CHAPITRE 1

La loi de réciprocité quadratique

L'objectif principal de ce premier chapitre est de rappeler la théorie des carrés de $\mathbb{Z}/N\mathbb{Z}$ développée par Fermat, Euler, Lagrange, Legendre et Gauss et notamment de démontrer la loi de réciprocité quadratique, le "theorema aureum" de Gauss, qui en est le résulat central. Nous introduirons au passage le symbole de Legendre, outil indispensable autant à l'élégance des énoncés qu'aux calculs pratiques de résidus quadratiques. Gauss a donné six démonstrations de la loi de réciprocité quadratique. Celle que nous présentons est la dernière, basée sur ce que l'on appelle depuis la somme de Gauss. Il sera commode d'introduire l'anneau des entiers algébriques, un outil dont on aurait pu se passer pour ce chapitre mais d'une grande importance pour la suite du cours. Enfin, nous terminerons par un théorème de Gauss sur la structure du groupe $(\mathbb{Z}/N\mathbb{Z})^\times$ des inversibles de l'anneau $\mathbb{Z}/N\mathbb{Z}$.

Les résultats de ce chapitre joueront un rôle essentiel dans la théorie des formes quadratiques binaires, par exemple pour les questions de représentation des entiers sous la forme $x^2 + dy^2$, ainsi que dans l'arithmétique des corps quadratiques.

Références : — C. F. Gauss, *Disquisitiones Arithmeticae*. Un grand classique traduit en français aux éditions Jacques Gabay. On y trouvera dans les chapitres I, II, III et IV les démonstrations (pour la plupart originales) de tous les résultats de ce chapitre, et bien plus encore.

— K. Ireland & M. Rosen, *A classical introduction to modern number theory*, Springer Verlag GTM **84**. Une excellente présentation, dans le language d'aujourd'hui, avec de multiples notes historiques. Notre présentation de la sixième preuve de Gauss est notamment issue du chapitre 6 de ce livre. De nombreuses autres démonstrations de la loi de réciprocité quadratique y sont exposées.

— Nous utiliserons librement le language de base de la théorie des groupes, pour lequel le lecteur pourra se reporter au livre *Algebra* de Serge Lang aux éditions Addison Wesley.

1. Carrés modulo un entier

Définition 1.1. *Soient N un entier ≥ 1 et $a \in \mathbb{Z}$. On dit que a est un carré modulo N, ou encore un résidu quadratique modulo N, s'il existe $b \in \mathbb{Z}$ vérifiant $a \equiv b^2 \bmod N$.*

Cette propriété ne dépend bien sûr que de la classe de a dans $\mathbb{Z}/N\mathbb{Z}$, et il revient au même de demander que cette classe est le carré d'un élément de l'anneau $\mathbb{Z}/N\mathbb{Z}$, c'est-à-dire de la forme x^2 avec $x \in \mathbb{Z}/N\mathbb{Z}$. Par exemple, les carrés modulo 5 sont

(les classes de ...) $0, 1$ et -1, et les non-carrés sont 2 et -2. De même, les carrés modulo 8 sont $0, 1$ et 4.

Il est évident que si a est un carré modulo N, et si M divise N, alors a est un carré modulo M. Nous allons donc commencer par étudier le cas (qui s'avèrera essentiel) où N est un nombre premier. Le cas du nombre premier 2 étant trivial, nous supposerons souvent que p est un nombre premier impair.

Proposition 1.2. *Soient p un nombre premier impair et $\mathrm{C}_p := \{x^2, x \in (\mathbb{Z}/p\mathbb{Z})^\times\}$ l'ensemble des carrés non nuls de $\mathbb{Z}/p\mathbb{Z}$.*

(i) C_p a exactement $\frac{p-1}{2}$ éléments, à savoir les classes modulo p des éléments de la forme i^2 pour $i = 1, 2, \ldots, \frac{p-1}{2}$.

(ii) C_p est un sous-groupe d'indice 2 du groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^\times$: le produit de deux éléments de $(\mathbb{Z}/p\mathbb{Z})^\times$ est un carré si et seulement s'ils sont soit tous deux des carrés, soit tous deux des non-carrés.

Démonstration — Soient $x, y \in \mathbb{Z}/p\mathbb{Z}$. On a la suite d'équivalences $x^2 = y^2 \Leftrightarrow (x-y)(x+y) = 0 \Leftrightarrow x = \pm y$, la dernière provenant de ce que l'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps pour p premier. Pour la même raison, on a $x \neq -x$ pour tout $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ car $p > 2$. La première assertion en découle.

Il est évident que C_p est un sous-groupe de $(\mathbb{Z}/p\mathbb{Z})^*$. On a $|(\mathbb{Z}/p\mathbb{Z})^\times|/|\mathrm{C}_p| = 2$ d'après le (i) [1], autrement dit C_p est d'indice 2. D'après Lagrange, C_p a donc exactement deux translatés (ou "classes") dans $(\mathbb{Z}/p\mathbb{Z})^\times$: on a

$$(\mathbb{Z}/p\mathbb{Z})^\times = \mathrm{C}_p \coprod a\mathrm{C}_p$$

où a est n'importe quel élément qui n'est pas dans C_p, c'est-à-dire un non-carré. Ainsi, si x et y ne sont pas des carrés, et donc tous deux dans $a\mathrm{C}_p$, alors xy est dans $a^2\mathrm{C}_p$: c'est donc un carré. De même, si $x \in \mathrm{C}_p$ et $y \notin \mathrm{C}_p$, alors $xy \in a\mathrm{C}_p$: le produit d'un non-carré par un carré est un non-carré. □

Définition 1.3. (Legendre) *Soient p un nombre premier impair et $a \in \mathbb{Z}$. Si a est premier à p, on pose $\left(\frac{a}{p}\right) = 1$ si a est un carré modulo p, $\left(\frac{a}{p}\right) = -1$ sinon. On pose enfin $\left(\frac{a}{p}\right) = 0$ si $a \equiv 0 \bmod p$.*

Ainsi défini, le nombre $\left(\frac{a}{p}\right)$ ne dépend que de la classe de a modulo p de sorte qu'il y a aussi un sens à écrire $\left(\frac{a}{p}\right)$ pour $a \in \mathbb{Z}/p\mathbb{Z}$. La seconde assertion de la proposition 1.2 se reformule alors de la manière suivante :

Corollaire 1.4. (Multiplicativité du symbole de Legendre) *Pour tous a, b dans $\mathbb{Z}$, on a $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.*

1. Nous aurions pu également introduire l'application $f : (\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ définie par $f(x) = x^2$. C'est un morphisme de groupes d'image C_p et de noyau $\{\pm 1\}$ d'après l'argument donné au (i). La formule $|\mathrm{Im}(f)| = |(\mathbb{Z}/p\mathbb{Z})^\times|/|\mathrm{Ker}(f)|$ redonne bien sûr l'égalité $|\mathrm{C}_p| = \frac{p-1}{2}$.

En particulier, il suffit de savoir déterminer les nombres $\left(\frac{a}{p}\right)$ avec $a = -1$, 2 ou a premier impair. Étant donné p, il est en théorie facile de déterminer tous les $a \in \mathbb{Z}$ tels que $\left(\frac{a}{p}\right) = 1$: il suffit d'énumérer les classes modulo p de i^2 pour $i = 1, \ldots, \frac{p-1}{2}$ (Proposition 1.2), qui est en particulier un problème fini. En revanche, un problème nettement plus difficile est de déterminer, étant donné $a \in \mathbb{Z}$, tous les nombres premiers p tels que $\left(\frac{a}{p}\right) = 1$. La table suivante donne quelques exemples.

p	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73	79
$\left(\frac{2}{p}\right)$	-1	-1	1	-1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	-1	-1	-1	1	1	1
$\left(\frac{3}{p}\right)$	0	-1	-1	1	1	-1	-1	1	-1	-1	1	-1	-1	1	-1	1	1	-1	1	1	-1
$\left(\frac{5}{p}\right)$	-1	0	-1	1	-1	-1	1	-1	1	1	-1	1	-1	-1	-1	1	1	-1	1	-1	1

TABLE 1. $\left(\frac{a}{p}\right)$ pour $p < 80$ et $a = 2, 3, 5$

Cette table peut soit être obtenue par énumération directe, bien que fastidieuse, des carrés modulo tous ces premiers, soit par exemple à l'aide du critère élégant suivant (mais pas très efficace non plus en pratique, il faut bien l'avouer, du moins sans l'aide de l'ordinateur).

