Résidus quadratiques
Lois de réciprocité quadratique

Cyril Banderier

Maîtrise de mathématiques pures
Université de Rouen
Septembre 1997

Directeur du travail d'étude et de recherche :

M. Legris

Table des matières

CHAPITRE 1

Prolégomènes

Ce mémoire a pour but d'éclairer divers liens entre la notion de résidu quadratique et de nombreux pans de la théorie des nombres (au sens large, cela va de la théorie additive, multiplicative des nombres – l'arithmétique – à la théorie algébrique des nombres en passant par la théorie analytique des nombres et en poussant jusqu'à la théorie des corps de classes). On aura ainsi un aperçu de la profondeur de la notion de résidu, tout en oscillant souvent entre prospective et épistémologie, entre démonstration et digression. On verra aussi quelques applications industrielles (traduire : *algorithmiques*).

Toutefois, pour des raisons de limitation (du nombre de pages et des connaissances de l'auteur), bien souvent, seuls les résultats sont cités, les démonstrations se trouvant dans les livres cités dans la bibliographie ou dans les articles cités dans ce mémoire. Cependant, un résultat aussi puissant que la loi de réciprocité d'Artin n'est même pas démontré dans l'ardu *Corps locaux* de J.P. Serre, qui renvoie à un livre de théorie des corps de classes. On trouvera dans nos pages quelques autres rouleaux compresseurs. Néanmoins, divers résultats d'arithmétiques seront démontrés aux chapitres 2 et 3, dont *last but not least* la loi de réciprocité quadratique, serpent de mer de ce TER. Nous espérons que le lecteur aura autant de plaisir que nous à se promener à travers les notions qui nous ont été offertes par deux siècles d'algèbre, voire d'analyse. Et maintenant, commençons à ouvrir nos horizons en définissant le champ de bataille.

CHAPITRE 2

Épisode premier : résidus historiques

1. Legendre, Gauss, Jacobi et les autres...

Définition : a est résidu quadratique modulo n (ou encore résidu quadratique de n) si et seulement si a est un carré dans $\mathbb{Z}/n\mathbb{Z}$. Eh oui ! C'est aussi simple que cela.

Exemple : Dans $\mathbb{Z}/6\mathbb{Z}$: $0 = 0^2, 1 = 1^2 = 5^2, 3 = 3^2, 4 = 2^2 = 4^2$ sont des résidus quadratiques ; 2 et 5 sont non résidus (sous entendu : quadratiques modulo 6).

Le terme "résidu quadratique" est fort poétique mais nous nous efforcerons, lorsqu'il n'y aura pas ambiguïté, à employer le terme "carré" ; ce dernier ayant l'avantage d'être bien plus explicite que le terme "résidu quadratique" qui, ne faisant qu'esbroufe, ralentit la compréhension des énoncés. Par ailleurs, nous dirons que deux nombres sont "étrangers" plutôt que de dire qu'ils sont "premiers entre eux", évitant ainsi une polysémie néfaste.

La notion de résidu quadratique apparaît dans un mémoire d'Euler de 1754–1755. D'aucuns, qui ne sont pas mathématiciens, se diront que c'est encore là une futilité de matheux, d'autres, qui le sont, se diront que c'est là une futilité d'arithméticien. Eh bien ! Nous allons nous efforcer, tout au long de ce mémoire, de démontrer le profond intérêt de cette *futilité*, de ces carrés carrément sans intérêt.

Les jolies formules se succéderont mais, étant conscient que l'esthétique n'est pas un motif d'intérêt pour beaucoup, nous verrons donc, pour ces réfractaires, quelques applications avec les tests de primalité, dont le test de Pépin. Cette miette mathématique est également à la base d'algorithmes de factorisation, avec la méthode de Gauss et celle de Kraïtchik (1920), ancêtre du moderne "algorithme de factorisation par crible quadratique" de Carl Pomerance (1990). La lecture du § 6.1 explicitera ce qu'on peut entendre par intérêt.

Comment savoir si a est un carré modulo n ? Construire la table des carrés de $\mathbb{Z}/n\mathbb{Z}$ devient vite fastidieux, si n est grand. Legendre donne un algorithme simple pour répondre à cette question. Celui-ci repose sur un résultat puissant de la théorie des nombres : la loi de réciprocité quadratique. Le premier à l'avoir énoncée (sans preuve) est Euler en 1783, après l'avoir frôlée en 1772. Indépendamment, Legendre l'énonce en 1785 avec une preuve incomplète, toujours insuffisante dans sa *Théorie des nombres*, en 1798. Gauss en trouva une preuve à l'âge de 18 ans, au bout d'un an de recherches, et en exposera la première démonstration rigoureuse dans ses *Recherches arithmétiques* en 1801.

Gauss considérait cette loi comme le joyau de l'arithmétique, l'appelant même le “théorème d'or” ; il en donnera sept démonstrations différentes. Aujourd'hui, des spécialistes en ont recensé au moins 163, on pourra en trouver une produite par un générateur informatique de théorèmes dans *A mechanical proof of quadratic reciprocity*, Journal of Automated Reasoning, 1992 de D. Russinoff et nous vous renvoyons à l'American Mathematical Monthly d'avril 1963 pour l'énoncé de la 152^e preuve de la loi de réciprocité quadratique, qui comme la plupart est basée sur le lemme de Gauss (voir § 4.4). En métamathématique, on dit qu'un tel théorème, aux démonstrations foisonnantes, a un degré d'ambiguïté élevé. Il en est de même, par exemple, du théorème de Pythagore ou du théorème de l'infinitude des nombres premiers. On en trouvera une douzaine copurchics dans [Ribenboim][1] ; nous en donnerons une dans le § 4.9 sur les progressions arithmétiques.

En revanche, le théorème des nombres premiers, qui a fêté l'an dernier son centenaire, n'est pas ambigu : il n'a pour l'instant que deux démonstrations. En effet, quoique conjecturé depuis Legendre et Gauss, et après des progrès dus à Tchebychev et Riemann, il ne fut prouvé qu'en 1896, par Hadamard et de La Vallée-Poussin, indépendamment l'un de l'autre. Ce n'est qu'en 1949 qu'on en trouva une démonstration 'élémentaire' (i.e. n'utilisant ni la fonction ζ de Riemann ni la théorie des fonctions holomorphes) due à Erdös et Selberg (médaille Fields en 1950). On trouvera une version améliorée de cette démonstration dans [Francinou].

La plus simple manifestation des lois de réciprocité est celle, déjà connue par Pierre de Fermat, qui affirme que les seuls diviseurs premiers de $x^2 + 1$ sont 2 et des nombres premiers du type $1 + 4k$ (voir § 4.3.1). Avec l'aide du symbole de Legendre, ceci se note

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

2. Lois de réciprocité d'ordre supérieur

La loi de réciprocité de Gauss a été généralisée à des congruences du type $x^n \equiv a\ [p]$ $(n > 2)$; on parle de réciprocité cubique pour $n = 3$, de réciprocité biquadratique ou quartique pour $n = 4$, de réciprocité quintique pour $n = 5$ ... Ceci impose une transition de l'arithmétique sur $\mathbb{Q}$ vers une arithmétique sur une extension finie $\mathbb{K}$ de $\mathbb{Q}$. Une telle extension de $\mathbb{Q}$ ou d'un corps fini $\mathbb{F}_p(X)$ est nommée un corps global, par opposition aux corps locaux [Serre 2] qui sont les complétés d'un corps de nombres algébriques, pour sa valeur absolue : c'est-à-dire soit $\mathbb{R}$, soit $\mathbb{C}$, soit les corps de nombres p-adiques (théorème d'Ostrowski). Un corps de nombres (algébriques) est une extension finie de $\mathbb{Q}$ contenue dans $\mathbb{C}$.

[1] Les noms entre crochets renvoient aux références bibliographiques à la fin du document.

Dans la généralisation aux résidus énièmes, l'extension doit contenir ζ, une racine énième primitive de l'unité (i.e. $\zeta^n = 1$ et $\zeta^k \neq 1 \, \forall k < n$). Nous désignerons, conventionnellement voire traditionnellement, un idéal premier par la lettre $\mathfrak{P}$ (ou $\mathfrak{p}$), P majuscule (ou minuscule) en alphabet gothique, en honneur à l'école algébrique allemande : en effet Kummer a introduit ses 'nombres idéaux' en 1844 [Dahan], puis Dedekind a développé la théorie des idéaux premiers. Dedekind, dans le *Supplément aux " Vorselungen über Zahlentheorie " de Dirichlet*, 1871, a introduit explicitement les notions de corps, d'anneau, de module et d'idéal.

Les idéaux premiers $\mathfrak{P}$ de $\mathbb{K}$ qui ne divisent pas n vérifient $N_{\mathfrak{P}} \equiv 1 \; [n]$ où $N_{\mathfrak{P}}$ est la norme de l'idéal $\mathfrak{P}$, égale au nombre de classes du plus grand ordre du corps modulo $\mathfrak{P}$, dit plus simplement, $N_{\mathfrak{P}}$ est le cardinal de $\mathbb{A}/\mathfrak{P}$ lorsque $\mathfrak{P}$ est un idéal de l'anneau $\mathbb{A}$ des entiers du corps $\mathbb{K}$. L'analogue du symbole de Legendre est défini par $\left(\frac{a}{\mathfrak{P}}\right)_n \equiv \zeta^k \equiv a^{(N_{\mathfrak{P}}-1)/n} \; [\mathfrak{P}]$. Tout comme pour le symbole de Jacobi, si $(b) = \prod_i \mathfrak{P}_i^{m_i}$ est la décomposition de l'idéal principal (b) en idéaux premiers, et si a et b sont des entiers algébriques étrangers, alors : $\left(\frac{a}{b}\right)_n = \prod_i \left(\frac{a}{\mathfrak{P}_i}\right)_n^{m_i}$. Si, avec ce symbole de résidu n-ième, on a $\left(\frac{a}{\mathfrak{P}}\right) = 1$, alors il existe un entier algébrique $b \in \mathbb{A}$ tel que $b^2 \equiv a \; [\mathfrak{P}]$.

La loi de réciprocité pour $n = 4$ dans le corps $\mathbb{Q}(i) = \mathbb{Q}(e^{2i\pi/4})$ a été établie par Gauss. Pour $n = 3$ dans le corps $\mathbb{Q}(e^{2i\pi/3})$, elle a été établie par Eisenstein : *Beweis des Reziprozitätgesetze für cübischen Reste*, J. Math., 1844, utilisant la formule

$$\sum_{k=1}^{m-1} \sin \frac{2k\alpha\pi}{m} \cot \frac{k\pi}{m} = m - 2\alpha$$

(valable pour $1 \leq a < m$). Kummer dans *Allgemeine Reziprozitätgesezte beliebig hohe Potentzreste*, Ber. K. Akad. Wiss., 1850, a établi la loi générale de réciprocité pour le symbole des résidus de degré p dans le corps $\mathbb{Q}(e^{2i\pi/p})$, pour p premier. Dans le chapitre sur les nombres premiers réguliers p (voir § 7.3), on donnera une loi de réciprocité dans $\mathbb{Q}(e^{2i\pi/p})$.

3. Le neuvième problème de Hilbert

En 1900, à Paris, lors du II^e Congrès international des Mathématiciens, Hilbert avait dressé une liste de 23 problèmes ouverts qui lui semblaient fondamentaux et dont la résolution était un défi pour le XX^e siècle. Le neuvième de ces problèmes consistait à établir une loi de réciprocité dans les corps de nombres algébriques.

On pourra remarquer que plusieurs sujets de T.E.R., outre le nôtre, recoupent des problèmes mis en évidence par Hilbert : le quatrième sur les géométries non euclidiennes, le septième sur la transcendance de certains nombres, le dix-huitième sur les pavages (de l'espace), le vingtième sur le problème de Dirichlet ...

