Chapitre 3

Résidus quadratiques

Dans ce chapitre, on s'intéresse à l'ensemble des carrés dans le corps $\mathbf{F}_p$, p premier. On introduit le symbole de Legendre qui permet de caractériser ces carrés et on développe les principales propriétés de ce symbole. On démontre notamment la "fameuse" loi de réciprocité quadratique due à Gauss. Cette formule admet de nombreuses démonstrations. Nous donnerons celle basée sur les sommes de Gauss. Ces sommes de Gauss seront également utilisées pour obtenir une formule pour le nombre de solutions d'une équation quadratique.

3.1 Résidus quadratiques modulo p.

Définition 3.1.1 *Soit p un nombre premier et a un entier tel que p ne divise pas a. Alors a est appelé un* **résidu quadratique** *modulo p si l'équation $x^2 \equiv a \pmod{p}$ possède une solution. Dans le cas contraire, a est appelé un* **non résidu quadratique** *modulo p.*

Autrement dit, un entier a est un résidu quadratique modulo p si et seulement si $a \bmod p$ est un carré dans $(\mathbb{Z}/p\mathbb{Z})^*$.

Commençons par un exemple simple. Dressons la table des carrés dans $\mathbb{Z}/p\mathbb{Z}$, avec $p = 7$.

$x \bmod 7$	0	1	2	3	4	5	6
$x^2 \bmod 7$	0	1	4	2	2	4	1

Parmi les 6 éléments non nuls, 3 sont des carrés $\{1, 2, 4\}$, les 3 autres ne sont pas des carrés. De plus, chaque carré non nul a deux racines carrées :

$$\sqrt{1} = \pm 1, \quad \sqrt{2} = \pm 3, \quad \sqrt{4} = \pm 2.$$

Les deux observations effectuées sur cet exemple sont en fait un théorème !

Théorème 3.1.2 *Soit p un nombre premier impair et g un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$. Un élément a de $(\mathbb{Z}/p\mathbb{Z})^*$ est un carré si et seulement si son logarithme en base g est pair. Parmi les $p-1$ éléments de $(\mathbb{Z}/p\mathbb{Z})^*$, la moitié exactement sont des carrés. Chaque carré a 2 racines carrés.*

Preuve : Soit $a \in (\mathbb{Z}/p\mathbb{Z})^*$ et k son logarithme en base g. Si $k = 2\ell$ est pair, alors on a

$$a = (g^\ell)^2$$

et donc a est un carré. Réciproquement, si a est le carré de g^t, pour un certain t, on a $a = g^{2t}$. Donc d'après le lemme 2.4.1, son logarithme discret est le reste de la division euclidienne de $2t$ par $p-1$. Ce reste est pair car $p-1$ est pair. On en déduit alors que les carrés de $(\mathbb{Z}/p\mathbb{Z})^*$ sont

$$\{g^t : 0 \leq t \leq p-2 : t \equiv 1 \pmod 2\}.$$

On en déduit donc qu'il existe exactement $(p-1)/2$ carrés dans $(\mathbb{Z}/p\mathbb{Z})^*$.

D'autre part, si a est un carré, $a = b^2$, l'élément $-b$ est aussi une racine du polynôme $x^2 - a$, distincte de la racine b (car $a \neq 0$). Le polynôme $x^2 - a$ de $\mathbf{F}_p[x]$ étant de degré 2, il n'admet pas d'autres racines.

□

En d'autres termes, le théorème 3.1.2 affirme qu'étant donné un nombre premier impair p, il existe exactement $(p-1)/2$ résidus quadratiques et $(p-1)/2$ non-résidus quadratiques modulo p.

Le résultat suivant fournit un critère pour qu'un entier soit un résidu quadratique modulo p.

Théorème 3.1.3 (Euler) *Soit p un nombre premier impair et a un entier tel que p ne divise pas a. Alors*

(a) a est un résidu quadratique modulo p si et seulement si $a^{(p-1)/2} \equiv 1 \pmod p$.

(b) a est un non-résidu quadratique modulo p si et seulement si $a^{(p-1)/2} \equiv -1 \pmod p$.