Proposition 1.5. (Critère d'Euler) *Soient p premier impair et $a \in \mathbb{Z}$, on a la congruence $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \bmod p$.*

DÉMONSTRATION — On peut supposer $a \not\equiv 0 \bmod p$. Nous allons montrer $(p-1)! \equiv -\left(\frac{a}{p}\right) a^{\frac{p-1}{2}} \bmod p$. Du cas $a = 1$ on en déduira $(p-1)! \equiv -1 \bmod p$ (théorème de Wilson) puis le résultat de l'énoncé.

On remarque que l'application $x \mapsto ax^{-1}$ est une involution [2] de $(\mathbb{Z}/p\mathbb{Z})^\times$ qui est sans point fixe, sauf si a est un carré modulo p auquel cas ses deux seuls points fixes sont u et $-u$ où $u^2 = a \bmod p$. Le produit des éléments de $(\mathbb{Z}/p\mathbb{Z})^\times$, qui est congru à $(p-1)!$, vaut donc $a^{\frac{p-1}{2}} \bmod p$ si $\left(\frac{a}{p}\right) = -1$, et $a^{\frac{p-3}{2}} \cdot (-a)$ si $\left(\frac{a}{p}\right) = 1$, ce qui conclut.

Donnons une seconde démonstration. Le petit théorème de Fermat montre que les $\frac{p-1}{2}$ éléments de l'ensemble C_p des carrés de $(\mathbb{Z}/p\mathbb{Z})^\times$ sont des racines du polynôme $P = X^{\frac{p-1}{2}} - 1$ dans $(\mathbb{Z}/p\mathbb{Z})[X]$. Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, C_p est exactement l'ensemble des racines de P. Ainsi, si x n'est pas dans C_p, et si $y = x^{\frac{p-1}{2}}$, alors $y \neq 1$ par ce que l'on vient de dire, et $y^2 = 1$ par le petit théorème de Fermat, donc $y = -1$. □

2. Une involution d'un ensemble X est une application $f : X \to X$ vérifiant que $f \circ f = \mathrm{id}_X$. Il est équivalent de se donner une action du groupe $\mathbb{Z}/2\mathbb{Z}$ sur l'ensemble X, l'élément non trivial de $\mathbb{Z}/2\mathbb{Z}$ agissant par la bijection f. En particulier, X est réunion disjointe d'orbites de cette action, qui sont soit de cardinal 1 (points fixes), soit de cardinal 2 (et de la forme $\{x, f(x)\}$ avec $f(x) \neq x$).

Par exemple, modulo 23 on a $\left(\frac{5}{23}\right) \equiv 5^{11} \equiv 5.2^5 \equiv 5.9 \equiv -1$. Remarquons que ce critère donne une autre démonstration de la multiplicativité du symbole de Legendre. Surtout, il admet le corollaire immédiat suivant.

Corollaire 1.6. (Fermat, Euler) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. *Autrement dit,* -1 *est un carré modulo le premier impair* p *si, et seulement si, on a* $p \equiv 1 \bmod 4$.

Un examen de la table 1 ci-dessus suggère des propriétés remarquables tout à fait non triviales. On observe notamment dans tous les cas les

$$\left(\frac{2}{p}\right) = 1 \text{ si, et seulement si, } p \equiv \pm 1 \bmod 8,$$

$$\left(\frac{3}{p}\right) = 1 \text{ si, et seulement si, } p \equiv \pm 1 \bmod 12,$$

$$\left(\frac{5}{p}\right) = 1 \text{ si, et seulement si, } p \equiv \pm 1 \bmod 5.$$

Il s'agit en fait de propriétés générales, toutes cas particulier du résultat fondamental suivant, conjecturé indépendamment par Euler, Gauss et Legendre (qui l'a démontré dans certains cas), et démontré en toute généralité par Gauss dans ses *Disquisitiones Arithmeticae*. En vertu de la multiplicativité du symbole de Legendre, cela fournit une recette pour determiner $\left(\frac{a}{p}\right)$ dans tous les cas.

Théorème 1.7. *(Loi de réciprocité quadratique) Soient* p *et* q *des nombres premiers impairs. On a*

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

De plus, on a la "loi supplémentaire" $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Remarque 1.8. (sur l'énoncé ci-dessus) Autrement dit, si $p \equiv 1 \bmod 4$ ou $q \equiv 1 \bmod 4$ on a $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$, et dans les autres cas on a $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$. Si l'on pose $p^\star := (-1)^{\frac{p-1}{2}}p$, le corollaire 1.6 permet également d'écrire la loi de réciprocité quadratique sous la forme condensée $\left(\frac{q}{p}\right) = \left(\frac{p^\star}{q}\right)$. La supplémentaire s'écrit aussi : 2 est un carré modulo p si, et seulement si, $p \equiv \pm 1 \bmod 8$.

La démonstration de ce résultat nous occupera dans les paragraphes qui vont suivre. Donnons-en tout d'abord quelques applications. Par exemple, sachant que 691 est premier, est-ce que 41 est un carré modulo 691 ? L'approche naïve est de lister les carrés modulo 691, ce qui est bien fastidieux ; le critère d'Euler (consistant à calculer $41^{345} \bmod 691$) ne poserait pas de problème à un ordinateur, mais est assez peu commode à la main. En utilisant la loi de réciprocité quadratique, il est essentiellement immédiat de justifier la suite d'égalités ci-dessous :

$$\left(\frac{41}{691}\right) = \left(\frac{691}{41}\right) = \left(\frac{35}{41}\right) = \left(\frac{7}{41}\right)\left(\frac{5}{41}\right) =$$

$$\left(\frac{41}{5}\right)\left(\frac{41}{7}\right) = \left(\frac{1}{5}\right)\left(\frac{6}{7}\right) = 1.(-1) = -1$$

donc 41 n'est pas un carré modulo 691 ! Le seul calcul réellement effectué ici est $691 \equiv 35 \bmod 41$...

Une autre conséquence immédiate de la loi de réciprocité quadratique, loin d'être évidente, est que q étant donné le nombre $\left(\frac{q}{p}\right)$ ne dépend que de $p \bmod 4q$. Donnons quelques exemples, expliquant notamment la table 1 :

Corollaire 1.9. *Soit p un nombre premier impair.*

(i) 3 *est un carré modulo p si, et seulement si, $p \equiv \pm 1 \bmod 12$ ou $p = 3$.*

(ii) 5 *est un carré modulo p si, et seulement si, $p \equiv \pm 1 \bmod 5$ ou $p = 5$.*

(iii) 7 *est un carré modulo p si, et seulement si, $p \equiv \pm 1, \pm 3, \pm 9 \bmod 28$ ou $p = 7$.*

Démonstration — On a $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$ car $5 \equiv 1 \bmod 4$. Les carrés modulo 5 étant 0 et ± 1, cela démontre le (ii). De même, on a $\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right)$, duquel on déduit le (i). Le (iii) est laissé en exercice au lecteur. □

Terminons par une discussion des carrés de $\mathbb{Z}/N\mathbb{Z}$ où N n'est plus nécessairement un nombre premier. Remarquons tout d'abord que le lemme chinois des restes, rappelé ci-dessous, montre que $a \in \mathbb{Z}$ est un carré modulo l'entier $N = \prod_i p_i^{n_i}$ où les p_i sont premiers distincts si, et seulement si, a est un carré modulo $p_i^{n_i}$ pour tout i.

Lemme 1.10. (Lemme chinois des restes) *Soient N et M des entiers premiers entre eux. L'application*

$$\mathbb{Z}/MN\mathbb{Z} \to \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$$

définie par $a \bmod MN \mapsto (a \bmod M, a \bmod N)$, est un isomorphisme d'anneaux.

