sujet extrêmement fécond, qui entretient des relations avec plusieurs disciplines mathématiques. Ces prolongements naturels des travaux relatés ici conduisent à de grands progrès dans la connaissance des nombres algébriques, et à la théorie du corps de classe (cf. [DD1], pp.191 sq.).

Nous ne pouvons développer plus avant ces questions, qui sortent de notre actuel propos, lequel se borne à décrire les origines, la naissance et le développement d'un théorème particulièrement remarquable, la loi de réciprocité quadratique. Ce n'est pas le moindre intérêt de ce théorème que d'avoir été à la source de tels progrès ultérieurs ; mais il s'agit là d'un autre sujet, sur lequel nous reviendrons sans doute en d'autres occasions.

# B I B L I O G R A P H I E

On ne saurait trop conseiller la fréquentation directe des sources. Mais, comme nous l'avons déjà signalé, la première difficulté dans l'étude de l'histoire mathématique est l'accès aux documents. Signalons deux éditeurs qui se sont spécialisés dans la republication de classiques mathématiques importants :

Librairie Albert Blanchard : 9, rue de Médicis 75 006 PARIS

Chelsea Publishing Compagy, Inc.
432 Park Avenue South, New-York, N Y 10016 .

Deux revues, qui paraissent depuis le dix-neuvième siècle, contiennent des articles intéressant notre sujet et reviennent plusieurs fois dans la bibliographie : elles sont connues sou es noms de " Journal de Liouville " et " Journal de Crelle " . Leur titre exact et complet est respectivement :

- Journal de mathématiques pures et appliquées .
- Journal für die reine und angewandte Mathematik .

★

★ ★

Les ouvrages cités ici se répartissent en quatre catégories :

S - Sources : ouvrages classiques mathématiques (Fermat, Euler, Gauss, ...)

H - Histoire des mathématiques .

HN - Ouvrages de théorie des nombres à orientation historique, qui constituent une bonne introduction à l'étude des classiques .

RQ - Ouvrages mathématiques traitant de la réciprocité quadratique .

La catégorie à laquelle appartient chaque texte est indiquée après son titre .

*

* *

[AP] T.M. Apostol , Introduction to analytic number theory . Springer - Verlag , 1976 . (RQ) .

[BA] Bachmann , Niedere Zahlentheorie. Vol. I, 1902 ; Vol. II, 1910 . Réimpression en un volume, Chelsea, 1968 . (HN) .

[BC] Z.I. Borevitch et I.R. Chafarevitch , Théorie des Nombres . Gauthier - Villars, 1967 . (RQ) .

[BO] E. Borel , Les Nombres Premiers . " Que Sais-Je " N°571, PUF 1953 . (HN).

[BU] P.M. Burton , Elementary Number Theory . Allyn Bacon, 1976 . (RQ) .

[CA1] A. Cauchy , Oeuvres, Série II, tome 2 . (S) .

[CA2] A. Cauchy , Oeuvres , Série I, tome 3 . (S) .

[CH] E. Cahen , Eléments de la théorie des nombres . Gauthier - Villars , 1900 . (RQ) .

[CL] E. Callandreau , Célèbres problèmes de mathématiques . Albin Michel , 1949 . (RQ) .

[CO1] J.P. Collette , Histoire des mathématiques . Editions du Renouveau Pédagogique, Québec, 1973, tome 1 . (H) .

[CO2] J.P. Collette , Id. , tome 2 , 1979 . (H) .

[CR] L. Carlitz , A note on Gauss' first proof of the quadratic reciprocity theorem . Proc. Am. Math. Soc. Vol. 11 , n°4 , August 1960 ; (HN) .

[CT] P. Cartier , Sur une généralisation des symboles de Legendre - Jacobi . L'enseignement Mathématique , IIe série , tome XVI , Fascicule 1 , Janvier - Avril 1970 . (HN) .

[CC] R. Cuculière , La Théorie des Nombres, de LeGendre et les Recherches Arithmétiques de Gauss) . Bulletin A.P.M.E.P. N°324, juin 1980 . (H) .

[CY] A. Cayley , Mathématical papers , Vol. III . (S) .

[DD1] J. Dieudonné & Coll , Abrégé d'histoire des mathématiques , tome 1 . Hermann , 1978 . (H) .

[DD2] J. Dieudonné & Coll , Id. tome 2 . (H) .

[DI] Diophante d'Alexandrie , les six livres arithmétiques et le livre des nombres polygones . Traduction, introduction et notes de Paul Ver Eecke, Librairie Blanchard , 1959 . (S) .
(voir aussi |HE|) .

[DK2] L.E. Dickson , History of the theory of numbers, Vol. II . Première édition 1919 ; réimpression Chelsea 1971 . (HN) .

[DK3] L.E. Dickson , Id. , Vol. III . (HN) .

[DR] M. Dörrie , 100 great problems of elementary mathematics . Dover , 1965 . (RQ) .