Preuve : D'après le théorème de Fermat (théorème 1.5.2), on a

$$\left(a^{(p-1)/2}\right)^2 = a^{p-1} \equiv 1 \pmod p.$$

Donc $a^{(p-1)/2}$ est une solution de la congruence $x^2 \equiv 1 \pmod p$ et donc

$$a^{(p-1)/2} \equiv \pm 1 \pmod p.$$

Supposons que a soit un résidu quadratique modulo p. Alors $a \equiv b^2 \pmod{p}$, pour un certain entier b et donc

$$a^{(p-1)/2} = b^{p-1} \equiv 1 \pmod{p}.$$

D'après le théorème 2.1.2, l'équation

$$x^{(p-1)/2} \equiv 1 \pmod{p}$$

a exactement $(p-1)/2$ solutions. Comme il y a $(p-1)/2$ résidus quadratiques modulo p, les solutions de l'équation précédente sont exactement les résidus quadratiques. Ainsi, pour un non-résidu quadratique a, on a $a^{(p-1)/2} \equiv -1 \pmod{p}$.

□

3.2 Le symbole de Legendre

Définition 3.2.1 *Soient p un nombre premier impair et $a \in \mathbb{Z}$. On définit le* **symbole de Legendre** *par*

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \textit{si } a \textit{ est un résidu quadratique modulo } p \\ -1 & \textit{si } a \textit{ est un non-résidu quadratique modulo } p \\ 0 & \textit{si } p \textit{ divise } a. \end{cases}$$

Il est clair que, pour tout nombre premier impair p, on a

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

Le résultat suivant est une conséquence immédiate du résultat d'Euler.

Corollaire 3.2.2 (Critère d'Euler) *Soient p un nombre premier impair et a un entier. On a*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

Théorème 3.2.3 (Périodicité du symbole de Legendre) *Soient p un nombre premier impair, $a \in \mathbb{Z}$ et $m \in \mathbb{Z}$. On a*

$$\left(\frac{a+mp}{p}\right) = \left(\frac{a}{p}\right).$$

Preuve : Il est clair que p divise a si et seulement si p divise $a + mp$. On peut donc supposer maintenant que p ne divise pas a. Alors $\left(\frac{a}{p}\right) = 1$ si et seulement si l'équation

$$x^2 \equiv a \pmod{p}$$

a une solution, ce qui est équivalent au fait que l'équation

$$x^2 \equiv a + mp \,(\mathrm{mod}\, p)$$

a une solution, c'est à dire que $\left(\frac{a+mp}{p}\right) = 1$.

□

Le théorème 3.2.3 permet d'étendre la définition du symbole de Legendre modulo p à $\mathbb{Z}/p\mathbb{Z}$. Ainsi, on pose

$$\left(\frac{a \bmod p}{p}\right) := \left(\frac{a}{p}\right).$$

Théorème 3.2.4 (Multiplicativité du symbole de Legendre) *Soient $a, b \in \mathbb{Z}$ et p un nombre premier impair. On a*

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

Preuve : En utilisant le critère d'Euler, on a

$$\begin{aligned}\left(\frac{ab}{p}\right) &\equiv (ab)^{(p-1)/2} \,(\mathrm{mod}\, p)\\ &\equiv a^{(p-1)/2} b^{(p-1)/2} \,(\mathrm{mod}\, p)\\ &\equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \,(\mathrm{mod}\, p),\end{aligned}$$

ce qui donne le résultat.

□

Le théorème 3.2.4 implique que le symbole de Legendre est complètement déterminé par ses valeurs en -1, 2 et aux entiers impairs. En effet, si a est un entier non divisible par p, alors on peut écrire a sous la forme

$$a = \pm 2^{r_0} q_1^{r_1} q_2^{r_2} \dots q_k^{r_k},$$

où $q_1, \dots, q_k$ sont des entiers premiers impairs, distinct et différent de p. Alors on a

$$\left(\frac{a}{p}\right) = \left(\frac{\pm 1}{p}\right)\left(\frac{2}{p}\right)^{r_0}\left(\frac{q_1}{p}\right)^{r_1} \dots \left(\frac{q_k}{p}\right)^{r_k}.$$

On peut déterminer l'ensemble des nombres premiers p pour lesquels -1 est un résidu quadratique. D'après le résultat suivant, cela dépend uniquement de la classe de congruence de p modulo 4.