Démonstration — C'est évidemment un morphisme d'anneaux. La source et le but ayant même cardinal MN il suffit de voir qu'il est injectif, ce qui est immédiat sous l'hypothèse $(M, N) = 1$. □

Il ne reste donc qu'à traiter le cas $N = p^n$ avec p premier et $n > 1$. Soit $a \in \mathbb{Z}$, écrivons $a = p^m a'$ avec $(a', p) = 1$. On peut également supposer $m < n$ sans quoi $a \equiv 0 \bmod p^n$ est évidemment un carré. Dans ce cas, il est facile de vérifier que a est un carré modulo p^n si, et seulement si, m est pair et a' est un carré modulo p^{n-m}. En conclusion, il suffit de déterminer les carrés de $(\mathbb{Z}/p^n\mathbb{Z})^\times$.

Lemme 1.11. *Soit $a \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ avec p premier et $n > 1$.*

(i) Si p est impair, alors a est un carré si et seulement si c'est un carré modulo p.

(ii) Si $p = 2$ et $n > 2$, alors a est un carré si, et seulement si, c'est un carré modulo 8.

On remarquera que si l'entier a est impair, alors a est un carré modulo 8 si, et seulement si, $a \equiv 1 \bmod 8$, ce qui permet de reformuler la condition du (ii) en la simple congruence "$a \equiv 1 \bmod 8$".

Démonstration — Montrons par récurrence sur n que si a est un carré modulo p^n, alors a est un carré modulo p^{n+1} ("raisonnement par approximations successives"). Écrivons $a = u^2 + p^n r$ avec $u, r \in \mathbb{Z}$. Si $v \in \mathbb{Z}$ est un entier quelconque, on observe les congruences

$$(u + p^n v)^2 \equiv u^2 + 2urp^n \equiv a + (2uv - r)p^n \bmod p^{n+1}.$$

Il suffit donc de voir que l'on peut choisir v de sorte que l'on ait $2uv \equiv r \bmod p$. Mais a est premier à p, ainsi donc que u, et aussi $2u$ si l'on suppose de plus $p > 2$. Dans ce cas, tout entier v tel que $v \equiv r(2u)^{-1} \bmod p$ convient. Si $p = 2$ il faut modifier un peu l'argument précédent à cause du facteur 2 qui devient gênant. Supposons donc $a = u^2 + 2^n r$, $u, r \in \mathbb{Z}$. Si $v \in \mathbb{Z}$ on a l'identité

$$(u + 2^{n-1}v)^2 \equiv a + (uv - r)2^n \bmod 2^{n+1}.$$

(Noter $2(n-1) \geq n+1$ car $n \geq 3$). Mais $uv \equiv r \bmod 2$ si $v \equiv r \bmod 2$, car u est impair, ce qui conclut. □

Si l'on met bout-à-bout les observations précédentes, nous avons démontré la proposition suivante.

Proposition 1.12. *Soit $\mathcal{Q} \subset \mathbb{N}$ la réunion de l'ensemble des premiers impairs et de $\{4, 8\}$. Un élément $a \in (\mathbb{Z}/N\mathbb{Z})^\times$ est un carré si, et seulement si, son image dans $(\mathbb{Z}/q\mathbb{Z})^\times$ est un carré pour tout $q \in \mathcal{Q}$ divisant N.*

2. Digression : l'anneau des entiers algébriques

Définition 1.13. *(Dedekind) Un entier algébrique est un nombre complexe annulé par un polynôme* unitaire *à coefficients entiers. On note $\overline{\mathbb{Z}} \subset \mathbb{C}$ l'ensemble des entiers algébriques.*

En particulier, un entier algébrique est un nombre algébrique. Par exemple, les complexes $\sqrt{N}$ et $e^{2i\pi/N}$ pour $N \in \mathbb{Z}$, les entiers usuels, ou encore tout $x \in \mathbb{C}$ tel que $x^3 = x + 1$, sont des entiers algébriques. On peut dire que les entiers algébriques sont aux nombres algébriques ce que les entiers sont aux nombres rationnels. La proposition suivante, classique à sa formulation près, en est un premier indicateur.

Proposition 1.14. *Les entiers algébriques qui sont rationnels sont dans $\mathbb{Z}$. Autrement dit, on a $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$.*

Démonstration — C'est le fait bien connu que si le rationnel p/q, avec $(p, q) = 1$, est racine d'un polynôme $P \in \mathbb{Z}[X]$, alors q divise le coefficient dominant de P, comme on le voit en regardant l'égalité $q^n P(p/q) = 0$ avec $n = \deg(P)$. Si P est unitaire, on a donc $q = \pm 1$, puis $p/q \in \mathbb{Z}$. □

Proposition 1.15. *$\overline{\mathbb{Z}}$ est un sous-anneau de $\mathbb{C}$.*

Observons cependant que $\overline{\mathbb{Z}}$ n'est pas un sous-corps de $\mathbb{C}$. En effet, on a $1/N \notin \overline{\mathbb{Z}}$ pour $N \geq 2$ d'après la proposition précédente. Pour démontrer la proposition 1.15, nous aurons besoin du critère d'intégralité suivant. Si $x_1, \ldots, x_r$ sont des nombres complexes, on note $\mathbb{Z}[x_1, \ldots, x_r] \subset \mathbb{C}$ le sous-ensemble des nombres de la forme $P(x_1, \ldots, x_r)$ avec $P \in \mathbb{Z}[X_1, \ldots, X_r]$. C'est le plus petit sous-anneau de $\mathbb{C}$ contenant les x_i.

Proposition 1.16. *(i) Si $x_1, \ldots, x_r \in \overline{\mathbb{Z}}$ alors le groupe additif de $\mathbb{Z}[x_1, \ldots, x_r]$ engendré par un nombre fini d'éléments.*

(ii) Soit $x \in \mathbb{C}$. Alors x est un entier algébrique si, et seulement si, il existe un sous-groupe (additif) non nul $A \subset \mathbb{C}$ engendré par un nombre fini d'éléments et tel que $xA \subset A$.

Démonstration — Montrons le (i). Fixons $1 \leq i \leq r$ et $P_i \in \mathbb{Z}[X]$ unitaire avec $P_i(x_i) = 0$. Posons $n_i = \deg P_i$. On constate que $x_i^{n_i}$ est une combinaison linéaire à coefficients dans $\mathbb{Z}$ des éléments x_i^k avec $k < n_i$. Par récurrence sur $m \geq n_i$, il en va donc de même des x_i^m avec $m \geq n_i$. On en déduit que le group $\mathbb{Z}[x_1, \ldots, x_r]$ est engendré par les éléments $\prod_{i=1}^r x_i^{k_i}$ avec $0 \leq k_i < n_i$, qui sont en nombre fini.

Montrons le (ii). Supposons d'abord x entier algébrique. Alors $A := \mathbb{Z}[x]$ convient d'après le (i). Réciproquement, soient $A \subset \mathbb{C}$ comme dans l'énoncé et $e_1, \ldots, e_n$ une famille génératrice de A. Ainsi, tout $a \in A$ s'écrit sous la forme $\sum_{i=1}^n m_i e_i$ (pas nécéssairement de manière unique) avec $m_i \in \mathbb{Z}$ pour tout i. Par hypothèse, on a $xe_j \in A$ pour tout j, et donc il existe des entiers $m_{i,j}$ tels que pour tout i,

$$xe_j = \sum_{i=1}^n m_{i,j} e_i.$$

Cela s'écrit encore $0 = \sum_{i=1}^n (x\delta_{i,j} - m_{i,j})e_i$ pour tout $j = 1, \ldots, n$: on reconnaît là un système linéaire en les e_i. Par hypothèse les e_j ne sont pas tous nuls, car $A \neq 0$, il s'ensuit que la matrice $(x\delta_{i,j} - m_{i,j})$ est non inversible. La nullité de son déterminant fournit l'équation $P(x) = 0$ où P est le polynôme caractéristique de $(m_{i,j})$: c'est un polynôme unitaire de $\mathbb{Z}[X]$. □

Démonstration — (de la proposition 1.15) Soient x, y des entiers algébriques. D'après la proposition 1.16 (i), le groupe abélien $A = \mathbb{Z}[x, y]$ est finiment engendré. On a clairement $1 \in A$ (donc $A \neq 0$), $xyA \subset A$ et $(x - y)A \subset A$: les éléments xy et $x - y$ sont donc dans $\overline{\mathbb{Z}}$ d'après le (ii) de la proposition 1.16. □

Observons que ces résultats permettent de vérifier que certains nombres algébriques ne sont pas des entiers algébriques. Par exemple $x = \frac{1+\sqrt{3}}{2}$ est un nombre algébrique, satisfaisant $x^2 - x - 1/2 = 0$. Si x était entier algébrique, il en serait de même de $x^2 - x = 1/2$, ce qui n'est pas. Mentionnons tout de même qu'il ne faut pas toujours se fier aux apparences : le nombre $\frac{1+\sqrt{5}}{2}$ est un entier algébrique ! (pourquoi ?)