A cette époque, une nouvelle étape dans la recherche de lois de réciprocité générales avait été franchie par Hilbert avec ses deux articles : *Die Theorie der algebraischen Zahlkörper* et *Über die Theorie der relativquadratischen Zahlkörpern*, Jahresber. Deutsch. Math., 1897 et 1899, dans lesquels il a éclairci leurs aspects locaux. Il avait établi, dans certains cas, une loi de réciprocité pour le symbole de Hilbert :

$$\prod_{\mathfrak{P}} \left(\frac{a, b}{\mathfrak{P}} \right) = 1.$$

Il avait aussi noté l'analogie entre cette formule et le théorème sur les résidus d'une fonction algébrique : ses points réguliers (dont la norme de Hilbert $\neq 1$) correspondent aux points de branchements sur une surface de Riemann (i.e. une variété analytique complexe de dimension 1).

La première moitié du XX^e siècle a vu diverses avancées dans l'étude des lois de réciprocité dues à Furtwängler, Artin, Hasse et Takagi. La loi de réciprocité dans les corps quadratiques dans le cas général est due à [Hecke] et la forme la plus élaborée a été obtenue par une apothéose due à I.R. Shafarevich : *A general reciprocity law*, Uspekhi Mat. Nauk., 1948.
Elle est, tout comme la loi de réciprocité de Gauss, très liée à l'étude de la décomposition d'un idéal $\mathfrak{P}$ d'un corps de nombres algébriques $\mathbb{K}$ dans une extension algébrique $\mathbb{L}/\mathbb{K}$ à groupe de Galois abélien. En particulier, la théorie des classes, qui donne la solution de ce problème, peut être basée sur la loi de réciprocité de Shafarevich comme l'ont fait Lapin, Cassels et [Neukirch].

Au jour d'aujourd'hui (redondance pléonastique voire superfétatoire ?), il reste quelques grandes conjectures offertes au monde mathématique. Gageons qu'elles figureront sur la liste des problèmes ouverts pour le XXI^e siècle.

Nous citerons les suivantes, qui sont plus ou moins en rapport avec notre sujet : – la conjecture de Riemann affirme que la fonction ζ (une fois prolongée analytiquement à $\mathbb{C} - \{1\}$) ne s'annule que sur la droite Re(z)=1/2 (à l'exception des zéros triviaux $-2\mathbb{N}^*$). La conjecture de Riemann généralisée affirme la “même chose” pour les L-séries de Dirichlet. Ces dernières sont définies par

$$L(s, \chi) = \sum_{n=1}^{\infty} \chi(n) n^{-s}$$

où χ est un caractère modulo k. La convergence a lieu si $\mathrm{Re}(s) > 0$ pour les caractères non principaux. Un caractère est un homomorphisme d'un groupe $\mathbb{G}$ dans le groupe multiplicatif $\mathbb{C}^*$. Il est dit principal s'il est constamment égal à 1 (on aurait pu plus simplement l'appeler caractère trivial). χ_k, le caractère modulo k, est défini par $\chi_k(n) = 0$ si $(n, k) \neq 1$ et par $\chi_k(n) = \chi(n \bmod k)$ sinon. On a l'équivalent de l'identité d'Euler :

$$L(s, \chi) = \prod_p (1 - \chi(p) p^{-s})^{-1}.$$

Les L-séries interviennent dans la démonstration du théorème de la progression arithmétique (voir § 4.9). Il y a un lien important entre la factorisation de polynômes sur des corps finis et la conjecture de Riemann, de plus le rapport entre la factorisation de polynômes et la notion de résidu quadratique (ou d'ordre supérieur) transpire au regard de l'équation $x^n \equiv a\ [p]$.

– la conjecture P $\neq$ NP : tout problème résoluble en temps polynomial non déterministe est-il résoluble en temps polynomial ? C'est-à-dire : si on peut vérifier une solution en temps polynomial, peut-on la trouver en temps polynomial ? Bien sûr, quelque soit la réponse, il restera toujours à trouver des algorithmes de complexité minimale pour une multitude de problèmes ... On connaît l'importance de tels progrès, et les retombées qu'ils pourraient avoir, en cryptographie notamment, puisque cette dernière est basée sur l'hypothèse que la factorisation ou que le logarithme modulaire sont NP.

– les mathématiciens, du moins ceux qui ne sont pas trop découragés par la réponse négative de Matijasevich au dixième problème de Hilbert (on s'est même demandé si le problème de Fermat n'était pas indécidable !), n'ont toujours pas résolu moult équations diophantiennes (Waring, Catalan).

– on ignore encore si de nombreuses familles de nombres vérifiant telle propriété sont finies : par exemple les nombres premiers jumeaux $(p, p+2)$, repunits $(1 \ldots 1)$, de Mersenne $(2^n - 1)$, de Fermat $(2^{2^n} + 1)$, de Cullen $(n2^n \pm 1)$, de Sophie Germain $(p, 2p+1)$, réguliers (voir § 7), de Wieferich $(2^{p-1} \equiv 1\ [p^2])$, de Wilson $((p-1)! \equiv -1\ [p^2])$ [Guy].

– voici, pour finir, un problème important de la théorie des nombres : la conjecture ABC. Soit $\mathcal{E}$ l'ensemble des triplets (A, B, C) d'entiers vérifiant

$$\frac{\ln \max(|A|, |B|, |C|)}{\ln R} \geq \eta$$

avec $A + B = C$ et pgcd(A, B, C)=1 et où R est le plus grand entier sans carré divisant ABC. La conjecture affirme que $\mathcal{E}$ est fini. La conjecture ABC généralisée affirme la même chose avec des n-uplets.

Pour les connexions entre la conjecture ABC et différents grands problèmes de la théorie des nombres, on pourra consulter [Granville] et la thèse d'A. Nitaj : *Conséquences et aspects de conjectures ABC et de Spiro*, université de Caen, 1994. Par exemple, le lien avec le grand théorème de Fermat se fait en posant : $a^p = A, b^p = B, c^p = C$ et alors, puisque $A + B = C$, on est ramené à l'étude de la courbe elliptique $y^2 = x(x - A)(x + B)$ de discriminant $(4ABC)^2$ (voir § 8.2). D'après une idée de G. Frey, K. Ribet a montré en 1988 qu'une courbe elliptique associée à des solutions de $a^p + b^p = c^p$ ne peut être modulaire. Or la conjecture de Taniyama-Weil (1955, 1967) implique que les courbes de Frey sont modulaires. Wiles (en juin 1993, puis comblant le fameux 'trou' avec R. Taylor en septembre 1994) a démontré un cas suffisamment large de cette conjecture pour impliquer la contradiction. Notons par ailleurs que, en 1977, G. Terjanian a utilisé la loi de réciprocité quadratique pour démontrer un cas général du 'premier cas du théorème de Fermat' (i.e. l'équation mod n).

CHAPITRE 3

Épisode second : un peu de symbolique

“ Un symbole est une concrétisation d'une réalité abstraite. Le sens étymologique du mot grec σύμβολον, dérivé du verbe συμβάλλω, “je joins”, définit un objet partagé en deux, la possession de chacune des deux parties par deux individus différents leur permettant de se rejoindre et de se reconnaître. [...] Le champ du symbole peut-il être limité ? Il semble que non. ” Encyclopædia Universalis, article “symbole”.

1. Le symbole de Legendre

On définit $\left(\frac{a}{p}\right)$ pour p premier comme égal à 1 si a est un carré dans $\mathbb{Z}/p\mathbb{Z}$, à -1 sinon. Ce symbole est multiplicatif :

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Ceci est dû au fait que le produit de deux carrés est un carré, (ceci est toujours vrai dans un groupe cyclique $\mathbb{Z}/n\mathbb{Z}$) et que, si nous sommes dans $\mathbb{Z}/p\mathbb{Z}$, p **premier**, alors le produit d'un carré par un non carré est un non carré et le produit de deux non carrés est un carré.

On peut aussi énoncer le fait suivant :
g est un générateur du groupe cyclique $\mathbb{G} \Longrightarrow g$ est un non carré. La réciproque est vraie si $\#\mathbb{G} - 1 = 2^k$.

La loi de réciprocité pour le symbole de Legendre affirme

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

Ainsi, de même que dans l'algorithme d'Euclide pour le calcul du PGCD ou que dans le test de primalité par descente-remontée (voir § 6.3), on est ramené, de proche en proche, à traiter des nombres de plus en plus petits.

L'intérêt d'une stratégie de “rapetissement progressif du problème” transparaît dans l'algorithme de calcul du pgcd de $(a, b) =: (r, s)$, dont voici l'algorithme :

```
DEBUT
tant que s ≠ 0 faire (r,s) := (s, r mod s) ;
(* on crunche et squeeze avec allégresse *)
retourner r ;
FIN
```

2. Le symbole de Jacobi

On trouvera dans [Naudin] une approche du symbole de Jacobi par Zolotarev basée sur la signature d'une permutation. Nous utiliserons la définition classique. On prolonge le symbole de Legendre par $\left(\frac{a}{b}\right) = 0$ si a est un multiple de b. Pour $a \in \mathbb{Z}$ et b entier impair, on définit le symbole de Jacobi par $\left(\frac{a}{b}\right) = \prod_i \left(\frac{a}{p_i}\right)$ avec $b = \prod_i p_i$ décomposition de b en facteurs premiers.On peut d'ores et déjà remarquer que $\left(\frac{a}{b}\right) = 0$ si et seulement si a et b ne sont pas étrangers.
Ainsi, si a est un carré modulo b (b étant étranger avec a) alors $\left(\frac{a}{b}\right) = 1$. On remarquera aussi que $\left(\frac{a}{b}\right) = -1 \Longrightarrow a$ est non carré modulo b mais qu'on peut avoir $\left(\frac{a}{b}\right) = 1$ sans que a soit un carré modulo b. Exemple : $\forall a \in \mathbb{Z}$ $\left(\frac{a}{9}\right) = \left(\frac{a}{3}\right)\left(\frac{a}{3}\right) = 1$, or $a = 5$ n'est pas un carré dans $\mathbb{Z}/9\mathbb{Z}$. Il est facile de voir que le symbole de Jacobi est un symbole totalement bimultiplicatif : il est totalement multiplicatif en sa première variable car

$$\left(\frac{a_1 a_2}{b}\right) = \left(\frac{a_1}{b}\right)\left(\frac{a_2}{b}\right)$$

et il est totalement multiplicatif en sa deuxième variable car

$$\left(\frac{a}{b_1 b_2}\right) = \left(\frac{a}{b_1}\right)\left(\frac{a}{b_2}\right).$$

Par conséquent, la loi de réciprocité, une fois démontrée pour le symbole de Legendre (ce que nous ferons dans le chapitre suivant), vaut aussi pour le symbole de Jacobi ; on obtient la **loi de réciprocité généralisée** :

$$\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right)(-1)^{\frac{(a-1)(b-1)}{4}}.$$

La multiplicativité du symbole de Jacobi en fait un *caractère* réel, on a vu l'importance de cette notion au § 2.3.

3. Application

713 est-il un carré modulo le premier 1009 ? En utilisant la loi de réciprocité quadratique et le calcul de $\left(\frac{2}{p}\right)$ fait au § 4.5, on a aisément :

$$\left(\frac{713}{1009}\right) = \left(\frac{1009}{713}\right)(-1)^{\frac{(1008)(712)}{4}} = \left(\frac{296}{713}\right)(+1) = \left(\frac{8.37}{713}\right) = \left(\frac{8}{713}\right)\left(\frac{37}{713}\right)$$
$$= \left(\frac{2}{713}\right)\left(\frac{37}{713}\right) \underbrace{=}_{\text{car } 713\equiv\pm1\ [8]} (+1)\left(\frac{37}{713}\right) = \left(\frac{713-740}{37}\right) = \left(\frac{-27}{37}\right)$$
$$= \left(\frac{10}{37}\right) = \left(\frac{2}{37}\right)\left(\frac{5}{37}\right) \underbrace{=}_{\text{car } 37\not\equiv\pm1\ [8]} (-1)\left(\frac{2}{5}\right)(-1)^{\frac{(4)(36)}{4}} = (-1)(-1)(+1) = 1.$$

Ainsi $\left(\frac{713}{1009}\right) = 1$ donc 713 est bien un carré modulo 1009.