[DO] M. Dourakine , Problèmes corrigés de mathématiques . Collection DIA , diffusion Belin , 1979 . (RQ) .

[ED] Edwards , Last Fermat's theorem . Springer-Verlag , 1977 . (HN) .

[EI1] G. Eisenstein , Einfacher Algorithmus zur Bestimmung der Werthes von $\left(\frac{a}{b}\right)$. Journal de Crelle , Tome 27 . (S) .

[EI2] G. Eisenstein , Geometrischer Beweis der Fundamental theorems für die quadratischen Reste . Journal de Crelle , tome 28 , p.246 . (S) .

[EI3] G. Eisenstein , La loi de réciprocité tirée des formules de M. Gauss , sans avoir déterminé préalablement le signe du radical . Journal de Crelle , tome 28 , p.41 . (S) .

[EI4] G. Eisenstein , Applications de l'Algèbre à l'Arithmétique transcendante. Journal de Crelle, tome 29 , p.177 . (S) .

[EU] L. Euler . (S) .
Pour les commentaires de L. Euler, nous avons repris la classification numérique de : G. Enestrom, Verzeichnis der Schriften Leonhard Euler (Leipzig 1910) .

[EU54] Theorematum quorundam ad numeros primos spectantium demonstratio (1736), Opera Omnia (1) 2, p.33 .

[EU134] Theoremata circa divisores numerorum (1747 - 48) , Opera Omnia (1) 2, p.70 .

[EU164] Theoremata circa divisores numerorum in hac forma paa ± qbb contentorum (1751) , Opera Omnia (1) 2, p.194 .

[EU228] De numeris, qui sunt aggregata duorum quadratorum (1752 - 53), Opera Omnia (1) 2, p.295 .

[EU242] Demonstratio theorematis Fermatiani omnem numerum sive integrum sive fractum esse summan quatuor pauciorumve quadratorum (1754 - 55) , Opera Omnia (1) 2, p.338 .

[EU256] Specimen de usu observationum in mathesi pura (1756 - 57) , Opera Omnia (1) 2, p.531 .

[EU272] Supplementum quorundam theorematum arithmeticorum , quae in nonnullis demonstrationibus supponantur (1760 - 61) , Opera Omnia (1) 2, p.556 .

[EU552] Observationes circa divisionem quadratorum per numeros primos (1783) , Opera Omnia (1) 3, p.497 .

[EU610] Novae demonstrationes circa divisores numerorum formae xx + nyy (1783) , Opera Omnia (1) 4, p.197 .

[FE1] P. de Fermat, Oeuvres, tome I . (S)

[FE2] P. de Fermat, Oeuvres, tome II . (S)

[FE3] P. de Fermat, Oeuvres, tome III . (S)

[FE4] P. de Fermat, Oeuvres, tome IV . (S)

Publiées par P. Tannery et C. Henry . Gauthier-Villars, 1891 - 1912 .

[FO] E. Fourrey , Curiosités géométriques . Vuibert , 1907 . (H) .

[FR] Frobenius , Gesammelte Abhandlungen . (Band III) Springer 1968 . (S) .

[GA1] F. Gauss , Werke , Band I . Göttingen 1870 . (S) .

[GA2] F. Gauss , Werke , Band II . Göttingen 1876 . (S) .

[GAD] F. Gauss , Recherches arithmétiques . Traduites par A.C.M. Poullet - Delisle , première édition 1807 , réimpression Librairie Blanchard , 1953 . (S) . (il existe une réimpression de 1979) .

[GO] R. Godement , Cours d'Analyse, Polycopié, Paris, Université Paris 7, 1977 . (RQ) .

[HE] Sir Thomas Heath , Diophantus of Alexandria . Seconde édition 1910 , republication Dover 1964 . (H) .

[HW] G. H. Hardy & E.M. Wright , An introduction to the theory of numbers . 4th edition 1960 , republication Oxford 1975 . (RQ) . (il existe une 5e édition , 1979) .

[IT1] J. Itard , Arithmétique et théorie des nombres . " Que sais-je " n°1093 , PUF 1963 . (HN) .

[JT2] J. Itard , Les nombres premiers . " Que sais-je " n°571 , PUF 1969 . (RQ) .

[JA1] C.G. Jacobi , Ueber die complexen Primzahlen , welche inder theorie ... Journal de Crelle , tome 19 , p.314 , 1839 . (S) .

[JA2] C.G. Jacobi , Mathematische Werke , Band 6 . Réédition Chelsea . (S) .

[KL] Morris Kline , Mathematical thought from ancient to modern time . N.Y. Oxford University Press , 1972 . (H) .

[KU] E.E. Kummer , Collected Papers . Springer . (S) .

[LA] J.L. Lagrange , Oeuvres , tome III . Gauthiers-Villars . (S) .

[LB] V.A. Lebesgue , Sur le symbole $\left(\frac{a}{b}\right)$ et quelques-unes de ses applications . Journal de Liouville , série 1 , tome 12 , 1847 . (S) .