3. Congruences dans $\overline{\mathbb{Z}}$

L'arithmétique de l'anneau $\overline{\mathbb{Z}}$, c'est-à-dire les questions de divisibilité, est immensément plus complexe que celle de $\mathbb{Z}$, et c'est un des buts de ce cours que d'en éclaircir les traits fondamentaux. Nous nous contenterons ici de dégager quelques faits élémentaires qui seront utiles à la démonstration de la loi réciprocité quadratique, et reportons une discussion plus raisonnable aux chapitres qui suivent.

Tout comme dans les entiers usuels, il y a un sens à considérer des congruences dans l'anneau $\overline{\mathbb{Z}}$. En effet, pour tout $N \in \overline{\mathbb{Z}}$, l'ensemble $N\overline{\mathbb{Z}} = \{Na, a \in \overline{\mathbb{Z}}\}$ est un idéal de $\overline{\mathbb{Z}}$ et il y a donc un sens à considérer l'anneau quotient

$$\overline{\mathbb{Z}}/N\overline{\mathbb{Z}}.$$

Concrètement, deux entiers algébriques $a, b \in \overline{\mathbb{Z}}$ seront dits congrus modulo N, et on écrira $a \equiv b \bmod N\overline{\mathbb{Z}}$, s'il existe $c \in \overline{\mathbb{Z}}$ tel que $a = b + Nc$, ou ce qui revient au même s'ils ont même image dans $\overline{\mathbb{Z}}/N\overline{\mathbb{Z}}$. Les propriétés générales des anneaux quotients se traduisent simplement par le fait que l'on peut additionner, soustraire et multiplier des congruences. Un cas particulier important est celui où $N \in \mathbb{Z}$.

Lemme 1.17. *Soient a, b et N dans $\mathbb{Z}$. Alors $a \equiv b \bmod N\overline{\mathbb{Z}} \Leftrightarrow a \equiv b \bmod N$.*

Démonstration — Il s'agit de voir que si $a = b + Nc$ avec $c \in \overline{\mathbb{Z}}$, alors $c \in \mathbb{Z}$ ou $N = 0$. On exclut ce dernier cas qui est trivial. Mais alors $c = \frac{a-b}{N} \in \mathbb{Q} \cap \overline{\mathbb{Z}}$, et on conclut d'après la proposition 1.14. □

Pour $a, b, N \in \overline{\mathbb{Z}}$ nous noterons par la suite simplement $a \equiv b \bmod N$ pour $a \equiv b \bmod N\overline{\mathbb{Z}}$. Le lemme ci-dessus assure que cette notation n'est pas en conflit avec la notation usuelle quand les deux ont un sens, c'est-à-dire quand $a, b, N \in \mathbb{Z}$.

La structure de l'anneau $\overline{\mathbb{Z}}/N\overline{\mathbb{Z}}$ est en général sensiblement plus compliquée que celle de $\mathbb{Z}/N\mathbb{Z}$ (qu'il contient par le lemme ci-dessus), et ce même quand N est un nombre premier. Par exemple, $\overline{\mathbb{Z}}/N\overline{\mathbb{Z}}$ n'est jamais un corps si $N > 1$! En effet, l'élément $\sqrt{N}$ est dans $\overline{\mathbb{Z}}$, n'est pas $\equiv 0 \bmod N$ (pourquoi ?) et son carré est $\equiv 0 \bmod N$. Une propriété générale fort utile que nous utiliserons est la suivante.

Lemme 1.18. *Soit p un nombre premier. Si $a, b \in \overline{\mathbb{Z}}$ on a*

$$(a + b)^p \equiv a^p + b^p \bmod p.$$

Démonstration — Cela découle de la formule du binôme et de ce que p divise $\binom{p}{k}$ pour $k = 1, \ldots, p - 1$. □

4. Sommes de Gauss

Soient p un nombre premier impair et $\zeta = e^{2i\pi/p}$.

Définition 1.19. (Gauss) *La* somme de Gauss *relative à p est le nombre complexe*

$$G = \sum_{a \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{a}{p}\right) \zeta^a.$$

Par exemple, si $p = 3$ alors $G = \zeta - \zeta^2 = i\sqrt{3}$. De même, si $p = 5$ alors $G = \zeta - \zeta^2 - \zeta^3 + \zeta^4 = 2\cos(2\pi/5) - 2\cos(4\pi/5) = \frac{-1+\sqrt{5}}{2} - \frac{-1-\sqrt{5}}{2} = \sqrt{5}$. La proposition suivante montre que c'est un phénomène général.

Proposition 1.20. (Gauss) $G^2 = (-1)^{\frac{p-1}{2}} p$.

Démonstration — Par multiplicativité du symbole de Legendre, on a

$$G^2 = \sum_{a,b \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{ab}{p}\right) \zeta^{a+b}.$$

Rappelons-nous $\left(\frac{a^2 t}{p}\right) = \left(\frac{t}{p}\right)$ si $a \in (\mathbb{Z}/p\mathbb{Z})^\times$. Posant $b = at$ on obtient donc

$$G^2 = \sum_{t \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{t}{p}\right) \left(\sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \zeta^{a(1+t)} \right).$$

Si $t = -1$, alors $\sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \zeta^{a(1+t)} = p - 1$. Sinon, $a \mapsto (1+t)a$ est une bijection de $(\mathbb{Z}/p\mathbb{Z})^\times$, et donc on a

$$\sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \zeta^{a(1+t)} = \zeta + \zeta^2 + \cdots + \zeta^{p-1} = -1.$$

Ainsi, $G^2 = \left(\frac{-1}{p}\right)(p-1) - \sum_{t \in (\mathbb{Z}/p\mathbb{Z})^\times \setminus \{-1\}} \left(\frac{t}{p}\right)$. On conclut d'après le lemme 1.21. □

Lemme 1.21. $\sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{a}{p}\right) = 0$.

Démonstration — En effet, il y a autant de carrés que de non carrés dans $(\mathbb{Z}/p\mathbb{Z})^\times$ par la proposition 1.2. □

Définition 1.22. *La somme de Gauss relativement au nombre premier 2 est $G = \zeta + \zeta^{-1}$ où $\zeta = e^{2i\pi/8}$.*

Comme $\zeta = \frac{1+i}{\sqrt{2}}$, on a simplement $G = \sqrt{2}$, ce qui constitue un analogue de la proposition 1.20.

Remarque 1.23. (signe de la somme de Gauss) Gauss a en fait démontré $G = \sqrt{p}$ si $p \equiv 1 \bmod 4$, et $G = i\sqrt{p}$ si $p \equiv 3 \bmod 4$. La preuve est nettement plus délicate : voir par exemple l'exercice 1.14 pour une élégante démonstration due à Dirichlet.