CHAPITRE 4

Quelques démonstrations de la loi de réciprocité

“ Les problèmes posés par les nombres entiers nécessitent de tels travaux et de telles réflexions que, finalement, c'est de là que sortent à peu près la moitié des théories mathématiques [...] Il y a beaucoup de mathématiciens à la suite de Bourbaki qui pensent que c'est la théorie des ensembles qu'il faut mettre au départ ; eh bien ! je ne le pense pas, je pense que c'est la théorie des nombres, des nombres entiers. ” Charles Pisot.

1. Savez-vous compter les résidus...

Ce paragraphe et les suivants sont directement recopiés sur [Francinou], ces derniers étant eux-mêmes parfois directement repiqués sur [Hardy] ... Mais puisque ni une démonstration ni une mise en page ne peut être copyrightée, n'ayons pas d'état d'âme et saluons ainsi ces deux ouvrages de références, quoiqu'aux ambitions différentes.

Soit $p \geq 3$ un nombre premier (notation conservée dans TOUT ce chapitre). $f\ : x \in (\mathbb{Z}/p\mathbb{Z})^* \mapsto x^2$ est un endomorphisme du groupe multiplicatif du corps $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Son noyau est {-1, +1}, les racines de $X^2 - 1$. Le noyau étant de cardinal 2, l'image de f est de cardinal Card($\mathbb{F}_p^*$)/Card(Ker$f$)= $\frac{p-1}{2}$. Il y a donc $\frac{p-1}{2}$ carrés dans $(\mathbb{Z}/p\mathbb{Z})^*$. 0 étant aussi un carré, $\mathbb{F}_p$ contient $\frac{p+1}{2}$ carrés.

2. Critère d'Euler

$\forall x \neq 0, (x^{(p-1)/2})^2 = x^{p-1} \equiv 1[n]$ donc $x^{(p-1)/2}$ est dans Ker$f = \pm 1$. Im(f) est un sous-groupe de F_p^* de cardinal $\frac{p-1}{2}$. Si x est un carré non nul, on a $x \in$ Im (f) et donc $x^{(p-1)/2} = (y^2)^{(p-1)/2} = y^{p-1} \equiv 1[p]$. D'autre part, remarquons que l'ensemble des racines du polynômes $X^{(p-1)/2} - 1$ contient les $\frac{p-1}{2}$ carrés non nuls. Or ce polynôme a au plus $\frac{p-1}{2}$ racines. Donc les racines de $X^{(p-1)/2} - 1$ et les carrés non nuls coïncident.

On en déduit le critère d'Euler : x est carré non nul si et seulement si

$$x^{(p-1)/2} = 1.$$

En résumé, avec le symbole de Legendre : $\left(\frac{x}{p}\right) \equiv x^{(p-1)/2}\ [p]$.

Il est intéressant de citer le **critère d'Euler généralisé** aux résidus n-ièmes : en posant $q = pgcd(n, p-1)$, $x^n \equiv a\ [p]$ est résoluble si et seulement si $a^{\frac{p-1}{q}} \equiv 1\ [p]$

et il y a alors q racines modulo p. On a donc, au total, $1+(p-1)/q$ résidus n-ièmes et $(q-1)(p-1)/q$ non résidus dans $\mathbb{Z}/p\mathbb{Z}$.

Vinogradov a par ailleurs montré que le nombre R de résidus quadratiques compris entre 1 et $n \leq p-1$ est $R = \frac{1}{2}n + \theta\sqrt{p}\ln p$ où $|\theta| \leq 1$ et a formulé l'hypothèse que la distance entre deux non résidus est $O(p^{\varepsilon})$, Linnik a d'ailleurs montré que c'était "presque toujours" le cas. En outre, le plus petit non résidu quadratique est $\leq p^{1/(2\sqrt{e})}(\ln p)^2$.

3. Calcul de $\left(\frac{-1}{p}\right)$

En appliquant le critère d'Euler à -1, on obtient : -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $(-1)^{(p-1)/2} = 1$, i.e. si et seulement si $(p-1)/2$ est pair.

En résumé : -1 est carré modulo $p \iff p = 4n+1$.

3.1. Application sur les diviseurs de $a^2 + b^2$.

$a^2 + b^2 \equiv 0\ [p] \iff$ (avec $r = a^2 \bmod p$ et $r' = b^2 \bmod p$) $r + r' \equiv 0\ [p] \iff r' \equiv -r\ [p] \iff r'q \equiv -1\ [p]$ où q est l'inverse de r, l'ensemble des carrés de $\mathbb{Z}/p\mathbb{Z}$ étant un groupe multiplicatif, q et donc qr' sont aussi des carrés. D'où $-1 = r'q$ est un carré modulo p or on vient de voir que ceci équivaut à $p = 4n+1$.

Les lecteurs attentifs ne devraient pas être parvenus à cette étape sans avoir au moins froncé les sourcils : en effet les lignes précédentes mal recopiées sur [Itard] souffrent d'une imperfection (euphémisme). Justifierez-vous cette litote en trouvant quelle est l'équivalence aporétique ?

Solution : Il suffit de remplacer $\mathbb{Z}/p\mathbb{Z}$ par $(\mathbb{Z}/p\mathbb{Z})^*$ qui lui sera bien un groupe multiplicatif. En effet, si $r \equiv 0\ [p]$, il ne sera pas inversible. On peut pallier cet inconvénient, si r ou r' n'est pas nul (ce qui revient à ce que tous deux soient non nuls), ainsi l'achoppement fatal saute si p ne divise ni a ni b, a fortiori si a et b sont étrangers, hypothèse apodictique et même salvatrice.

En résumé : **les seuls diviseurs d'une somme de deux carrés étrangers sont 2 et des nombres premiers de la forme $4n+1$.**
Un résultat de Fermat affirme même qu'un nombre premier de la forme $4n+1$ est somme de deux carrés ; en 1977, Larson en a donné une démonstration qui utilise le placement de n reines sur un échiquier $n \times n$ sans qu'aucune ne soit en prise.

4. Lemme de Gauss

Soit p un premier impair. Pour $n \in \mathbb{N}$, on appelle résidu minimal de n (modulo p) l'unique entier $n' \in]-p/2, p/2[$ tel que $n \equiv n'\ [p]$. Soit $m \in \mathbb{N}$, non multiple de p. On note μ le nombre d'entiers de $\{m, 2m, \ldots, \frac{p-1}{2}m\}$ dont le résidu minimal est strictement négatif.

Montrons que $\left(\frac{m}{p}\right) = (-1)^{\mu}$.

Posons $\lambda = \frac{p-1}{2} - \mu$. Considérons l'ensemble des résidus minimaux de

$$\{m, 2m, \ldots, \frac{p-1}{2}m\}.$$

Soient $r_1, \ldots, r_\lambda$ les résidus minimaux positifs et $-r'_1, \ldots, -r'_\mu$ les résidus minimaux strictement négatifs. Comme les éléments de $\{m, 2m, \ldots, \frac{p-1}{2}m\}$ ne sont pas congrus deux à deux, les r_i sont distincts deux à deux. Il en va de même des r'_i. Montrons par l'absurde que pour tout $(i,j), r_i \neq r'_j$. Soient donc a et b dans $\{1, 2, \ldots, (p-1)/2\}$ tels que $am \equiv r_i = r'_j \equiv -bm$ $[p]$. Alors $0 \equiv am + bm \equiv (a+b)m$ $[p]$. p ne divisant pas m, p divise $a+b$ ce qui est impossible car $0 < a+b < p$. Ainsi, $\{r_1, r_2, \ldots, r_\lambda, r'_1, r'_2, \ldots, r'_\mu\} = \{1, 2, \ldots, \frac{p-1}{2}\}$.
On peut donc écrire modulo p :
$m.2m.3m \ldots \frac{p-1}{2}.m \equiv (-1)^\mu r_1 r_2 \ldots r_\lambda . r'_1 r'_2 \ldots r'_\mu \equiv (-1)^\mu \frac{p-1}{2}!$

Comme p ne divise pas $\frac{p-1}{2}!$, il vient : $m^{\frac{p-1}{2}} \equiv (-1)^\mu$ $[p]$ donc, d'après le critère d'Euler :

$$\left(\frac{m}{p}\right) = (-1)^\mu.$$

Le lemme de Gauss peut être utilisé pour déterminer les nombres premiers pour lesquels un entier préalablement choisi est un carré. C'est ce que nous allons faire avec les entiers 2 et -3 pour obtenir quelques formules, souvent appelées "complémentaires".

5. Calcul de $\left(\frac{2}{p}\right)$

Nous allons montrer que $\left(\frac{2}{p}\right) = (-1)^{E(\frac{p+1}{4})} = (-1)^{\frac{p^2-1}{8}}$ où $E(x)$ désigne la partie entière de x, i.e. le plus petit entier $\leq x$.

Il s'agit de calculer μ pour $m = 2$, i.e. le nombres de résidus minimaux de $\{2, 4, \ldots, p-1\}$ strictement négatifs.
On est donc ramené à compter les entiers k tels que : $p/2 < 2k < p$.
On vérifie aisément que si $p \equiv 1$ $[4], \lambda = \frac{p-1}{4}$ et $\mu = \frac{p-1}{2} - \frac{p-1}{4} = \frac{p-1}{4}$.
Si $p \equiv 3$ $[4], \lambda = E(\frac{p-1}{4}) = \frac{p-3}{4}$ et $\mu = \frac{p-1}{2} - \frac{p-3}{4} = \frac{p+1}{4}$.
Ainsi, dans tous les cas : $\mu = E(\frac{p+1}{4})$. Notons $r = 2\frac{p-1}{4}\frac{p+1}{4} = \frac{p^2-1}{8}$. Ainsi $r \in \mathbb{N}$ et si $p \equiv 1$ $[4]$ (resp. $p \equiv 3$ $[4]$), r a la même parité que $\frac{p-1}{4}$ (resp. $\frac{p+1}{4}$). Donc, dans tous les cas, r a même parité que μ et : $\left(\frac{2}{p}\right) = (-1)^r = (-1)^{\frac{p^2-1}{8}}$.

En résumé : 2 est un carré modulo $p \Longleftrightarrow p = 8n \pm 1$.

6. Calcul de $\left(\frac{-3}{p}\right)$

Il s'agit de calculer μ pour $m = -3$, i.e. le nombres de résidus minimaux de $\{-3, -6, \ldots, -3\frac{p-1}{2}\}$ strictement négatifs. On est donc ramené à compter les entiers k tels que : $p/2 < -3k < p$.

- Si $1 \leq k < p/6$ alors $p/2 < p - 3k \leq p - 3 < p$, les résidus minimaux sont strictement négatifs.
- Si $p/6 < k < p/3$ alors $0 < p - 3k < p/2$, les résidus minimaux ne sont pas strictement négatifs, donc on ne retient pas ces valeurs de k.
- Si $p/3 < k < p/2$ alors $p/2 < 2p - 3k < p$, les résidus minimaux sont strictement négatifs.