[LD1] G.P. Lejeune - Dirichlet , Math. Werke . Band I , 1889 . (S) .

[LD2] G.P. Lejeune - Dirichlet , Math. Werke . Band II , 1897 . Réimpression en un volume , Chelsea , 1969 . (S) .

[LD3] G.P. Lejeune - Dirichlet , Uber den ersten der von Gauss Gegebenen Beweise des Reciprocitäts gesetzes in der Theorie der quadratischen reste. Journal de Crelle 1857 , Band 47 , S. 139-150 . Mathematische Werke , Band II, p.121 .

Traduction française dans le journal de Liouville, 2e série, tome IV, 1859 : "sur la première démonstration par Gauss de la loi de réciprocité dans la théorie des résidus quadratiques". (S) .

[LG1] A.M. Legendre , Recherches d'Analyse indéterminée . Histoire de l'Académie Royale des Sciences, Volume de 1785 , pp.465 à 559 . (S) .

[LG2] A.M. Legendre , Théorie des Nombres . 4e édition , tome 1 . (S) .

[LG3] A.M. Legendre , Théorie des Nombres . 4e édition , tome 2 . (S) .

[LI] J. Liouville , Sur la loi de réciprocité dans la théorie des résidus quadratiques . Journal de Liouville , tome XII , 1847 . (S) .

[LN] S. Lang , Algebraic number theory . Addison-Wesley , 1970 . (RQ).

[LP] Léonard de Pise , le livre des nombres carrés . Traduction, introduction et notes de Paul Ver Eecke , Desclée de Brouwer , Bruges , 1952 . (S) .

[LU] E. Landau , Elementary number theory . Première édition , 1927 . Réimpression Chelsea , 1966 .

[LV1] W.J. LeVeque , Topics in Number Theory . Addison-Wesley , 1958 , Vol. I . (RQ) .

[LV2] W.J. LeVeque , Id., Vol. II . (RQ) .

[LV3] W.J. LeVeque , Fundamentals of Number Theory . Addison-Wesley , 1978 . (HN)

[MA] G.B. Mathews , Number theory . Première édition Cambridge 1892 ; réimpression Chelsea . (HN) .

[MI] J. Milnor , Introduction to algebraic K-theory . Princeton University Press , 1971 . (RQ) .

[MO] Mordell , On a simple summation of the series $\sum_{s=0}^{n-1} e^{2s^2\pi i/n}$ .

Messenger of Math. , Vol. XLVII , May 1917 - April 1918 , p.54 . (RQ) .

[NA] T. Nagell , Introduction to Number Theory . J. Wiley & Sons , 1951 . (RQ) .

[NI] B. Niewenglowski , Questions d'arithmétique . Vuibert 1927 . (RQ) .

[OC] M. D'Ocagne , Histoire abrégée des Sciences Mathématiques . Vuibert , 1952 . (H) .

[RE] Abel Rey , La jeunesse de la science grecque . Albin Michel , 1933 . (H) .

[RI] P. Ribenboim, L'arithmétique des corps . Hermann . (RQ) .

[RO] J. Roberts , Elementary Number theory - a problem oriented approach .
the MIT Press, 1977 . (RQ) .

[RS] M. Riesz , Sur le lemme de Zolotareff et sur la loi de réciprocité des restes quadratiques , Math. Scand., 1, 1953 , p.159 - 169 . (HN) .

[SA] P. Samuel , Théorie algébrique des nombres . Hermann , 1967 . (RQ) .

[SC] E. Schering , Zur theorie der quadratischen Resten . Acta Math. 1 (1882) pp.153 - 170 . (S) .

[SE] J.P. Serre , Cours d'Arithmétique . PUF , 1970 . (RQ) .

[SI] W. Sierpinski , Elementary Number theory . Warszawa , 1964 . (RQ) .

[SM] H.J.S. Smith , The collected Mathematical papers of Henry John Stephen Smith , Volume I . Réimpression Chelsea . (HN) .

[TA] J. Tannery , Leçons d'Arithmétique théorique et pratique . Armand Colin , 1884 . (RQ) .

[UN] Encyclopaedia Universalis : articles:Euler, Gauss, formes quadratiques , théorie des nombres.

[VE] B.A. Venkov , Elementary Number Theory . (HN) .

[WA] A. Warusfel , Structures algébriques finies . Hachette , 1971 . (RQ) .

[WE1] A. Weil , Essais historiques sur la théorie des nombres . Monographie n°22 de l'Enseignement Mathématique . (H) .

[WE2] A. Weil , Number theory for beginners . Springer-Verlag , 1979 . (RQ) .

[ZO] M. Zolotareff , Nouvelle démonstration de la loi de réciprocité de LeGendre . Nouvelles Annales de Math., 2e série, tome 11, 1872, pp.354 - 362 . (S) .

UNIVERSITÉ PARIS 13
I.R.E.M.
99, Avenue Jean-Baptiste Clément
93430 VILLETANEUSE
Tél. 01 49 40 36 40