5. Une démonstration de la loi de réciprocité quadratique

Fixons p un nombre premier et q un nombre premier impair différent de p. Soit G la somme de Gauss relative à p. On a

$$G \in \mathbb{Z}[e^{\frac{2i\pi}{p}}] \subset \overline{\mathbb{Z}}.$$

La stratégie de Gauss est grosso-modo la suivante. Observons que G est une racine carré dans $\overline{\mathbb{Z}}$ de $(-1)^{\frac{p-1}{2}}p$ d'après la proposition 1.20. Sa réduction mod $q\overline{\mathbb{Z}}$ est donc naturellement un candidat pour être une racine carré de $(-1)^{\frac{p-1}{2}}p \bmod q$. La question qui se pose est donc de savoir à quelle condition G est congrue modulo $q\overline{\mathbb{Z}}$ à un élément de $\mathbb{Z}$. Une condition nécessaire[3] est que $G^q \equiv G \bmod q$ (petit théorème de Fermat), ce qui pousse à s'intéresser à $G^q \bmod q\overline{\mathbb{Z}}$.

Proposition 1.24. *Soient G la somme de Gauss relative au premier p et $q \neq p$ premier. On a $G^q \equiv \left(\frac{q}{p}\right) G \bmod q$ si $p > 2$, et $G^q \equiv (-1)^{\frac{q^2-1}{8}} G \bmod q$ si $p = 2$.*

Démonstration — Supposons d'abord p impair. Alors d'après le lemme 1.18 on a

$$G^q \equiv \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{a}{p}\right)^q \zeta^{aq} \bmod q.$$

Remarquons que pour tout $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ on a

$$\left(\frac{a}{p}\right)^q = \left(\frac{a}{p}\right) = \left(\frac{q}{p}\right)\left(\frac{qa}{p}\right),$$

la première égalité venant de ce que q est impair et la seconde de la multiplicativité du symbole de Legendre. La proposition résulte alors du changement de variables $t = aq$. Si $p = 2$, on conclut de même en remarquant que $\zeta^q + \zeta^{-q} = G$ si $q \equiv \pm 1 \bmod 8$, $-G$ sinon (noter $\zeta^3 = -\zeta$). □

Démontrons enfin la loi de réciprocité quadratique. On calcule pour cela $G^q \bmod q$ d'une autre façon. Supposons d'abord p impair. D'après la proposition 1.20, on a

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

Le critère d'Euler assure donc

$$G^q \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right) G \bmod q.$$

En comparant avec la proposition précédente on obtient

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right) G \equiv \left(\frac{q}{p}\right) G \bmod q,$$

puis en multipliant par $(-1)^{\frac{p-1}{2}} G$ et par la proposition 1.20 à nouveau

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right) p \equiv \left(\frac{q}{p}\right) p \bmod q,$$

3. Nous renvoyons au *cours d'arithmétique* de Serre chapitre I pour une variante de la démonstration de ce paragraphe utilisant la somme de Gauss dans les corps finis, dans laquelle la stratégie ci-dessus est encore plus transparente.

qui est une congruence traditionnelle, de laquelle on déduit la loi de réciprocité quadratique car p est inversible dans $\mathbb{Z}/q\mathbb{Z}$ et $q \neq 2$.

Il ne reste donc qu'à étudier le cas $p = 2$. L'argument ci-dessus, et la relation $G^2 = 2$, montrent cette fois

$$\left(\frac{2}{p}\right) G \equiv (-1)^{\frac{q^2-1}{8}} G \bmod q$$

d'où l'on déduit la loi supplémentaire. □

6. Symbole de Jacobi

Le symbole de Jacobi est une extension formelle du symbole de Legendre dont les propriétés permettent en retour de calculer plus facilement des symboles de Legendre.

Définition 1.25. (Jacobi) *Soient m et n des entiers avec n impair positif. On pose*

$$\left(\frac{m}{n}\right) = \prod_{i=1}^{r} \left(\frac{m}{p_i}\right)$$

où $n = p_1 p_2 \cdots p_r$ est la décomposition de n en facteurs premiers (non nécessairement distincts).

Par convention on pose aussi $\left(\frac{m}{1}\right) = 1$ pour tout $m \in \mathbb{Z}$. Par définition, $\left(\frac{m}{n}\right)$ ne dépend que de m modulo n et coïncide avec le symbole de Legendre si n est premier. On prendra garde que l'égalité $\left(\frac{m}{n}\right) = 1$ n'entraîne pas en général que m est un carré modulo n, par exemple $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)\cdot(-1) = 1$ mais 2 n'est pas un carré modulo 15 car il ne l'est pas modulo 3 (ni modulo 5).

Proposition 1.26. *Soient $m, m', n, n' \in \mathbb{Z}$ avec n, n' impairs positifs. On a*

$$\left(\frac{mm'}{n}\right) = \left(\frac{m}{n}\right)\left(\frac{m'}{n}\right), \quad \left(\frac{m}{nn'}\right) = \left(\frac{m}{n}\right)\left(\frac{m}{n'}\right),$$

$$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}, \quad \left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}},$$

et si m est impair positif

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

En effet, la première propriété découle de la multiplicativité du symbole de Legendre et la seconde est évidente. Les autres se déduisent immédiatement par multiplicativité des propriétés correspondantes du symbole de Legendre et du lemme suivant, qui est laissé en exercice au lecteur.

Lemme 1.27. *Soient $n, m \in \mathbb{Z}$ des entiers impairs.*

(i) $\frac{n-1}{2} + \frac{m-1}{2} \equiv \frac{nm-1}{2} \bmod 2$.

(ii) Si $n = \prod_i n_i$ *et* $m = \prod_j m_i$, *alors* $\sum_{i,j} \frac{n_i-1}{2}\frac{m_j-1}{2} \equiv \frac{n-1}{2}\frac{m-1}{2} \bmod 2$.

(iii) $n^2 \equiv 1 \bmod 8$.

(iv) $\frac{n^2-1}{8} + \frac{m^2-1}{8} \equiv \frac{n^2m^2-1}{8} \bmod 2$.

Un premier intérêt du symbole de Jacobi est de fournir un algorithme efficace de calcul de $\left(\frac{m}{n}\right)$ pour tout $m \in \mathbb{Z}$ et tout entier n impair positif premier avec m :

(1) On cherche $-\frac{n-1}{2} \leq m' < \frac{n-1}{2}$ tel que $m \equiv m' \bmod n$ (division euclidienne),

(2) On factorise m' sous la forme $\varepsilon 2^q m''$ avec m'' impair positif et $\varepsilon = \pm 1$,

(3) On applique les propriétés du symbole de Jacobi :

$$\left(\frac{m}{n}\right) = \left(\frac{m'}{n}\right) = \varepsilon^{\frac{n-1}{2}} \left(\frac{2}{n}\right)^q (-1)^{\frac{n-1}{2}\frac{m''-1}{2}} \left(\frac{n}{m''}\right).$$

(4) Si $m'' = 1$ c'est terminé, sinon on retourne au (1) en remarquant que l'on a $m'' < n$ et $(n, m'') = 1$.

L'avantage principal d'un point de vue algorithmique est qu'en phase (2) il n'est pas nécessaire de factoriser m' entièrement (problème réputé très couteux, par exemple impossible pour un ordinateur si m a plus de 200 chiffres), mais simplement d'en extraire la plus grande puissance de 2 (ce qui est très rapide). Au final, on se ramène donc essentiellement à effectuer des divisions euclidiennes.

Par exemple, est-ce que 3763 est un carré modulo le nombre premier 20353 ? On calcule alors $20353 \equiv 1538 \bmod 3763$, $1538 = 2 \cdot 769$, $3763 \equiv -82 \bmod 769$, $82 = 2 \cdot 41$, $769 \equiv -10 \bmod 41$, d'où l'on tire :

$$\left(\frac{3763}{20353}\right) = \left(\frac{1538}{3763}\right) = -\left(\frac{769}{3763}\right)$$

$$= -\left(\frac{-82}{769}\right) = -\left(\frac{41}{769}\right) = -\left(\frac{-10}{41}\right) = -\left(\frac{5}{41}\right) = -1.$$

Ce n'est donc pas un carré. Nous n'avons pas eu à factoriser 3763 (qui vaut en fait $53 \cdot 71$). Le symbole de Jacobi est notamment utilisé dans le test de primalité de *Solovay-Strassen* (voir les exercices).