Théorème 3.2.5 (Caractère quadratique de -1) *Soit p un nombre premier impair. Alors*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1 \,(\mathrm{mod}\, 4) \\ -1 & \text{si } p \equiv 3 \,(\mathrm{mod}\, 4). \end{cases}$$

De façon équivalente, on a

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

Preuve : Observons que

$$(-1)^{(p-1)/2} = \begin{cases} 1 & \text{si } p \equiv 1 \,(\mathrm{mod}\, 4) \\ -1 & \text{si } p \equiv 3 \,(\mathrm{mod}\, 4). \end{cases}$$

D'autre part, en appliquant le critère d'Euler, on a

$$\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \,(\mathrm{mod}\, p)$$

et le résultat suit immédiatement car chacun des termes de la congruence est ± 1.

□

Le résultat suivant donne un critère pour que 2 soit un carré modulo p.

Théorème 3.2.6 (Caractère quadratique de 2.) *Soit p un entier premier impair. On a*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{si } p \equiv \pm 1 \,(\mathrm{mod}\, 8) \\ -1 & \text{si } p \equiv \pm 3 \,(\mathrm{mod}\, 8). \end{cases}$$

Preuve : Soit ζ une racine primitive 8-ème de l'unité sur $\mathbf{F}_p$ et posons $y = \zeta + \zeta^{-1}$. On a $y^2 = \zeta^2 + \zeta^{-2} + 2$. D'autre part, comme $\zeta^8 = 1$, on a $\zeta^4 = \pm 1$; mais le cas $\zeta^4 = 1$ est exclu car sinon ζ ne serait pas une racine primitive. Il en résulte donc que $\zeta^4 = -1$. Cela implique que $\zeta^2 = -\zeta^{-2}$ et donc $y^2 = 2$. En utilisant la formule du binôme de Newton, on obtient également que

$$y^p = \zeta^p + \zeta^{-p} + \sum_{1 \le i \le p-1} \binom{i}{p} \zeta^i \zeta^{-p+i}.$$

Or $\binom{i}{p} \equiv 0 \,(\mathrm{mod}\, p)$ pour tout $1 \le i \le p-1$, d'où

$$y^p = \zeta^p + \zeta^{-p}.$$

Comme $y^2 = 2$, on obtient que 2 est un carré modulo p si et seulement si $y \in \mathbf{F}_p$, ce qui est équivalent à $y^p = y$. Si $p \equiv \pm 1 \,(\mathrm{mod}\, 8)$, alors on a

$$y^p = \zeta + \zeta^{-1} = y,$$

donc 2 est un carré modulo p et $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = 1$. Si $p \equiv \pm 3 \,(\mathrm{mod}\, 8)$, on a

$$y^p = \zeta^3 + \zeta^{-3},$$

et en utilisant que $\zeta^4 = -1$, on obtient

$$y^p = -\zeta^{-1} - \zeta = -y$$

et donc 2 n'est pas un carré modulo p. D'où $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = -1$.

□

Lemme 3.2.7 *On a*

$$\sum_{\bar{a}\in\mathbf{F}_p^*}\left(\frac{a}{p}\right)=0.$$

Preuve : Il suffit de se rappeler qu'il y a autant de carrés que de non-carrés dans $\mathbf{F}_p^*$ d'après le théorème 3.1.2.

□

3.3 Les sommes de Gauss

Les sommes de Gauss sont très importantes en arithmétique. Nous allons les utiliser pour donner une démonstration de la loi de réciprocité quadratique. Nous les utiliserons également pour calculer le nombre de solutions modulo p d'une équation quadratique. Dans cette section, nous introduisons ces sommes et donnons quelques formules utiles pour la suite.