Ainsi, les valeurs de k pour lesquelles les résidus minimaux sont strictement négatifs sont : $1, 2, \ldots, E(p/6)$ et $E(p/3)+1, E(p/3)+2, \ldots, E(p/2)$ donc $\mu = E(p/6) + E(p/2) - E(p/3)$. D'où si $p = 6n+1$ alors $\mu = n + 3n - 2n$ est pair et si $p = 6n+5$ alors $\mu = n + (3n+2) - (2n+1)$ est impair.

En résumé : -3 est un carré modulo $p \geq 5 \iff p = 6n+1$.

7. Calcul de $\left(\frac{5}{p}\right)$

p, car premier > 5, est de la forme $10n + k$ où k vaut 1,3,7 ou 9. Nous appliquons alors la loi de réciprocité quadratique :

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)(-1)^{\frac{p-1}{2}\frac{5-1}{2}} = \left(\frac{10n+k}{5}\right) = \left(\frac{k}{5}\right).$$

Or dans $(\mathbb{Z}/5\mathbb{Z})^*$, les seuls carrés sont 1 et 4, d'où $\left(\frac{k}{5}\right) = 1$ pour $k = 1, 9$ et $\left(\frac{k}{5}\right) = -1$ pour $k = 3, 7$.

En résumé : 5 est un carré modulo $p \iff p = 10n \pm 1$.

On montre également : 7 est un carré modulo $p \iff p \equiv \pm 1, \pm 3, \pm 9$ [28].

Avec ces quelques résultats et la bimultiplicativité du symbole de Jacobi, il vous est désormais possible de calculer très rapidement $\left(\frac{a}{b}\right)$. Par exemple, $\left(\frac{3}{p}\right)$ peut s'obtenir comme combinaison des résultats précédents sur $\left(\frac{-1}{p}\right)$ et $\left(\frac{-3}{p}\right)$, on obtient ainsi :
3 est un carré modulo $p \iff p = 12n \pm 1$.

8. Quod erat demanstrandum

Soient p et q deux nombres premiers impairs, $p \neq q$. On écrit $p = 2p' + 1$ et $q = 2q' + 1$. Pour tout $k \in \{1, 2, \ldots, q'\}$, on note $(-1)^{e_k} r_k$ (où $1 \leq r_k \leq q'$ et $e_k \in \{0, 1\}$) le résidu de kp modulo q de plus petite valeur absolue.

8.1. Primo.

Soit $\alpha \in \mathbb{Z}$ avec $kp = q\alpha + (-1)^{e_k} r_k$. Alors $\alpha = kp/q - (-1)^{e_k} r_k/q$.
On a $0 < |(-1)^{e_k} r_k/q| < 1/2$. Si $e_k = 0, \alpha \in]\frac{kp}{q} - \frac{1}{2}, \frac{kp}{q}[$ et nécessairement, $\alpha = E(kp/q) = E(kp/q) + e_k$. Si $e_k = 1, \alpha \in]\frac{kp}{q}, \frac{kp}{q} + \frac{1}{2}[$ et nécessairement, $\alpha = E(kp/q) + 1 = E(kp/q) + e_k$.

Ainsi $kp = q(E(\frac{kp}{q}) + e_k) + (-1)^{e_k} r_k$.

8.2. Secundo.

Montrons que $\{r_1, \ldots, r'_q\} = \{1, \ldots, q'\}$.

Il suffit de prouver que si $k \neq l$ alors $r_k \neq r_l$. Soit $(k, l) \in \{1, 2, \ldots, q'\}^2$. Si $r_k = r_l$, on obtient modulo $q : 0 \equiv (-1)^{e_k} kp - (-1)^{e_l} lp \equiv p(\pm k \pm l)$. D'où $\pm k \pm l \equiv 0\ [q]$, et comme $| \pm k \pm l| \leq 2q' < q, \pm k \pm l = 0$ et nécessairement $k = l$. CQFD.

8.3. Tertio.

Cette démonstration est aussi celle qui figure dans *La loi de réciprocité quadratique*, Revue de Mathématiques Spéciales, mars 1990 par P. Delezoide. Ce dernier en profite d'ailleurs pour faire quelques remarques d'ordre géométrique qui figurent également dans [Hardy]. On note $J_q^p = \prod_{h=1}^{p'} \prod_{k=1}^{q'} \frac{hq-kp}{|hq-kp|}$. Notons que J_q^p est bien défini puisque pour tout $(h, k), hq - kp \neq 0$. Fixons k. Alors dire que $hq - kp \leq 0$ revient à dire $1 \leq h \leq kp/q$. Il y a donc $E(kp/q)$ valeurs de h pour lesquelles $hq - kp \leq 0$. Ainsi $J_q^p = \prod_{k=1}^{q'} (-1)^{E(kp/q)}$. En passant modulo 2 la relation du primo, on obtient $k \equiv E(kp/q) + e_k + r_k$ [2]. Donc $J_q^p = \prod_{k=1}^{q'} (-1)^{k - r_k + e_k} = (-1)^{(\sum_{k=1}^{q'} k) - (\sum_{k=1}^{q'} r_k) + (\sum_{k=1}^{q'} e_k)}$. Or $(\sum_{k=1}^{q'} k) - (\sum_{k=1}^{q'} r_k = 0)$ d'après le secundo. Il en résulte $J_q^p = \prod_{k=1}^{q'} (-1)^{e_k}$. La relation du primo donne $kp \equiv (-1)^{e_k} r_k\ [q]$. Donc $J_q^p \equiv \prod_{k=1}^{q'} \frac{kp}{r_k} \underbrace{\equiv}_{secundo} p^{q'} \equiv \left(\frac{p}{q}\right)\ [q]$. Comme $J_q^p \in \{\pm 1\}$, on a bien $J_q^p = (\frac{p}{q})$.

8.4. In fine.

On a, d'après ce qui précède,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \prod_{h=1}^{p'} \prod_{k=1}^{q'} \frac{hq-kp}{|hq-kp|} \frac{kp-hq}{|kp-hq|} = (-1)^{p'q'}$$

ce qui démontre la loi de réciprocité quadratique.

9. Un petit théorème de progression arithmétique

Soit $n \geq 3$. Soit p un nombre premier divisant $n!^2 + 1$. Nécessairement $p > n$. De plus, en passant modulo p, on a $n!^2 + 1\ [p] = 0\ [p]$ d'où $n!^2 \equiv -1\ [p]$, i.e. -1 est le carré de $n!$. Donc $p \equiv 1\ [4]$ d'après le théorème sur $\left(\frac{-1}{p}\right)$. Avec le même raisonnement appliqué à $p!^2 + 1$, on obtient un autre nombre premier $\equiv 1\ [4]$. Ainsi, de proche en proche, on construit une suite infinie : il existe une infinité de nombres premiers congrus à 1 mod 4. Ce qui montre, incidemment, qu'il existe une infinité de nombres premiers (voir § 2.1 de notre exorde).

On peut également montrer, avec des notions élémentaires d'arithmétique, qu'il y a une infinité de nombres premiers du type $4k + 3, 6k + 5, 8k + 5$. Mais ce résultat a la généralisation suivante : pour a et b étrangers, la suite $an + b$

contient une infinité de nombres premiers. C'est le célèbre théorème de la progression arithmétique démontré en 1837 par Dirichlet dont on pourra trouver une démonstration dans [Serre 1] ou dans [Dieudonné]. Aucune d'entre elle n'est vraiment élémentaire ; elles sont toutes analytiques et elles marquent d'ailleurs le début de la théorie analytique des nombres. C'est tout le génie de Dirichlet d'avoir su repérer la fécondité d'un mariage entre l'analyse et l'arithmétique, hyménée que des mathématiciens comme Riemann, Tchebychev et Hardy entretiendront par la suite. En fait, en partant de l'identité d'Euler, il a introduit les séries de Dirichlet [Ogg] et la notion de caractère d'un groupe abélien fini $\mathbb{G}$ pour en arriver à ce que l'on nomme aujourd'hui le théorème de Dirichlet.

10. Quod erat demanstrandum (bis repetita placent)

Parmi les nombreuses démonstrations de la loi de réciprocité, il en est qui utilisent les corps finis. En voici donc une seconde, une tirée de [Naudin]. On considère un sur-corps Ω_p de $\mathbb{F}_p$ contenant une racine ω de l'unité, d'ordre q. On introduit la somme de Gauss : $\tau = \sum_{x\in\mathbb{F}_q{}^*} \left(\frac{x}{q}\right) \omega^x$. Gauss les a utilisées pour sa sixième (1808) et huitième (1818) preuve de la loi de réciprocité. On remarquera, puisque $\omega^q = 1$, que $x \in \mathbb{F}_q \mapsto \omega^x \in \Omega_p$ est bien définie et vérifie $\omega^{x+y} = \omega^x\omega^y$. Dans le corps Ω_p, τ est une racine carrée de $\pm q$, comme le montre le lemme suivant.

10.1. Lemme sur la somme de Gauss.

Avec les notations précédentes, on a : $\tau^2 = \left(\frac{-1}{q}\right) q$. Preuve : On a

$$\tau^2 = \tau.\tau = (\sum_x \left(\frac{x}{q}\right) \omega^x)(\sum_y \left(\frac{y}{q}\right) \omega^y) = \sum_{x,y} \left(\frac{xy}{q}\right) \omega^{x+y}.$$

Réalisons le changement de variable $y = xz$ et, en utilisant

$$\left(\frac{xy}{q}\right) = \left(\frac{x}{q}\right)^2 \left(\frac{z}{q}\right) = \left(\frac{z}{q}\right),$$

on a :

$$\tau^2 = \sum_z \left(\frac{z}{q}\right) \sum_x \omega^{x(1+z)}.$$

Or

$$\sum_{t\in\mathbb{F}_q} \omega^t = 1 + \omega + \cdots + \omega^{p-1} = 0,$$

par conséquent

$$\sum_{t\in\mathbb{F}_q^*} \omega^t = -1.$$

Si $z \neq -1$, l'application $x \mapsto x(1+z)$ est une permutation de $\mathbb{F}_q^*$ donc

$$\sum_x \omega^{x(1+z)} = -1$$

et donc
$$\tau^2 = \left(\frac{-1}{q}\right)(q-1) + \sum_{z\neq -1} - \left(\frac{z}{q}\right).$$
Si on utilise maintenant le fait qu'il y a dans $\mathbb{F}_q^*$ autant de carrés que de non carrés, ce qui entraîne
$$\sum_{x\in\mathbb{F}_q^*} \left(\frac{x}{q}\right) = 0,$$
on obtient ce que l'on voulait :
$$\tau^2 = \left(\frac{-1}{q}\right)(q-1) + \left(\frac{-1}{q}\right) = \left(\frac{-1}{q}\right) q.$$

Une généralisation abstraite (le théorème de Kronecker-Weber) affirme que tout corps de nombres algébriques dont le groupe de Galois sur $\mathbb{Q}$ est commutatif est un sous-corps d'un corps cyclotomique.

10.2. Retour à notre seconde preuve de la loi de réciprocité.

La somme de Gauss $\tau \in \Omega_p$ est une racine carrée de $\left(\frac{-1}{q}\right) q$; il s'ensuit que $\left(\frac{-1}{q}\right) q$ est un carré dans $\mathbb{F}_p$ si et seulement si $\tau \in \mathbb{F}_p$. Rappelons à cette occasion qu'un élément $\theta \in \Omega_p$ appartient à $\mathbb{F}_p$ si et seulement si $\theta^p = \theta$: en effet, le polynôme $X^p - X$ a au plus p racines dans le corps Ω_p et tous les éléments de $\mathbb{F}_p$ sont racines. Le calcul de τ^p est facilité par le fait que nous sommes en caractéristique p :
$$\tau^p = \sum_{x\in\mathbb{F}_q^*} \left(\frac{x}{q}\right)\omega^{px} = \left(\frac{p}{q}\right)^{-1} \sum_{y\in\mathbb{F}_q^*} \left(\frac{y}{q}\right)\omega^{y} = \left(\frac{p}{q}\right)\tau.$$
On en déduit que $s{-}1qq$ est un carré dans $\mathbb{F}_p$ si et seulement si p est un carré modulo q. Il vient donc :
$$\left(\frac{p}{q}\right) = \left(\frac{\left(\frac{-1}{q}\right) q}{p}\right) = \left(\frac{(-1)^{\frac{q-1}{2}}}{p}\right)\left(\frac{q}{p}\right) = \left(\frac{-1}{p}\right)^{\frac{q-1}{2}}\left(\frac{q}{p}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$
QED.