7. Complément : la structure de $(\mathbb{Z}/N\mathbb{Z})^\times$

Terminons ce chapitre par une étude du groupe $(\mathbb{Z}/N\mathbb{Z})^\times$. On rappelle que c'est un groupe de cardinal $\varphi(N)$ (indicatrice d'Euler).

Proposition 1.28. *L'isomorphisme chinois induit un isomorphisme de groupes*

$$(\mathbb{Z}/MN\mathbb{Z})^\times \xrightarrow{\sim} (\mathbb{Z}/M\mathbb{Z})^\times \times (\mathbb{Z}/N\mathbb{Z})^\times.$$

Démonstration — Si A et B sont deux anneaux commutatifs unitaires, on vérifie immédiatement l'égalité $(A \times B)^\times = A^\times \times B^\times$. La proposition découle alors du lemme chinois des restes. □

Il suffit donc d'étudier la structure du groupe $(\mathbb{Z}/p^m\mathbb{Z})^\times$ lorsque p est un nombre premier et $m \geq 1$. Il est de cardinal $\varphi(p^m) = (p-1)p^{m-1}$. Commençons par le cas crucial $m = 1$.

Théorème 1.29. (Gauss) *Le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique d'ordre $p-1$.*

Rappelons que $\mathbb{Z}/p\mathbb{Z}$ est un corps, en particulier $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{Z}/p\mathbb{Z} - \{0\}$ a $p-1$ éléments. Nous allons en fait démontrer le résultat plus général suivant : si k est un corps (commutatif) et si G est un sous-groupe fini de $k^\times$, alors G est cyclique.

Démonstration — Soient k et $G \subset k^\times$ comme ci-dessus. Posons $n = |G|$. Il suffit de démontrer que, si $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ est la décomposition en facteurs premiers de n, alors G possède un élément x_i d'ordre $p_i^{\alpha_i}$ pour tout i. En effet, le lemme ci-dessous assurera alors que l'élément $x_1 x_2 \cdots x_r$ est d'ordre n.

Considérons le polynôme $P = X^n - 1 \in k[X]$. Comme k est un corps, P admet au plus n racines dans k. D'autre part, le théorème de Lagrange assure que les n éléments de G sont racines de P : il est donc scindé à racines distinctes, égales aux éléments de G. Remarquons que si d est un diviseur de n, alors $X^d - 1$ divise $X^n - 1$ dans $k[X]$, le quotient étant $\sum_{i=0}^{n/d-1} X^{id}$. En particulier, $X^d - 1$ est aussi scindé à racines distinctes dans G. Pour tout i, il existe donc au moins une racine x_i de $X^{p_i^{\alpha_i}} - 1$ dans G qui n'est pas racine de $X^{p_i^{\alpha_i - 1}} - 1$. Un tel élément est donc d'ordre $p_i^{\alpha_i}$, ce qui conclut la démonstration. □

Lemme 1.30. *Soient H un groupe commutatif fini, et $x, y \in H$ d'ordres respectifs a et b. Si a et b sont premiers entre eux alors xy est d'ordre ab.*

Démonstration — Considérons l'intersection $M = \langle x \rangle \cap \langle y \rangle$. C'est un sous-groupe de $\langle x \rangle$ et de $\langle y \rangle$. D'après Lagrange, $|M|$ divise a et b et donc $M = \{1\}$. Vérifions maintenant que xy est d'ordre ab. Soit $k \in \mathbb{Z}$. Comme $xy = yx$, on a $(xy)^k = x^k y^k$. En particulier, $(xy)^{ab} = 1$. Réciproquement, si $(xy)^k = 1$ alors $x^k = y^{-k} \in M = \{1\}$, et donc $x^k = y^{-k} = 1$. Ainsi, $a|k$ et $b|k$ puis $ab|k$. □

Théorème 1.31. (Gauss)

(i) Si p est premier impair, alors $(\mathbb{Z}/p^m\mathbb{Z})^\times$ est cyclique.

(ii) Si $m \geq 2$ alors $(\mathbb{Z}/2^m\mathbb{Z})^\times \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{m-2}\mathbb{Z})$.

Commençons par établir une congruence utile.

Lemme 1.32. *Soit $k \geq 0$ un entier.*

(i) Si p est un nombre premier impair, alors $(1+p)^{p^k} \equiv 1 + p^{k+1} \bmod p^{k+2}$.

(ii) De plus, on a $(1+4)^{2^k} \equiv 1 + 2^{k+2} \bmod 2^{k+3}$.

Démonstration — Commençons par une observation : si p est un nombre premier, et si $k \geq 1$, alors $a \equiv b \bmod p^k$ entraîne $a^p \equiv b^p \bmod p^{k+1}$. En effet, cela découle immédiatement de ce que $\binom{p}{i} \equiv 0 \bmod p$ si $i = 1, \ldots, p-1$. Le (i) et (ii) s'en déduisent par récurrence sur k. Remarquer aussi que le (i) ne s'étend pas au cas $p = 2$ et $k = 1$. □

Démonstration — (de la proposition) Le lemme précédent (ii) assure que la classe de 5 est d'ordre 2^{m-2} dans $(\mathbb{Z}/2^m\mathbb{Z})^\times$. Vérifions que le morphisme de groupes

$$\mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/2^{m-2}\mathbb{Z}) \to (\mathbb{Z}/2^m\mathbb{Z})^\times,$$

donné par $(p, q) \mapsto (-1)^p 5^q \bmod 2^m$, est un isomorphisme. Pour des raisons de cardinalité, il suffit de voir qu'il est injectif. Mais si $(-1)^p 5^q \equiv 1 \bmod 2^m$, alors par réduction modulo 4 on obtient $(-1)^p = 1$, puis $5^q \equiv 1 \bmod 2^m$ et donc $q = 0$ car 5 est d'orde 2^{m-2} modulo 2^m, ce qui démontre le (ii).

Supposons maintenant p impair. Le lemme précédent assure que $1+p$ est d'ordre p^{m-1} modulo p^m. Comme $(p-1, p) = 1$, et d'après le lemme 1.30, il suffit pour conclure de trouver un élément d'ordre $p-1$ dans $(\mathbb{Z}/p^m\mathbb{Z})^\times$. D'après Gauss, il existe un entier a dont la classe engendre $(\mathbb{Z}/p\mathbb{Z})^\times$ modulo p. Soit d l'ordre de la classe de a dans $(\mathbb{Z}/p^m\mathbb{Z})^\times$. En réduisant modulo p la relation $a^d \equiv 1 \bmod p^m$ on constate que $p-1$ divise d. On vérifie alors immédiatement que $a^{\frac{d}{p-1}}$ est d'ordre $p-1$ dans $(\mathbb{Z}/p^m\mathbb{Z})^\times$. □

Un entier a dont la classe dans $\mathbb{Z}/N\mathbb{Z}$ engendre $(\mathbb{Z}/N\mathbb{Z})^\times$ est parfois appelé une *racine primitive modulo* N. Par exemple, 2 est une racine primitive modulo 5 mais pas modulo 7. En effet, les puissances successives de 2 modulo 5 sont $\equiv 1, 2, 4, 3$ et parcourent donc tout $(\mathbb{Z}/5\mathbb{Z})^\times$. Par contre, les puissances successives de 2 modulo 7 sont $\equiv 1, 2, 4$ et 2 est seulement d'ordre 3 modulo 7. Le théorème de Gauss assure l'existence de racines primitives modulo tout nombre premier p, mais ne fournit pas pour autant de procédé constructif efficace pour en construire. Mentionnons cette conjecture célèbre due à E. Artin : "tout entier $a \neq -1$ qui n'est pas un carré est une racine primitive modulo p pour une infinité de nombres premiers p".

En guise d'application du théorème de Gauss, voici une généralisation du critère d'Euler.