Soient p un nombre premier impair, K un corps de caractéristique q différente de p et soit ζ une racine primitive p-ième de l'unité sur K. Pour $x\in\mathbb{Z}$, l'élément ζ^x ne dépend que de $x \bmod p$ et donc il garde un sens pour $x\in\mathbf{F}_p$. Pour $a\in\mathbf{F}_p^*$, on pose

$$\tau(a)=\sum_{x\in\mathbf{F}_p^*}\left(\frac{x}{p}\right)\zeta^{ax}.$$

L'élément $\tau(a)$, qui appartient à $\Sigma_p(K)$ (le corps des racines p-ième de l'unité sur K, voir appendice) s'appelle la **somme de Gauss** sur K associée à a.

Théorème 3.3.1 *Soient K un corps de caractéristique q, soit p un nombre premier impair, $p\neq q$. Alors, on a les propriétés suivantes :*

(i) pour tout $a\in\mathbf{F}_p^*$,

$$\tau(a)=\left(\frac{a}{p}\right)\tau(1).$$

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

(iii) si q est un nombre premier impair, pour tout $a\in\mathbf{F}_p^*$, on a

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

Preuve : (i) : l'application $x\longmapsto ax$ est une bijection de $\mathbf{F}_p^*$ sur $\mathbf{F}_p^*$. On a donc

$$\begin{aligned}\tau(a) &= \sum_{y\in\mathbf{F}_p^*}\left(\frac{a^{-1}y}{p}\right)\zeta^y\\ &= \sum_{y\in\mathbf{F}_p^*}\left(\frac{a^{-1}}{p}\right)\left(\frac{y}{p}\right)\zeta^y\\ &= \left(\frac{a^{-1}}{p}\right)\tau(1).\end{aligned}$$

Or $\left(\frac{a^{-1}}{p}\right) = \left(\frac{a}{p}\right)^{-1} = \left(\frac{a}{p}\right)$ car $\left(\frac{a}{p}\right) \in \{-1, 1\}$. D'où $\tau(a) = \left(\frac{a}{p}\right)\tau(1)$.

(ii) : pour simplifier, nous noterons $\tau = \tau(1)$. En utilisant le théorème 3.2.4, on a

$$\tau^2 = \left(\sum_{x\in\mathbf{F}_p^*}\left(\frac{x}{p}\right)\zeta^x\right)\left(\sum_{y\in\mathbf{F}_p^*}\left(\frac{x}{p}\right)\zeta^y\right) = \sum_{x,y\in\mathbf{F}_p^*}\left(\frac{xy}{p}\right)\zeta^{x+y}.$$

Si on effectue le changement de variable $t = x^{-1}y$, on a $y = xt$ et donc $xy = x^2t$. D'où

$$\left(\frac{xy}{p}\right) = \left(\frac{x^2t}{p}\right) = \left(\frac{x^2}{p}\right)\left(\frac{t}{p}\right) = \left(\frac{t}{p}\right).$$

Donc

$$\tau^2 = \sum_{x,t\in\mathbf{F}_p^*}\left(\frac{t}{p}\right)\zeta^{x(1+t)} = \sum_{t\in\mathbf{F}_p^*}\left(\frac{t}{p}\right)\left(\sum_{x\in\mathbf{F}_p^*}\zeta^{x(1+t)}\right).$$

Si $1 + t \equiv 0 \pmod{p}$, alors $\zeta^{x(1+t)} = 1$ donc

$$\sum_{x\in\mathbf{F}_p^*}\zeta^{x(1+t)} = p - 1.$$

Si $1 + t \not\equiv 0 \pmod{p}$, alors l'application $x \longmapsto x(1 + t)$ est une bijection de $\mathbf{F}_p^*$ sur $\mathbf{F}_p^*$, d'où

$$\sum_{x\in\mathbf{F}_p^*}\zeta^{x(1+t)} = \zeta + \zeta^2 + \cdots + \zeta^{p-1} = -1.$$

Ainsi

$$\tau^2 = \left(\frac{-1}{p}\right)(p-1) - \sum_{t\neq -1}\left(\frac{t}{p}\right) = \left(\frac{-1}{p}\right)p - \sum_{t\in\mathbf{F}_p^*}\left(\frac{t}{p}\right).$$

Il reste à appliquer le lemme 3.2.7 pour conclure la preuve du (ii).