CHAPITRE 5

Extraction de racine carrée

“ Votre mémoire est fort bien fait, vous y avez inclus deux de vos derniers théorèmes qui m'ont l'air très prometteurs. Vous avez trouvé une astuce très jolie pour montrer l'unicité de la décomposition mais vous n'avez pas montré l'existence et pour cause ... Je vous renvoie à l'article de Mantnie qui vient de démontrer que vous nous avez parlé de l'ensemble vide ! ” Un directeur de thèse.

Puisque nous savons désormais facilement si un nombre est un carré ou non, il est temps de donner une méthode *effective* de calcul de la racine carrée [Naudin]. Le cas où la caractéristique est 2 étant trivial (car alors $x^2 = x$), nous ne perdons rien à supposer que nous sommes dans un corps $\mathbb{K}$ de caractéristique $\neq 2$. Notons $\#\mathbb{K}$ son cardinal, on a alors u carré si et seulement si $u^{\frac{\#\mathbb{K}-1}{2}} = 1$.

Si $\#\mathbb{K} \equiv 3\ [4]$, la racine carrée s'obtient directement par $\sqrt{u} = u^{\frac{\#\mathbb{K}+1}{4}}$, que l'on calculera rapidement en utilisant l'algorithme d'exponentiation dichotomique. Si $\#\mathbb{K} \equiv 1[4]$, on a deux célèbres méthodes :

1. Méthode de Zassenhauss-Cantor

En voici l'algorithme, sachant que $\#\mathbb{K} - 1 = 2^k q$ avec q impair et que la norme est définie par

$$N(a + b\overline{X}) = (a + b\overline{X})(a + b\overline{X})^{\sigma} = a^2 - ub^2.$$

```
DEBUT
répéter
choisir ''au hasard'' t ∈ 𝕂 ;
y := t + X̄ ;
si N(y) = 0 alors retourner t ; (* N(y) = t² − u ⟹ t = √u *)
sinon z = a + bX̄ := y^q ;
tant que z ∉ 𝕂
Si N(z − 1) = 0 alors retourner (a − 1)b⁻¹
sinon si N(z + 1) = 0 alors retourner (a + 1)b⁻¹ ;
z := z² ;
fin( tant que )
(* le y = t + X̄ était défavorable, on va en essayer un autre *)
fin( répéter )
FIN
```

2. Méthode de Shanks

On écrit toujours $\#\mathbb{K} - 1 = 2^k q$ avec q impair. Or

$$(u^{\frac{q+1}{2}})^2 = u.u^q \iff u = (u^{\frac{q+1}{2}})^2 (u^q)^{(-1)} \iff \sqrt{u} = u^{\frac{q+1}{2}} \sqrt{(u^q)^{-1}}.$$

Pour trouver la racine carrée de u, on est donc ramené, d'après la formule magique ci-dessus, à élaborer un algorithme d'extraction de racine carrée de u^{-q} qui est élément d'un sous-groupe $\mathbb{G}$ cyclique, d'ordre 2^k.

ω étant un générateur de $\mathbb{G}$, voici l'algorithme :

DEBUT
$(x, z, h, a) := (u^q, u^{\frac{q+1}{2}}, k, \omega)$;
On calcule le plus petit j tel que $x^{2^j} = 1$;
Si $j = k$ alors on s'arrête car u n'est donc pas un carré ;
tant que $j \neq 0$ (* $ux = z^2$, $\mathrm{Ord}(a) = 2^h$, Ord $x = 2^j, j < h$ *)
$(x, z, h, a) := (xa^{2^{h-j}}, za^{2^{h-j-1}}, j, a^{2^{h-j}})$;
Calculer le plus petit j tel que $x^{2^j} = 1$;
fin(tant que)
Retourner z ; (* $x = 1$ et z est une racine carrée de u *)
FIN

3. Et maintenant, extrayons !

Nous allons calculer une racine carrée de $x_0 = 160$ dans $\mathbb{Z}/641\mathbb{Z}$ avec la méthode Shanks. On a $p = 641 = 5.2^7 + 1$, *i.e.* $q = 5$, $k = 7$ et on peut vérifier que $\omega = 21$ est un générateur de $\mathbb{G}$.

$x_0^{2^4} = -1 \Longrightarrow (x_0\omega^{2^2})^{2^4} = x_0^{2^4} \times \omega^{2^6} = (-1) \times (-1) = 1$

On pose $x_1 = x_0\omega^{2^2} = 256$, si bien que $x_1^{2^4} = 1$. On vérifie que x_1 est d'ordre 8, d'où :

$x_1^{2^2} = -1 \Longrightarrow (x_1\omega^{2^4})^{2^2} = x_1^{2^2} \times \omega^{2^6} = (-1) \times (-1) = 1$

On pose $x_2 = x_1\omega^{2^4} = 487$, si bien que $x_2^{2^2} = 1$. On vérifie que x_2 est d'ordre 4, d'où :

$x_2^2 = -1 \Longrightarrow (x_2\omega^{2^5})^2 = x_2^2 \times \omega^{2^6} = (-1) \times (-1) = 1$

Et on s'arrête car $x_3 = x_2\omega^{2^5} = 1 = x_1\omega^{2^4}\omega^{2^5} = x_0\omega^{2^2}\omega^{2^4}\omega^{2^5} = x_0\omega^{52}$, si bien que $x_0 = (x_0\omega^{26})^2$ i.e. $\sqrt{x_0} = 160 \times 308 = 564$.

CHAPITRE 6

Réciprocité et tests de primalité

"... both Gauss and lesser mathematicians may be justified in rejoicing that there is one science (number theory) at any rate, and their own, whose very remoteness from ordinary human activities should keep it gentle and clean." G.H. Hardy, A Mathematician's Apology.

1. Résidus démocratiques

Hardy ne pouvait deviner que, peu de temps après sa mort, l'avènement de l'informatique devait démentir ses propos, à un point tel, qu'aux USA, les militaires ont interdit la divulgation de certaines avancées en théorie des nombres, les classant comme "technologies sensibles". L'inventeur, en 1984, du programme de codage *Pretty Good Privacy*, Philipp Zimmermann est même menacé de prison pour avoir distribué (librement) son programme en dehors des USA via Internet. En France, les outils servant au codage des informations sont toujours considérés comme des "armes de guerre de deuxième catégorie qui peuvent mettre en péril la Défense et la Sécurité nationale" [Science et Vie Micro d'avril 1997]. Ainsi, l'auteur de ce TER, pour avoir consciencieusement appliqué une démarche scientifique d'expérimentation de P.G.P., est passible d'une amende de 6000 à 300 000F et/ou 1 à 3 mois d'emprisonnement (confer les lois du 29/12/90, 11/07/91 et 28/12/92). Dans la plupart des autres pays, l'utilisation est désormais légale, seule l'exportation est parfois interdite, aux États-Unis par exemple.

Rappelons la recette du système de codage à clef publique R.S.A., inventé par Ron Rivest, Adi Shamir et Len Adleman en 1977 : prenez deux nombres premiers p et q ; vous obtenez ainsi un entier $n = pq$. Prenez maintenant un entier e, qui est appelé la clef, tel que $2 < e < \varphi(n)$ et qui soit étranger avec $\varphi(n) = (p-1)(q-1)$; on peut donc appliquer le théorème de Bézout pour trouver $1 < d < \varphi(n)$ et k tels que $ed + \varphi(n)k = 1$. Vous rendez publics n et d (par exemple, ils peuvent être mis dans l'annuaire à côté de votre numéro de téléphone). La formule magique $M^{ed} \bmod n = M$ (conséquence du théorème d'Euler $a^{\varphi(n)} \equiv 1 \bmod n$) est alors à la base de ce codage. Dès ce moment, on peut vous envoyer un message par $C = M^d \bmod n$ que vous seul pourrez décrypter en calculant $C^e \bmod n = M$, de plus, vous pouvez certifier que vous êtes bien l'auteur de vos messages par $C = M^e \bmod n$, vous seul pouvant fournir un tel C, ce que tout chacun pourra vérifier en calculant $C^d \bmod n = M$.

Il ne faut pas négliger la cryptographie comme fondement mathématique des démocraties de demain, on peut penser non seulement, comme c'est déjà le cas depuis une vingtaine d'année, aux applications bancaires, et aux échanges, plus récents, de courrier avec signature numérique mais également à des possibilités de démocraties directes avec vote électronique. Nombreux sont les pessimistes qui craignent une société "Big Brotherisée" et d'autres, pour un point de vue tout à fait opposé, semblant raviver le poncif anarchistes versus ultrasécuritaires, avancent que ces outils de confidentialité serviront avant tout à des organisations mafieuses. Ils pourront arguer de cette récente affaire basque où l'E.T.A. a demandé la plus forte rançon de tous les temps, communiquant par E-mail crypté avec la famille pour tenir la police à l'écart. Mais sont-ce bien de tels arguments qu'il faille avancer pour justifier l'interdiction de la cryptographie ?

2. Critère de Pépin sur les nombres de Fermat

Soit $p = F_n = 2^{2^n} + 1$ un nombre de Fermat premier, avec $n \geq 2$.
Montrons qu'un élément est un générateur de $U(\mathbb{F}_p)$ (l'ensemble des inversibles) si et seulement s'il n'est pas résidu quadratique.

Un générateur du groupe des inversibles n'est pas un résidu quadratique. Réciproquement, si x n'est pas résidu quadratique, cela signifie que

$$-1 = \left(\frac{x}{p}\right) \equiv x^{\frac{p-1}{2}} \ [p]$$

et puisque l'ordre de x divise une puissance de 2, cet ordre est exactement $p-1$.

Montrons que 3, 5 et 7 sont des générateurs de $U(\mathbb{F}_p)$, si $n \geq 2$.

D'après la loi de réciprocité quadratique, si $p \neq 5$, alors 5 est un carré modulo p si et seulement si p est un carré modulo 5. Or $p = 4^{2^{n-1}} + 1 \equiv 2$ [5] et 2 n'est pas un carré modulo 5. De la même manière, on montre que si $p \neq 3$, alors 7 est un carré modulo p si et seulement si p est un carré modulo 7. Or p est congru à 3 ou 5 modulo 7 et les seuls carrés modulo 7 sont 1, 2 et 4.

Montrons finalement le critère de Pépin :

$$p = F_n \text{ estpremier} \iff 3^{\frac{p-1}{2}} \equiv -1 \ [F_n].$$

Supposons la congruence vérifiée. On a $3^{p-1} \equiv 1$ $[p]$; l'ordre de 3 modulo p est exactement $p-1$. L'anneau $\mathbb{Z}/p\mathbb{Z}$ est donc un corps. Réciproquement, supposons p premier ; tout revient à voir que 3 n'est pas un carré modulo p. On remarque que $p \equiv 2$ [3] n'est pas un carré modulo 3, et donc, comme ci-dessus, 3 n'est un carré modulo p (sauf, bien sûr, si p=3).

On fait également appel aux résidus quadratiques pour montrer la première implication [Naudin] du test de Lucas-Lehmer sur les nombres de Mersenne : un nombre de Mersenne $M_n = 2^n - 1$ $(n \geq 3)$ est premier $\iff L_{q-2} \equiv 0$ $[M_q]$ où $L_0 = 4$ et $L_{i+1} = L_i^2 - 2$ $[M_q]$.