Proposition 1.33. (Critère d'Euler généralisé) *Soient p un nombre premier impair et n un entier divisant $p-1$. Alors $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ est une puissance n*ième *si, et seulement si, $x^{\frac{p-1}{n}} = 1$.*

Le critère d'Euler s'en déduit : en effet, le petit théorème de Fermat assure que si $(a, p) = 1$, alors $(a^{\frac{p-1}{2}})^2 \equiv 1 \bmod p$ et donc $a^{\frac{p-1}{2}} \equiv \pm 1 \bmod p$ par un argument déjà donné dans la preuve de la proposition 1.2.

Démonstration — (du critère d'Euler généralisé) Si $x = y^n$ avec $y \in (\mathbb{Z}/p\mathbb{Z})^\times$, le petit théorème de Fermat entraîne que $x^{\frac{p-1}{n}} = 1$. Réciproquement, supposons que $x^{\frac{p-1}{n}} = 1$. Soit $y \in (\mathbb{Z}/p\mathbb{Z})^\times$ un générateur (qui existe d'après le théorème de Gauss), écrivons $x = y^k$ pour un certain $k \in \mathbb{Z}$. Il vient $y^{k\frac{p-1}{n}} = 1$ et donc $p-1$ (l'ordre de

y) divise $k\frac{p-1}{n}$. Ceci entraîne que n divise k, puis que $x = (y^{k/n})^n$ est une puissance $n$ième. □

Remarque 1.34. En guise d'autre application, retrouvons que si $a \equiv 1 \bmod 8$ alors a est un carré dans $\mathbb{Z}/2^m\mathbb{Z}$ pour tout entier $m \geq 3$ (Lemme. 1.11). D'après la démonstration du théorème 1.31, a s'écrit $(-1)^p 5^q$ avec $(p, q) \in (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{m-2}\mathbb{Z})$. Comme $a \equiv 1 \bmod 8$, on a $p = 0$ et $q \equiv 0 \bmod 2$, mézalor $a = (5^{q/2})^2$ est un carré. On en déduirait de même aisément le reste du lemme 1.11.

8. Exercices

Dans ces exercices, le nombre p désignera par défaut un nombre premier impair.

Exercice 1.1. *Est-ce que* 47 *est un carré modulo* 79 *?*

Exercice 1.2. *Soient p et q des nombres premiers impairs. Vérifier que la loi de réciprocité quadratique s'écrit aussi $\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right)$ où $q^* = (-1)^{\frac{q-1}{2}} q$.*

Exercice 1.3. *Soient $a, b \in \mathbb{Z}$ et $D := a^2 - 4b$. Montrer que l'image du polynôme $X^2 + aX + b$ dans $(\mathbb{Z}/p\mathbb{Z})[X]$ (resp. $(\mathbb{Z}/2\mathbb{Z})[X]$) est irréductible si, et seulement si, on a $\left(\frac{D}{p}\right) = -1$ (resp. $D \equiv 5 \bmod 8$).*

Exercice 1.4. *On se propose de calculer $\left(\frac{-3}{p}\right)$ sans utiliser la loi de réciprocité quadratique.*

(i) Montrer que $(\mathbb{Z}/p\mathbb{Z})^\times$ admet un élément d'ordre 3 si, et seulement si, $p \equiv 1 \bmod 3$.

(ii) Conclure en considérant le polynôme $X^2 + X + 1$ dans $(\mathbb{Z}/p\mathbb{Z})[X]$.

Exercice 1.5. *On suppose $p \equiv 1 \bmod 4$. Montrer $(\frac{p-1}{2})!^2 \equiv -1 \bmod p$.*

Exercice 1.6. *(i) Montrer qu'au moins l'un des entiers -1, 2 ou -2 est un carré modulo p.*

(ii) En déduire que le polynôme X^4+1 est irréductible dans $\mathbb{Q}[X]$ mais réductible dans $(\mathbb{Z}/p\mathbb{Z})[X]$ pour tout nombre premier p.

Exercice 1.7. *Montrer que -1 est une puissance 4ème modulo p si, et seulement si, on a $p \equiv 1 \bmod 8$.*

Exercice 1.8. (Carrés modulo p de l'intervalle $\{1, \ldots, \frac{p-1}{2}\}$). *Soit C le nombre de carrés modulo p appartenant à l'intevalle $\{1, \ldots, \frac{p-1}{2}\}$, et soit N celui des non-carrés, de sorte que l'on ait $C + N = \frac{p-1}{2}$.*

(i) Montrer que $p \equiv 1 \bmod 4$ *entraîne* $C = \frac{p-1}{4}$.

(ii) Montrer que l'on a $C = N$, *si, et seulement si,,* $p \equiv 1 \bmod 4$.

On se propose de montrer que si $p \equiv 3 \bmod 8$ *et* $p \neq 3$ *alors* $C \equiv N \bmod 3$. *On introduit les entiers*

$$A = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) a, \quad B = \sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right) a \text{ et } C = \sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right).$$

(iii) Montrer $A = (1 - \left(\frac{-1}{p}\right))B + p\left(\frac{-1}{p}\right)C$.

(iv) Montrer $A = \left(\frac{2}{p}\right)\left[2\,(1 - \left(\frac{-1}{p}\right))B + p\left(\frac{-1}{p}\right)C\right]$.

(v) En déduire que si $p \equiv 3 \bmod 8$ *alors on a* $pC = 3B$.

(vi) Conclure et donner quelques exemples.

Exercice 1.9. *Soient* $\alpha, \beta \in (\mathbb{Z}/p\mathbb{Z})^\times$. *On se propose de calculer le nombre* S *des solutions* $(x, y) \in (\mathbb{Z}/p\mathbb{Z})^2$ *de l'équation* $\alpha x^2 + \beta y^2 = 1$.

(i) Soit $a \in \mathbb{Z}/p\mathbb{Z}$. *Montrer le nombre* $\mathrm{N}(x^2 = a)$ *des* $x \in \mathbb{Z}/p\mathbb{Z}$ *tels que* $x^2 = a$ *vaut* $1 + \left(\frac{a}{p}\right)$.

(ii) En déduire $S = \sum_{a,b \in \mathbb{Z}/p\mathbb{Z}, \alpha a + \beta b = 1} \mathrm{N}(x^2 = a)\mathrm{N}(x^2 = b)$, *puis* $S = p + \left(\frac{\beta}{p}\right) J$ *où* $J = \sum_{a \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{a(1-\alpha a)}{p}\right)$.

(iii) Montrer $J = \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{a^{-1} - \alpha}{p}\right)$, *puis* $S = p - \left(\frac{-\alpha\beta}{p}\right)$.

(iv) En déduire $S \neq 0$.

(v) Que dire du nombre des solutions $(x, y) \in (\mathbb{Z}/p\mathbb{Z})^2$ *de l'équation* $\alpha x^2 + \beta y^2 = 0$ *?*

Exercice 1.10. *Soient* $m, n \in \mathbb{Z}$ *avec* n *impair positif. Montrer que si le symbole de Jacobi* $\left(\frac{m}{n}\right)$ *vaut* -1 *alors* m *n'est pas un carré modulo* n.

Exercice 1.11. (Test de primalité de Solovay-Strassen) *Soit* n *un entier impair positif.*

(i) Montrer que n *est premier si, et seulement si,* $x^{\frac{n-1}{2}} \equiv \left(\frac{x}{n}\right) \bmod n$ *pour tout* $x \in (\mathbb{Z}/n\mathbb{Z})^\times$.

(ii) En déduire que si n *n'est pas premier, au moins la moitié des* $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ *vérifient* $x^{\frac{n-1}{2}} \not\equiv \left(\frac{x}{n}\right) \bmod n$.