(iii) : remarquons que $\left(\frac{a}{p}\right)^{q-1} = 1$. Donc, d'après (i), il suffit de prouver le résultat pour $a = 1$. En notant $\tau = \tau(1)$, comme la caractéristique de $\Sigma_p(K)$ est égale à q, on a

$$\tau^q = \sum_{x\in\mathbf{F}_p^*}\left(\frac{x}{p}\right)^q\zeta^{qx}.$$

Or comme q est impair, on a

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

d'où

$$\tau^q = \sum_{x\in\mathbf{F}_p^*}\left(\frac{x}{p}\right)\zeta^{qx} = \left(\frac{q}{p}\right)\sum_{x\in\mathbf{F}_p^*}\left(\frac{qx}{p}\right)\zeta^{qx}.$$

L'application $x \longmapsto qx$ est une bijection de $\mathbf{F}_p^*$ sur $\mathbf{F}_p^*$, d'où

$$\tau^q = \left(\frac{q}{p}\right)\sum_{x\in\mathbf{F}_p^*}\left(\frac{x}{p}\right)\zeta^x = \left(\frac{q}{p}\right)\tau.$$

Or d'après (ii), $\tau \neq 0$, d'où on en tire que $\tau^{q-1} = \left(\frac{q}{p}\right)$.

□

Dans le cas où le corps K est $\mathbb{Q}$, une racine primitive p-ième de l'unité est donnée par $\zeta = e^{2i\pi/p}$. On peut alors donner une autre expression des sommes de Gauss qui nous sera utile dans les applications. Pour prouver ce lemme, nous aurons besoin de la formule suivante

$$\sum_{x\in\mathbf{F}_p} \exp\left(\frac{2i\pi xy}{p}\right) = \begin{cases} p & \text{si } y = 0 \bmod p \\ 0 & \text{sinon.} \end{cases} \tag{3.1}$$

dont la preuve (simple) est laissée en exercice.

Lemme 3.3.2 *On a*

$$\tau(a) = \sum_{y\in\mathbf{F}_p} \exp\left(\frac{2i\pi ay^2}{p}\right).$$

Preuve : On vérifie facilement que l'équation $y^2 = x$ admet $1 + \left(\frac{x}{p}\right)$ solutions. On en déduit, en utilisant (3.1) que

$$\begin{aligned} \tau(a) &= \sum_{x\in\mathbf{F}_p} \left(\frac{x}{p}\right) \exp\left(\frac{2i\pi ax}{p}\right) = \sum_{x\in\mathbf{F}_p} \left(1 + \left(\frac{x}{p}\right)\right) \exp\left(\frac{2i\pi ax}{p}\right) \\ &= \sum_{y\in\mathbf{F}_p} \exp\left(\frac{2i\pi ay^2}{p}\right). \end{aligned}$$

□

3.4 La loi de réciprocité quadratique

Le résultat fondamental suivant a été démontré par Gauss. Il existe de nombreuses preuves. Celle que nous utilisons est basée sur les "sommes de Gauss".

Théorème 3.4.1 (Loi de réciprocité quadratique) *Soient p et q des nombres premiers impairs distincts. On a*

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

Autrement dit, si $p \equiv 1 \pmod 4$ ou $q \equiv 1 \pmod 4$, alors $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$, sinon $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

Preuve : Soit ζ une racine primitive p-ième de l'unité sur $\mathbf{F}_q$ et soit $\tau = \tau(1)$ la somme de Gauss associée dans $\Sigma_p(\mathbf{F}_q)$. En utilisant le corollaire 3.2.2 et le théorème 3.3.1, on obtient les égalités suivantes dans $\Sigma_p(\mathbf{F}_q)$:

$$\begin{aligned} \left(\frac{p}{q}\right) &= p^{(q-1)/2} = \left(\left(\frac{-1}{p}\right)\tau^2\right)^{(q-1)/2} = (-1)^{(p-1)(q-1)/4}\tau^{q-1} \\ &= (-1)^{(p-1)(q-1)/4}\left(\frac{q}{p}\right), \end{aligned}$$

ce qui donne le résultat.