Notons qu'on a ainsi obtenu les 36 nombres premiers M_q pour q= 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433, 1257787, 1398269 et 2976221. $M_{2976221}$ est en outre le plus grand nombre premier actuellement connu (c'est-à-dire en septembre 1997, voir le site web cité ci-dessous pour évité de colporter des informations surannées). Il arrive souvent que le record du "plus grand nombre premier connu" soit battu par des nombres de Mersenne, de par la facilité d'implémentation du test (quoique ce dernier nécessite, pour des nombres aussi grands, l'utilisation de cet outil puissant qu'est la transformée de Fourier rapide, théorie développée en 1965 par Cooley et Tuckey puis par Schönhage et Strassen). Soyons assurés que le prochain record sera également un nombre de Mersenne et qu'il sera trouvé, comme les derniers, par D. Slowinski sur des super-ordinateurs Cray ou par le projet international accessible sur Internet (www.mersenne.org) où tout un chacun peut offrir un peu de sa puissance CPU.

3. Un test de primalité

Si, pour x non multiple de p, $x^{p-1} \not\equiv 1$ $[p]$, alors p n'est pas premier (contraposée du petit théorème de Fermat). On a la "réciproque " : si $x^{n-1} \bmod n = 1$ et $x^{(n-1)/p} \bmod n \neq 1$ pour tout facteur premier p de $n-1$ alors n est premier. C'est la base même du test de primalité par descente-remontée (ou downrun) dont voici un exemple tiré de [Knuth] :
$n_0 = 378668090616600572642192533 97$;
puisque $3^{n_0-1} \bmod n_0 = 1$, n_0 est sûrement premier.
$n_0 - 1 = 2.2.19.107.353.n_1$ avec $n_1 = 13191270754108226049301$;
puisque $3^{n_1-1} \bmod n_1 \neq 1$, n_1 est composé.
En effet $n_1 = 91813.n_2$ où $n_2 = 143675413657196977$;
puisque $3^{n_2-1} \bmod n_2 = 1$, n_2 est sûrement premier.
$n_2 - 1 = 2^4.3^2.547.n_3$ et $n_3 = 1103.n_4$ où $n_4 = 1653701519$;
puisque $3^{n_4-1} \bmod n_4 = 1$, n_4 est sûrement premier.
$n_4 - 1 = 2.7.19.23.137.1973$ est complètement factorisé donc on peut commencer notre test :

x	p	$x^{(n_4-1)/p} \bmod n_4$	$x^{n_4-1} \bmod n_4$
2	2	1	1
2	7	766408626	1
2	19	332952683	1
2	23	1154237810	1
2	137	373782186	1
2	1973	490790919	1
3	2	1	1
5	2	1	1
7	2	1653701518	1

Pour $p = 2$, on a essayé $x = 2, 3, 5$ avant de trouver $x = 7$ pour conclure. Donc n_4 est premier d'où n_2 est complètement factorisé. Et ainsi, en faisant un tableau similaire pour n_0 (car on a complètement factorisé $n_0 - 1$), on obtient que n_0 est premier. Mais bien sûr, on peut encore gagner du temps en utilisant la loi de réciprocité quadratique qui nous aurait indiqué, par le simple calcul de n_4 mod 10, que $5^{\frac{n_4-1}{2}} \bmod n_4 = 1$.

CHAPITRE 7

Réciprocité et nombres premiers réguliers

“ Although it is not well known, Kummer at one time believed he had found a complete proof of Fermat's theorem ... Seeking the best critic for his proof, Kummer sent his manuscript to Dirichlet ... After a few days, Dirichlet replied with the opinion that the proof was excellent and certainly correct, provided the numbers in α could not only be decomposed into indecomposable factors, as Kummer proved, but that this could be done in only one way. If however, the second hypothesis couldn't be satisfied, most of the theorem for the arithmetic of numbers in α would be unproven and the proof of Kummer's theorem would fall apart. Unfortunately, it appeared to him that the numbers in α didn't actually possess this property in general. ” Kurt Hensel, Commemoration of the first centennial of Kummer's birth (1910) [Ribenboim 2].

Cet apologue est semblable à celui qui, en 1847, arriva à Lamé : lorsqu'il présenta sa démonstration du théorème de Fermat à l'Académie, il se vit aussitôt opposer une objection dirimante de Liouville qui fit remarquer une non unicité potentielle de la décomposition en facteurs irréductibles d'expressions polynomiales en racines énièmes de l'unité (confer *Compte rendu des séances de l'Académie des Sciences*, séance du 1^{er} mars 1847).

1. Nombres premiers réguliers

Un nombre premier impair p est dit **régulier** s'il ne divise pas le nombre de classes du corps cyclotomique $\mathbb{Q}(e^{2i\pi/p})$, que l'on note aussi $\mathbb{Q}(\zeta_p)$,voire $\mathbb{Q}(\sqrt[p]{1})$.

Kummer, après vingt années de travail pour calculer les nombres de classes d'idéaux dans les anneaux $\mathbb{Z}[\sqrt[p]{1}]$, a pu donner la liste des nombres premiers irréguliers (i.e. les nombres premiers impairs qui ne sont pas réguliers) p inférieurs à 163.

p :	37	59	67	101	103	131	149	157
“Multiples” de p :	B_{34}	B_{44}	B_{58}	B_{68}	B_{24}	B_{22}	B_{130}	B_{62} et B_{110}

Pour ce faire, il a utilisé le **critère de Kummer** :
un entier premier impair est régulier si et seulement si p ne divise dans $\mathbb{Z}_{(p)}$ aucun des nombres de Bernoulli $B_2, B_4, \ldots, B_{p-3}$ i.e. si et seulement si p ne divise aucun des numérateurs des nombres de Bernoulli $B_2, B_4, \ldots, B_{p-3}$. Ceci est équivalent à ce que p^2 ne divise aucune des sommes $1^k+2^k+\cdots+(p-1)^k$ pour $k = 2, 4, \ldots, p-3$.

Rappel : $\mathbb{Z}_{(p)}$ est le localisé de $\mathbb{Z}$ en p, i.e. l'ensemble des rationnels dont le dénominateur est étranger avec p : on peut le voir comme l'anneau local des fractions de $\mathbb{Z}$ par rapport au complémentaire de l'idéal premier (p). Un anneau local est un anneau commutatif unitaire n'ayant qu'un seul idéal maximal.

Théorème de Jensen :
Il existe une infinité d'entiers premiers irréguliers congrus à 3 modulo 4.

Théorèmes de Metsänkylä :
– Il existe une infinité d'entiers premiers irréguliers congrus à 1 mod 3 ou à 1 mod 4. On ne sait toutefois même pas si l'une de ces deux classes est infinie.
– Les classes du complémentaire de tout sous-groupe propre de $\mathbb{Z}/n\mathbb{Z}$ contiennent une infinité d'entiers premiers irréguliers (modulo n, bien sûr).
Il est clair que le théorème de Jensen n'est qu'alors un corollaire immédiat de ce théorème pour $n = 4$.

Théorème de Kummer :
La conjecture de Fermat est vraie pour tout exposant p entier premier régulier. Cette conjecture marginale affirme, on le rappelle :

$$\forall p > 2\ \forall (x, y, z) \in \mathbb{Z}^3\ (x^p + y^p + z^p = 0 \Longrightarrow xyz = 0).$$

2. Post hoc, ergo propter hoc

On peut considérer la conjecture de Fermat comme un baromètre de l'évolution de la théorie des nombres et de l'algèbre. Il en est de même des lois de réciprocité. Il serait sans doute excessif d'affirmer que, sans ces deux problèmes, les mathématiciens n'auraient pas développé les notions de congruence, d'idéal, d'analyse complexe (via le théorème des nombres premiers [voir § 2.1] et via le théorème de la progression arithmétique [voir § 2.4]), de corps de classes (et donc les idèles de Chevalley puis les adèles de Weil), de courbes elliptiques ... En revanche, on affirmera sans vergogne le rôle moteur de ces deux problèmes. Il est toutefois amusant de remarquer que la victoire sur le théorème de Fermat ne s'est pas faite avec la théorie développée par Kummer : en fait la méthode de Wiles, qui permet de montrer $x^p + y^p + \gamma z^p = 0 \Longrightarrow xyz = 0$ pour $p \geq 11$ et γ puissance d'un nombre premier impair, est basée sur les courbes elliptiques, nouvelle drogue des mathématiciens, pour ceux qui voudraient s'y mithridatiser confer [Hellegouarch] et [Lang].

3. Loi de réciprocité pour un nombre premier régulier

Si p est un nombre premier régulier, on a :

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1} = \zeta^{l^{(1)}(a)l^{(p-1)}(b)+\cdots+l^{(p-1)}(a)l^{(1)}(b)}$$

où a et b sont dans $\mathbb{Q}[e^{2i\pi/p}]$ avec $a \equiv b \equiv 1 \bmod (\zeta - 1)$
et $l^{(k)}(x) = [\ln^{(k)}((f(\exp(t)))]_{t=0}$ où f est un polynôme de degré $p-1$ vérifiant $f(\zeta) = a$ et $f(1) = 1$.

CHAPITRE 8

Réciprocité dans un corps quadratique imaginaire

“ L'Esprit divin s'est manifesté d'une façon sublime dans cette merveille de l'analyse, ce prodige d'un monde idéal, cet intermédiaire entre l'être et le non-être, que nous appelons la racine imaginaire de l'unité négative. ” Gottfried Leibniz.

1. Une formule accorte

L'article *Loi de réciprocité dans les corps quadratiques imaginaires*, Annales de l'Institut Fourier, 1995, de A. Bayad, nous donne, dans un tel corps $\mathbb{K}$:

$$\left(\frac{\alpha}{\beta}\right)_2 \cdot \left(\frac{\beta}{\alpha}\right)_2 = \xi_\alpha^{\frac{N(\beta)-1}{2}} \xi_\beta^{\frac{N(\alpha)-1}{2}} (-1)^{\frac{N(\alpha)-1}{2}\frac{N(\beta)-1}{2}}.$$

Dans les précisions suivantes ν désigne à la fois α et β, des entiers algébriques. $N(\nu)$ désigne la norme de ν dans $\mathbb{K}/\mathbb{Q}$.

Rappel sur l'anneau $\mathbb{A}$ des entiers de $\mathbb{Q}(\sqrt{d})$:
si $d \equiv 1$ [4] alors

$$\mathbb{A} = \mathbb{Z}[\frac{1+\sqrt{d}}{2}] = \{\frac{u+v\sqrt{d}}{2} \mid u, v \in \mathbb{Z}, u \equiv v\ [2]\}$$

et le discriminant est donné par $D_{\mathbb{K}} = d$;
si $d \equiv 2, 3$ [4] alors

$$\mathbb{A} = \mathbb{Z}[\sqrt{d}] = \mathbb{Z} + \sqrt{d}\mathbb{Z}$$

et le discriminant est donné par $D_{\mathbb{K}} = 4d$.

2. Fonction de Weierstrass et courbes elliptiques

Nous aurons besoin de la fonction $\wp$ de Weierstrass qui est à la base de la théorie des courbes elliptiques dont les résultats suivants dérivent [Bayad], [Lang]. Soit R le réseau $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. $\wp$ est définie par

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in R^*} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right)$$

On peut sommer sur R car il y a convergence normale donc commutative.