Exercice 1.12. *Soit* $0 \leq i \leq p-1$. *Montrer que la somme* $\sum_{a \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{a}{p}\right) a^i$ *vaut* 0 *si* $i \neq \frac{p-1}{2}$, $p-1$ *sinon.*

Exercice 1.13. *Si G désigne la somme de Gauss relative à p, montrer l'identité $G = \sum_{a=0}^{p-1} \zeta^{a^2}$.*

Exercice 1.14. (Le signe de la somme de Gauss,[4] d'après Dirichlet) *Soient $N \geq 1$ et $G_N = \sum_{a=0}^{N-1} e^{\frac{2i\pi a^2}{N}}$.*

(i) Soient $a < b$ deux entiers et $f : [a, b] \to \mathbb{C}$ une fonction continue et $\mathcal{C}^1$ par morceaux. Montrer

$$\frac{f(a) + f(b)}{2} + \sum_{k=a+1}^{b-1} f(k) = \sum_{n\in\mathbb{Z}} \int_a^b f(t)e^{2i\pi nt}dt.$$

(ii) Montrer $G_N = (1 + i^{-N})N^{\frac{1}{2}}I$ où $I = \int_{-\infty}^{+\infty} e^{2i\pi t^2}dt$.

(iii) En déduire $I = \frac{1+i}{2}$ (intégrale de Gauss) et

$$G_N = \begin{cases} (1+i)N^{\frac{1}{2}} & \text{si } N \equiv 0 \bmod 4, \\ N^{\frac{1}{2}} & \text{si } N \equiv 1 \bmod 4, \\ 0 & \text{si } N \equiv 2 \bmod 4, \\ iN^{\frac{1}{2}} & \text{si } N \equiv 3 \bmod 4. \end{cases}$$

Exercice 1.15. *(i) Montrer que si $a \in \mathbb{Z}$ est un carré modulo p, alors a n'est pas une racine primitive modulo p.*

(ii) On suppose de plus que $\frac{p-1}{2}$ est premier. Montrer que $a \in \mathbb{Z}$ est une racine primitive modulo p si, et seulement si, $\left(\frac{a}{p}\right) = -1$ et $a \not\equiv \pm 1 \bmod p$.

Exercice 1.16. *On suppose que p est un nombre premier de Fermat[5], c'est-à-dire de la forme $2^{2^m} + 1$. Par exemple, $p = 3, 5, 17, 257$ ou 65537.*

(i) Montrer que $a \in \mathbb{Z}$ est une racine primitive modulo p si, et seulement si, $\left(\frac{a}{p}\right) = -1$.

(ii) En déduire que 3 est une racine primitive modulo p dès que $p \neq 3$.

Exercice 1.17. *Quelle est la période du décimal $\frac{1}{65537}$?*

Exercice 1.18. *Montrer que le groupe multiplicatif du corps (non-commutatif) des quaternions de Hamilton contient un sous-groupe fini non-cyclique.*

Exercice 1.19. *(i) Montrer que si G est un groupe cyclique et si q divise $|G|$, alors G a un unique sous-groupe de cardinal q, qui est cyclique.*

---

4. Lorsque N est premier impair, cette somme est bien la somme de Gauss relative à N d'après l'exercice 1.13.

5. Fermat avait conjecturé que tous les nombres de la forme $F_m = 2^{2^m} + 1$ sont des nombres premiers. Euler a remarqué qu'il n'en est rien car 641 divise F_5. En fait, les seuls F_m premiers connus actuellement sont F_0 à F_4 cités ci-dessus.

(ii) En déduire que $(\mathbb{Z}/N\mathbb{Z})^\times$ est cyclique si, et seulement si, $N = 2, 4, p^m, 2p^m$ où p est premier impair et $m \geq 0$.

Exercice 1.20. *Soient $N \geq 2$ un entier et soit $\mathcal{Q}$ la réunion de l'ensemble des nombres premiers impairs et de $\{4, 8\}$. Soient s le nombre d'éléments de $\mathcal{Q}$ divisant N et $C(N)$ l'ensemble des carrés de $(\mathbb{Z}/N\mathbb{Z})^\times$.*

(i) Montrer $|C(N)| = \frac{\varphi(N)}{2^s}$ et $(\mathbb{Z}/N\mathbb{Z})^\times/C(N) \simeq (\mathbb{Z}/2\mathbb{Z})^s$.

(ii) Montrer que si $a \in C(N)$, il existe exactement 2^s éléments $b \in (\mathbb{Z}/N\mathbb{Z})^\times$ tels que $a = b^2$.

Exercice 1.21. *Soit $N \geq 2$ un entier. Montrer que $\overline{\mathbb{Z}}/N\overline{\mathbb{Z}}$ est infini.*

Exercice 1.22. (Une démonstration géométrique de la loi de réciprocité quadratique, d'après Eisenstein [6]) *Soit p un nombre premier impair et soit $q \geq 1$ un entier impair premier à p. On se propose de montrer, suivant Eisenstein, la relation*

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

où e désigne le nombre des points de coordonnées entières à l'intérieur du triangle OP'S' (figure 1).

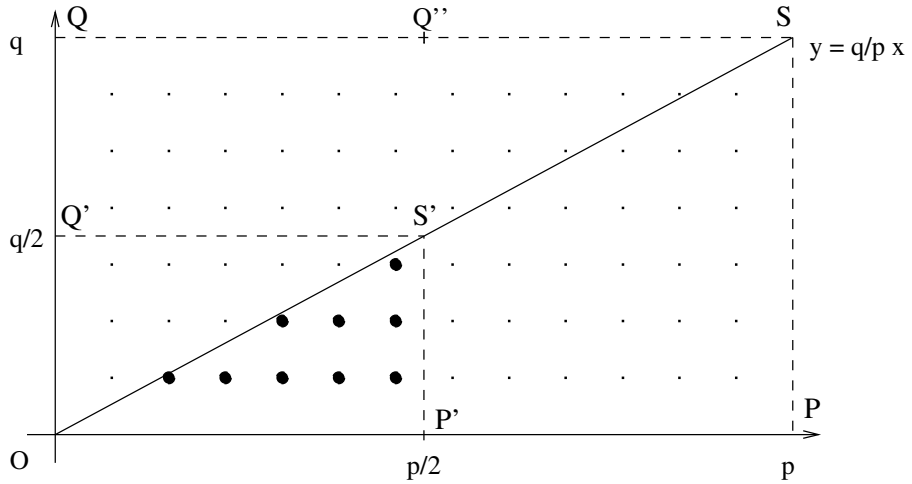

FIGURE 1. $\left(\frac{q}{p}\right) = (-1)^e$ où e est le nombre de points noirs (Eisenstein)

(i) En déduire la loi de réciprocité quadratique.

On suppose d'abord simplement l'entier $q \geq 1$ premier à p. On pose $X = \{2, 4, \ldots, p-1\}$ et on note $R \subset \{1, \ldots, p-1\}$ l'ensemble des restes de la division par p des qx, pour $x \in X$.

6. *Geometrischer Beweis des Fundamentaltheorems für die quadratischen Reste*, Crelle's Journal 28, 246–249 (1844).

(ii) Vérifier que l'application $\{1, \dots, p-1\} \to X$*, définie par*

$$r \mapsto \begin{cases} r & \text{si } r \text{ est pair,} \\ p-r & \text{sinon,} \end{cases}$$

induit une bijection de R *sur* X*.*

(iii) En déduire $\left(\frac{q}{p}\right) = (-1)^{\sum r}$*, la somme portant sur les* $r \in R$*. (On pourra considérer le produit des éléments de* X *modulo* p*)*

(iv) Vérifier que si $x \in X$*, et si* r *est le reste de la division de* qx *par* p*, on a* $r \equiv [qx/p] \bmod 2$*.*

(v) En déduire $\left(\frac{q}{p}\right) = (-1)^f$ *où* f *désigne le nombre des points à l'intérieur du triangle* OPS *dont les coordonnées sont entières, et d'abscisse paire.*

(vi) On suppose q *impair. Soit* A *(resp.* B*) le nombre des points à coordonnées entières et d'abscisse paire à l'intérieur du trapèze* $P'PSS'$ *(resp. du triangle* $S'SQ''$*). Montrer* $A \equiv B \bmod 2$*.*

(vii) En déduire la relation d'Eisenstein.

(viii) Montrer aussi $\left(\frac{2}{p}\right) = (-1)^f$ *où* f *désigne le nombre d'entiers pairs compris entre* $p/2$ *et* p*, puis* $f \equiv \frac{p^2-1}{8} \bmod 2$*.*