□

3.5 Le symbole de Jacobi

Sachant que le nombre 239 est premier, proposons nous de calculer le symbole de Legendre $\left(\frac{143}{239}\right)$. Pour appliquer la loi de réciprocité quadratique, il faudrait que le symbole de Legendre $\left(\frac{239}{143}\right)$ soit défini donc que 143 soit premier. Ce n'est pas le cas car $143 = 11 \times 13$. Le seul moyen d'avancer dans le calcul est d'utiliser cette factorisation, et la multiplicativité du symbole de Legendre. On écrit alors

$$\left(\frac{143}{239}\right) = \left(\frac{11}{239}\right)\left(\frac{13}{239}\right).$$

La loi de réciprocité s'applique maintenant car 11 et 13 sont premiers et cela conduit à

$$\left(\frac{143}{239}\right) = -\left(\frac{239}{11}\right)\left(\frac{239}{13}\right) = -\left(\frac{8}{11}\right)\left(\frac{5}{13}\right) = -\left(\frac{2}{11}\right)^3\left(\frac{13}{5}\right).$$

Or d'après le théorème 3.2.6, $\left(\frac{2}{11}\right) = -1$, d'où

$$\left(\frac{143}{239}\right) = \left(\frac{13}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

Le calcul est très simple ici car la factorisation de 143 est évidente. Dans le cas général, le calcul du symbole de Legendre $\left(\frac{a}{p}\right)$ lorsque a est non premier nous ramène au problème de la factorisation de a qui est un problème difficile. Le symbole de Jacobi supprime cette difficulté.

Définition 3.5.1 *Soit n un entier positif impair dont la décomposition en facteurs premiers est $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$. Le* **symbole de Jacobi** $\left(\frac{m}{n}\right)$ *est défini par*

$$\left(\frac{m}{n}\right) = \left(\frac{m}{p_1}\right)^{\alpha_1}\left(\frac{m}{p_2}\right)^{\alpha_2}\dots\left(\frac{m}{p_k}\right)^{\alpha_k}.$$

Théorème 3.5.2 *Soient m et n des entiers positifs impairs et $a, b, k \in \mathbb{Z}$. On a*

(a) $\left(\frac{a+kn}{n}\right) = \left(\frac{a}{n}\right)$.

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

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

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

(e) $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{(m-1)(n-1)}{4}}$.

Preuve : La preuve se déduit des propriétés analogues du symbole de Legendre et les détails sont laissés en exercice.

□

Il faut prendre garde au fait que le symbole de Jacobi ne caractérise pas les carrés modulo n (si a est premier avec n et est un carré modulo n alors $\left(\frac{a}{n}\right) = 1$ mais la réciproque est fausse si n est composé. Ceci montre que le symbole de Jacobi n'a pas de signification intéressante, contrairement au symbole de Legendre qui permet de distinguer les carrés. En revanche, c'est un outil de calcul indispensable. Reprenons l'exemple du calcul de $\left(\frac{143}{239}\right)$. On commence par appliquer la loi de réciprocité quadratique pour le symbole de Jacobi et on écrit

$$\begin{aligned}\left(\frac{143}{239}\right) &= -\left(\frac{239}{143}\right) = -\left(\frac{96}{143}\right) = -\left(\frac{2^5.3}{143}\right) \\ &= -\left(\frac{2}{143}\right)^5\left(\frac{3}{143}\right) = -\left(\frac{3}{143}\right) \\ &= \left(\frac{143}{3}\right) = \left(\frac{2}{3}\right) = -1.\end{aligned}$$

Il n'est plus nécessaire de factoriser les entiers, sauf pour sortir les facteurs 2 lorsque l'argument figurant au dénominateur est pair. On utilise essentiellement la loi de réciprocité et la périodicité. Le calcul du symbole de Jacobi $\left(\frac{a}{b}\right)$ est semblable au calcul du pgcd de a et b par l'algorithme d'Euclide. Le calcul d'un symbole de Legendre en utilisant les symboles de Jacobi ne nécessite que $O(\log b)$ divisions.

3.6 Nombre de solutions d'une équation quadratique

On rappelle que si $Q(x) = \sum_{1\leq i,j\leq n} a_{i,j}x_ix_j$ est une forme quadratique sur $\mathbf{F}_p^n$, on dit qu'elle est non dégénérée si $\det(Q) := \det(a_{i,j}) \neq 0$.