On note

$$g_2 = 60 \sum_{\omega \in R^*} \frac{1}{\omega^4} \quad \text{et} \quad g_3 = 140 \sum_{\omega \in R^*} \frac{1}{\omega^6}.$$

On obtient ainsi la formule clef reliant la fonction de Weierstrass aux courbes elliptiques, permettant de considérer $\wp$ comme une "paramétrisation" de la courbe elliptique E :

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3.$$

Ainsi $(\wp, \wp')$ paramétrise $Y^2 = 4X^3 - g_2X - g_3$, de discriminant : $\Delta = g_2^3 - 27g_3^2 \neq 0$. On a ainsi un isomorphisme entre $\mathbb{C}/R$ et E donné par $z \mapsto (\wp(z), \wp'(z))$.

3. Définition du symbole quadratique

Le symbole quadratique $(\frac{\alpha}{\beta})_2$ est défini pour $\alpha, \beta \in \mathbb{Z}[i]$ et $\alpha, \beta, 2$ étrangers (ce qui est désormais supposé) par $\left(\frac{\alpha}{\beta}\right)_2 = \prod_{\sigma \in S_\beta} \varepsilon(\alpha, \sigma)$ où $\alpha\sigma = \varepsilon(\alpha, \sigma)\gamma(\sigma)$ avec $\varepsilon(\alpha, \sigma) \in \{-1, 1\}$, où $\gamma(\sigma) \in S_\beta$ et où $\{S_\beta, -S_\beta\}$ est un système complet de représentants ($\simeq$ une partition) de $R/\beta R$.

4. Réciprocité dans un corps quadratique

Quand le discriminant D est différent de $-4, -3$, *i.e.* quand on est dans $\mathbb{Q}(\sqrt{d})$ avec d différent de $-1, -3$, $\xi_\nu \in \{-1, 1\}$ est défini par

$$\xi_\nu = \nu \prod_{\gamma \in \operatorname{Ker} \nu - \{0\}} g(\gamma + \frac{\omega_1}{2})$$

où g est la fonction elliptique associée au réseau R définie par

$$g(z) = \frac{\wp(z) - \wp(\frac{\omega_1+\omega_2}{2})}{\wp'(z)} \sqrt{\frac{12\wp(\frac{\omega_2}{2})^2 - g_2}{\wp(\frac{\omega_2}{2}) - \wp(\frac{\omega_1+\omega_2}{2})}}.$$

Rappelons que $\operatorname{Ker} \nu$ désigne le noyau de la multiplication par ν, i.e. le noyau de l'endomorphisme de E qui à $z \mapsto \nu z$.

5. Loi de réciprocité quadratique dans $\mathbb{Q}(i)$

Quand $d = -1$, on a $\xi_\nu = 1$ si $\nu \equiv 1 \bmod (\sqrt{2\mathbb{Z}[i]})^3$;
$\xi_\nu = -1$ si $\nu \equiv -1 \bmod (\sqrt{2\mathbb{Z}[i]})^3$;
$\xi_\nu = i$ si $\nu \equiv i \bmod (\sqrt{2\mathbb{Z}[i]})^3$;
$\xi_\nu = -i$ si $\nu \equiv -i \bmod (\sqrt{2\mathbb{Z}[i]})^3$.

6. Loi de réciprocité quadratique dans $\mathbb{Q}(j)$

Quand $d = -3$, i.e. quand on est dans $\mathbb{Q}(j)$ (car $\mathbb{Q}(j) = \mathbb{Q}(\frac{1+\sqrt{-3}}{2}) = \frac{1}{2}\mathbb{Q} + \frac{1}{2}\mathbb{Q}(\sqrt{-3}) = \mathbb{Q} + \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\sqrt{-3})$), on a

$$\xi_\nu = \nu \prod_{\gamma \in \operatorname{Ker} \nu - \{0\}} g(\gamma + \frac{1}{2})$$

où g est la fonction elliptique pour le réseau $\mathbb{Z}[j]$ définie par

$$g(z) = 2\frac{\wp(z) - \wp(j^2/2)}{\wp'(z)} \sqrt{\wp(\frac{1}{2})(j-1)}.$$

Nota bene : $\xi_\nu \in \{-1, 1\}$.

Les courbes elliptiques commencent à inonder le monde mathématique de leurs bienfaits. Durant ces dernières années, ne citons que la victoire de Wiles sur le problème de Fermat (voir § 2.2 et § 7.1) ou le pavé dans la mare de Lenstra lorsqu'il sortit un nouvel algorithme de factorisation en 1985. On pourra consulter [Hellegouarch], [Knuth] et [Koblitz] pour une première approche.

CHAPITRE 9

Pour quelques réciprocités de plus

1. Résidu quadratique dans les corps p-adiques $\mathbb{Q}_p$

Les nombres p-adiques ont été introduits par Hensel, on peut se les représenter comme l'ensemble des nombres $up^k, k \in \mathbb{Z}$ et u inversible. Le symbole de Hilbert sur les nombres p-adiques est défini comme suit :

$$(\alpha,\beta)_{\mathbb{Q}_p} = \begin{cases} +1 \text{ si } \alpha \mathrm{x}^2 + \beta \mathrm{y}^2 - \mathrm{z}^2 = 0 \text{ a une solution dans } \mathbb{Q}_\mathrm{p} \text{ ;} \\ -1 \text{ sinon.} \end{cases}$$

On a le résultat suivant : α est un carré si $\forall\beta\ (\alpha,\beta)_{\mathbb{Q}_p} = 1$.

2. Loi de réciprocité quartique, de Burde, de Scholz

La première a été découverte par Gauss sur ses désormais célèbres entiers : pour $p = 4n + 1 = a^2 + b^2 = (a + ib)(a - ib) = p_1 p_2$, on a

$$\left(\frac{p_1}{q_1}\right)_4 \left(\frac{q_1}{p_1}\right)_4 = (-1)^{(p_1-1)(q_1-1)/16}$$

q ue l'on affine par les formules complémentaires : -1 est une puissance quatrième $\Longleftrightarrow p = 8n + 1$ et 2 est une puissance quatrième $\Longleftrightarrow p = a^2 + 64b^2$.

Emma Lehmer (en 1958) et Klaus Burde (en 1969) ont donné respectivement les formules suivantes, sous l'hypothèse $\left(\frac{p}{q}\right)_2 = 1$:

$$\left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 = \left(\frac{2}{q}\right)_2 \left(\frac{a+\sqrt{p}}{q}\right)_2 \quad \text{et} \quad \left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 = (-1)^{\frac{q-1}{4}} (\frac{aB - bA}{q})_2$$

où $p = a^2 + b^2$ et $q = A^2 + B^2$ avec $a \equiv A \equiv 1$ [4]. Ces deux formules sont en fait équivalentes.

Emma Lehmer et Ezra Brown en 1971 ont également donné, pour $p \equiv q \equiv 1$ [4] tels que $p = c^2 + qd^2$: $\left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 = (-1)^d$ si $q \equiv 5$ [8] et $\left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 = 1$ si $q \equiv 1$ [8]. Il faut savoir que tout nombre premier $p \equiv 1$ [4] et carré modulo q est du type $c^2 + qd^2$ pour q=5, 13 et 37.

Citons maintenant la loi de réciprocité de Scholz (1934), puisqu'il faut rendre à César ce qui appartient à César, et à la théorie des corps de classes ce qui appartient à la théorie des corps de classes :

$$\left(\frac{\varepsilon_q}{p}\right) = \left(\frac{\varepsilon_p}{q}\right).$$

En fait cette formule a été redécouverte, plus de trente ans après, sous la forme $\left(\frac{\varepsilon_q}{p}\right) = \left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4$, par induction sur les résultats suivants concernant les unités quadratiques (i.e. les éléments de norme ± 1) : $\left(\frac{\varepsilon_2}{p}\right) = \left(\frac{1+\sqrt{2}}{p}\right) = 1 \iff p = c^2 + 32d^2$; $\left(\frac{\varepsilon_5}{p}\right) = \left(\frac{(1+\sqrt{5})/2}{p}\right) = 1 \iff \left(\frac{\varepsilon_{13}}{p}\right) = \left(\frac{(3+\sqrt{13})/2}{p}\right) = 1 \iff p = c^2 + qd^2$ avec q impair ; $\varepsilon_{17} = 4 + \sqrt{17}$ est toujours un résidu quadratique modulo p.

3. Loi de réciprocité octale et plus si affinité

Je n'ai pas osé le néologisme "octique" mais je pense que tout un chacun aura deviné ce dont nous allons parler.

En 1976, K.S. Williams et P.Y. Wu ont fourni, indépendamment, le résultat suivant : soit $p = a^2 + b^2 = c^2 + 2d^2 \equiv 1$ [8] et $q = A^2 + B^2 = C^2 + 2D^2$ avec $a \equiv c \equiv A \equiv C \equiv 1$ [4] et $\left(\frac{p}{q}\right)_4 = \left(\frac{q}{p}\right)_4 = 1$, alors

$$\left(\frac{p}{q}\right)_8 \left(\frac{q}{p}\right)_8 = \left(\frac{aB - bA}{q}\right)_4 \left(\frac{cD - dC}{q}\right)_4.$$

De plus, $\left(\frac{2}{p}\right)_8 = 1 \iff p = a^2 + 256b^2 \equiv 1\ [16]$ ou bien $p = a^2 + 64b^2 \equiv 9\ [16]$ avec b impair.

Dans cette course aux lois de réciprocité, nous aurons besoin de la généralisation suivante du lemme de Gauss :

$$(-1)^{\mu_p(\lambda)} = \left(\frac{\lambda}{p}\right)_{2k}$$

où $\mu_p(\lambda)$ désigne le nombre d'éléments modulo p, qui une fois multipliés par λ sont négatifs (voir § 4.4).

On obtient alors directement :

$$\left(\frac{p}{q}\right)_{2k} \left(\frac{q}{p}\right)_{2k} = (-1)^{\mu_p(q)+\mu_q(p)} \text{ si } \left(\frac{p}{q}\right)_k = \left(\frac{q}{p}\right)_k = 1.$$

Bien qu'elles existent, nous ne donnerons pas ici de lois de réciprocité "rationnelles" pour les entiers impairs 3 et 5, cela nous embarquerait dans la représentation de nombres premiers par des formes quadratiques tarabiscotées [Faisant]. Nous nous contenterons de signaler que cela permet incidemment de prouver la primalité d'un nombre en montrant l'unicité d'une telle représentation.

4. Une démonstration exprès

Les plus courtes étant souvent les meilleures, voici une preuve “exprès” de la loi de réciprocité pour le symbole de Legendre, d'après G. Rousseau dans *On the quadratic reciprocity law*, Australian Mathematical Society, 3 (1991) : considérons le groupe quotient multiplicatif $G = \Big((Z/p\mathbb{Z})^* \times (Z/q\mathbb{Z})^*\Big)/U$, où $U = \{\pm(1,1)\}$. Le produit m de tous les éléments de G est

$$m = \prod_{i=1}^{p-1} \prod_{j=1}^{\frac{q-1}{2}} (i,j)U = \left((p-1)!^{\frac{q-1}{2}}, (q-1)!^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\right) U.$$

D'après le théorème chinois, m est aussi égal à

$$\prod_{\substack{1 \le k \le \frac{pq-1}{2} \\ pgcd(k,pq)=1}} (k,k)U,$$

donc, d'après le critère d'Euler,

$$m = \left((p-1)!^{\frac{q-1}{2}} \left(\frac{q}{p}\right), (q-1)!^{\frac{p-1}{2}} \left(\frac{p}{q}\right)\right) U.$$

La loi s'obtient en comparant les expressions pour m.

Des preuves encore plus élémentaire ont été données, cf. J.S. Frame [Amer. Math. Monthly 85 (1978), 10, 818–819], mais la preuve précédente est l'une des plus simples à retenir. La loi de réciprocité et la formule $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ (un cas spécial du critère d'Euler) sont facilement étendues par multiplicativité au symbole de Jacobi pour tous $p, q > 1$ *impairs*.

La loi complémentaire pour $\left(\frac{2}{p}\right)$ peut être simplement déduite du théorème : on écrit $p = 4k + e$ avec $e = \pm 1$, $k \geq 1$. Remarquons alors que $a = (p+e)/2$ est *impair* donc

$$\left(\frac{2e}{p}\right) = \left(\frac{2e+2p}{p}\right) = \left(\frac{4a}{p}\right) = \left(\frac{a}{p}\right) = \left(\frac{ep}{a}\right) = \left(\frac{2ea-1}{a}\right) = \left(\frac{-1}{a}\right).$$

Ainsi

$$\left(\frac{2}{p}\right) = \left(\frac{e}{p}\right)\left(\frac{-1}{a}\right) = (-1)^k = (-1)^{(p^2-1)/8}.$$

CHAPITRE 10

Nanobiographies

“ La philatélie ne serait que pure futilité si l’on n’y apprenait son histoire et sa géographie. ” Un philatéliste.

On devrait trouver ci-dessous les noms des intervenants plus ou moins illustres de ce T.E.R.

Abel, Niels Henrik (1802-1829) norvégien
Artin, Emil (1898-1962) autrichien, américain
Bachet de Méziriac, Claude Gaspard (1581-1638) français
Bernoulli, Jacques I^{er} (1654-1705) suisse
Bézout, Étienne (1739-1783) français
Bourbaki, Nicolas (1939) français
Cassels, John William Scott (1922) anglais
Catalan, Eugène Charles (1814-1894) français
César, Jules (100-44 av. J.-C.) romain
Chevalley, Claude (1909-1984) français
Dedekind, Richard Julius Wihelm (1831-1916) allemand
Dieudonné, Jean (1906-1992) français
Diophante d’Alexandrie (III^{e} siècle ap. J.-C.) grec
Dirichlet, Peter Gustav Lejeune- (1805-1859) allemand
Eisenstein, Ferdinand Gotthold (1823-1852) allemand
Ératosthène (284-192 av. J.-C.) grec
Erdös, Pal (1913-1996) hongrois
Euclide (III^{e} siècle av. J.-C.) grec
Euler, Leonhard (1707-1783) allemand
Fermat, Pierre Simon de (1601-1665) français
Fields, John Charles (1863-1932) canadien
Fourier, Jean Baptiste Joseph (1768=1830) français
Frame, James Sutherland (1907) américain
Galois, Évariste (1811-1832) français
Gauss, Karl Friedrich (1777-1855) allemand
Germain, Sophie (1776-1831) française
Goldbach, Hermann (1690-1764) allemand
Hadamard, Jacques (1865-1963) français
Hardy, Godfrey Harold (1877-1947) anglais
Hasse, Helmut (1898-1980) allemand

Hecke, Erich (1887-1947) polonais
Hensel, Kurt (1861-1941) allemand
Hilbert, David (1862-1943) allemand
Jacobi, Carl Gustav (1804-1851) allemand
Jensen, Johannes Ludwig Wilhelm (1859-1925) allemand
Knuth, Donald Erwin (1938) américain
Kraïtchik, Maurice Borisovitch (1882-1957) russe, belge
Kronecker, Leopold (1823-1891) allemand
Kummer, Ernst Eduard (1810-1893) allemand
Lagrange, Joseph Louis (1736-1813) français
La Vallée Poussin, Charles Jean Gustave (1866-1962) belge
Legendre, Adrien Marie (1752-1833) français
Lehmer, Derrick Henry (1905-1991) américain
Leibniz, Gottfried William (1646-1716) allemand
Linnik, Iurii Vladimirovich (1915-1972) russe
Liouville, Joseph (1809-1882) français
Lucas, François Edouard Anatole (1842-1891) français
Mersenne, Marin (1588-1648) français
Ostrowski, Alexander Markus (1893)
Pépin, Jean-François Théophile (1826-1904) français
Pisot, Charles (1910-1984) français
Riemann, Georg Friedrich Bernhard (1826-1866) allemand
Selberg, Atle (1917) norvégien
Serre, Jean-Pierre (1926) français
Shafarevich, Igor Rostilavovich (1923) russe
Sylow, Peter Ludwig Mejdell (1832-1918) norvègien
Takagi, Teiji (1875-1960) japonais
Taniyama, Yutaka (1027-1958) japonais
Tchebychev, Pafnuti Livovic (1821-1894) russe
Thomas D'Aquin, saint (1225-1274) italien
Vinogradov, Ivan Metveevitch (1891-1983) russe
Waring, Edward (1736-1798) anglais
Weber, Heinrich (1842-1913) allemand
Weierstrass, Karl Theodor Wilhelm (1815-1897) allemand
Weil, André (1906) français
Wiles, Andrew (1953) britannique
Wilson, John (1741, 1793) anglais
Wright, Edward Maitland (1906) anglais
Zassenhauss, Hans Julius (1912-1991) allemand, américain
Zimmermann, Philipp (1954) américain
Zolotarev, Egor Ivanovich (1847-1878) russe

Les mathématiciens cités dans ce mémoire et qui ne figurent pas dans cette liste (tels Adleman, Len ; Alford, W. Red ; Brown, Ezra ; Burde, Klaus ; Cantor, David Geoffrey ; Cooley, James William (1926) ; Cullen, J. ; Frey, Gerhard ; Granville, Andrew ; Lapin ; Larson ; Lehmer, Emma (1906) ; Lenstra, Hendrik Willem ; Lenstra, Arjen K. ; Matijasevich, Yuri ; Metsänkylä, Tauno ; Neukirch, Jürgen (1937) ; Nitaj, Abderrahmane ; Pomerance, Carl ; Ribet. Kenneth A. ; Rivest, Ron ; Rousseau, George ; Scholz, Arnold ; Schönhage, Arnold ; Shamir, Adi ; Shanks, Daniel Charles (1917) ; Slowinski, David ; Spiro, Claudia ; Strassen, Volker (1936), Taylor, R. ; Terjanian, Gérard ; Tuckey, John Wilder (1915) ; Wieferich, Arthur ; Williams, Kenneth S. ; Wu, Ping Yuan et Young, Paul Thomas) sont des contemporains, ou tout au plus, des mathématiciens du début du siècle.

CHAPITRE 11

Remerciements

Je tiens à remercier ou à saluer :
– mes lecteurs, si j'en ai encore à cette page. Mais j'ai pleinement conscience que de nombreux curieux commenceront par lire ces remerciements et je les incite donc à consulter également le restant de ce mémoire (je ne rentrerai pas le débat qui consiste à savoir si le directeur de TER est à incorporer dans la catégorie "lecteurs") ;
– ceux dont j'admire le travail, tel Knuth qui met puis offre au monde TEX ;
– ceux dont j'admire les idéaux, tel Zimmermann ;
– ceux dont j'admire les idées, tel Pomerance ;
- Gérard Duchamp, professeur, pour ses encouragements à me mettre au TEX et ses conseils ;
– Thierry Oger, ingénieur système, pour m'avoir facilité l'utilisation de LATEX au laboratoire d'informatique de Rouen ;
– les gens du laboratoire de mathématiques, qui m'ont permis de taper ce dossier ;
– les bibliothécaires de la B.U. des sciences de Rouen, qui n'ont pas hésité à s'enfoncer dans les méandres des vieux fonds pour mon bon plaisir ;
– Laurent Deséchalliers, pour m'avoir prêté les deux bouquins de Serre ;
– Claude Duvallet et Alexandre Pacini, pour m'avoir chacun imprimé ce mémoire ;
– les diverses imprimantes qui se sont évertuées à ne faire pas leur travail ;
– Sandra Matéos, pour avoir dénigré mon mauvais *accent* et pour avoir tenté de me faire introduire de l'*esprit*, hellénisation qui a été pitoyablement sacrifiée sur l'autel de la texnologie ;
– Vincent Tilman, qui fut le premier d'une longue série à être horrifié par la densité de ma première mise en page. J'ai finalement suivi ces (ses) conseils, faisant de multiples efforts de présentation (si, si) malgré que j'en eusse, et c'est ainsi que le lecteur a entre ses mains un mémoire bien plus lisible mais dont les imperfections subsistantes ne sauraient être imputées à mes conseillers ;
– tout quidam qui me signalerait, dans ce mémoire, une faute typographique (qui ne soit toutefois pas le fruit d'un choix ostensiblement iconoclaste de l'auteur), orthographique (fors les transcriptions du russe et du chinois qui, je le sais, laissent à désirer fortement), grammaticale (non, je ne rejette pas les remarques des puristes et me tient à leur entière disposition), historique, mathématique (mais n'oublions point que, pour vulgariser, il faut savoir transiger, même - surtout ? - en mathématique) ou morale (voir néanmoins la remarque précédente) ;
– mon directeur de TER, M. Legris, s'il a résisté aux bras de Morphée et s'il résiste à ceux d'Anastasie ...

CHAPITRE 12

Bibliographie

“ Timeo hominem unius libri. ” saint Thomas d'Aquin, patron des universités.

Ce mémoire est le fruit de divers emprunts aux ouvrages cités ci-dessous. On pourra le qualifier, au choix, de rhapsodie, de plagiat, de péculat, de florilège, de pot-pourri, de recueil, de compilation ou de mégamix. Chacun s'entendant sur les nuances ... En tous cas, ce rapport m'aura permis de mieux asseoir mes connaissances en TEX, en version anglaise et, incidemment, en algèbre. En tout cas, je vous invite à partager le plaisir que j'ai eu à parcourir les livres de cette liste, chacun étant un *κτῆμα εἰς ἀεί*[1], vous laissant ainsi faire de sérendipiteuses découvertes.

Bourbaki, N. : *Algèbre chapitres 4 et 5*, Hermann, 1959
Chabert, J.L. & coll. : *Histoire d'algorithmes*, Belin, 1994
Dahan-Dalmedico, A. & Peiffer, J. : *Une histoire des mathématiques*, Seuil, 1986
Dieudonné, J. & Houzel, C. : *article “ théorie des nombres ”*, Encyclopædia Universalis, 1995
Faisant, A. : *L'équation diophantienne du second degré*, Hermann, 1991
Francinou, S. & Gianella, H. : *Exercices de mathématiques pour l'agrégation*, Masson, 1995
Granville, A. : *Analytic number theory*, Birkhäuser, 1990
Guy, R.K. : *Unsolved problems in number theory*, Springer, 1994
Hardy G.H. & Wright E.M. : *An introduction to the theory of numbers*, Clarendon Press, 1959
Hecke, E. : *Lectures on the theory of algebraic numbers*, Springer, 1981
Hellegouarch, Y. : *Invitation aux mathématiques de Fermat-Wiles*, Masson, 1997
Itard J. : *Les nombres premiers*, Que sais-je n^o571, PUF, 1976
Knuth, D.E. : *Seminumerical algorithms*, Addison-Wesley, 1981
Koblitz, N. : *A course in number theory and cryptography*, Springer, 1987
Lang, S. : *Elliptic functions*, Addison-Wesley, 1973
Legendre, A.M. : *Théorie des nombres*, Blanchard, 1955
Naudin, P. & Quitté, C. : *Algorithmique algébrique*, Masson, 1992
Neukirch, J. : *Class field theory*, Springer, 1986
Ogg, A. : *Modular forms and Dirichlet series*, Benjamin, 1969
Ribenboim, P. : *The new book of prime number records*, Springer, 1996

[1] Le lecteur, étant fort probablement autant helléniste que l'auteur, est renvoyé, ainsi que pour toute citation sibylline, aux pages roses du Petit Larousse Illustré, qui clôt ainsi notre bibliographie.

Ribenboim, P. : *13 lectures on last Fermat theorem*, Springer, 1979
Serre, J.P. : *Cours d'arithmétique*, PUF, 1970
Serre, J.P. : *Corps locaux*, Hermann, 1962