Théorème 3.6.1 *Soit Q une forme quadratique en n variables non dégénérée à coefficients dans $\mathbf{F}_p$ où p est un nombre premier impair. Alors*

$$card\{x \in \mathbf{F}_p^n : Q(x) = 0\} = p^{n-1} + \varepsilon(p-1)p^{\frac{n}{2}-1},$$

où

$$\varepsilon = \begin{cases} 0 & \text{si } n \text{ est impair} \\ \left(\frac{(-1)^{\frac{n}{2}}\det(Q)}{p}\right) & \text{si } n \text{ est pair.} \end{cases}$$

Preuve : Etape 1 : on se ramène au cas où Q est diagonale, c'est-à-dire de la forme

$$Q(x) = a_1x_1^2 + a_2x_2^2 + \ldots a_nx_n^2.$$

Ecrivons $Q(x) = {}^txAx$. Comme

$$Q(x) = \sum_{1\leq i,j\leq n} \frac{1}{2}(a_{i,j} + a_{j,i})x_ix_j,$$

on peut supposer que la matrice A est symétrique (quitte à changer A en $\frac{1}{2}(A + {}^tA)$). En utilisant un résultat classique sur les formes quadratiques symétriques non dégénérées, on sait qu'il existe une matrice de changement de base U et il existe $a_1, a_2, \ldots, a_n \in \mathbf{F}_p$ tels que si $x = Uy$, alors

$$Q(x) = Q^\sharp(y) = a_1 y_1^2 + \cdots + a_n y_n^2.$$

De plus, comme ${}^txAx = {}^ty{}^tUAUy$, la matrice $A^\sharp := {}^tUAU$ est la matrice associée à $Q^\sharp$. Il reste à remarquer alors que

$$\det(Q^\sharp) = \det(A^\sharp) = (\det(U))^2 \det(Q),$$

ce qui implique

$$\left(\frac{\det(Q^\sharp)}{p}\right) = \left(\frac{\det(Q)}{p}\right),$$

et achève de prouver l'étape 1.

Etape 2 : on prouve le résultat dans le cas où Q est diagonale.

Notons

$$N_p = \mathrm{card}\{x \in \mathbf{F}_p^n : Q(x) = 0\}.$$

et montrons que

$$pN_p = \sum_{a=0}^{p-1} \sum_{x \in \mathbf{F}_p^n} \exp\left(\frac{2i\pi a Q(x)}{p}\right). \tag{3.2}$$

On a, tout d'abord,

$$\sum_{a=0}^{p-1} \sum_{\substack{x \in \mathbf{F}_p^n \\ Q(x)=0}} \exp\left(\frac{2i\pi a Q(x)}{p}\right) = \sum_{a=0}^{p-1} N_p = pN_p.$$

D'autre part, en utilisant (3.1), on a

$$\sum_{a=0}^{p-1} \sum_{\substack{x \in \mathbf{F}_p^n \\ Q(x)\neq 0}} \exp\left(\frac{2i\pi a Q(x)}{p}\right) = \sum_{\substack{x \in \mathbf{F}_p^n \\ Q(x)\neq 0}} \sum_{a=0}^{p-1} \exp\left(\frac{2i\pi a Q(x)}{p}\right) = 0,$$

ce qui donne la formule (3.2). On écrit maintenant

$$\begin{aligned}
pN_p &= p^n + \sum_{a=1}^{p-1} \sum_{x \in \mathbf{F}_p^n} \exp\left(\frac{2i\pi a Q(x)}{p}\right) \\
&= p^n + \sum_{a=1}^{p-1} \sum_{x_1, x_2, \ldots, x_n \in \mathbf{F}_p} \exp\left(\frac{2i\pi a (a_1 x_1^2 + a_2 x_2^2 + \cdots + a_n x_n^2)}{p}\right) \\
&= p^n + \sum_{a=1}^{p-1} \prod_{j=1}^{n} \sum_{x_j \in \mathbf{F}_p} \exp\left(\frac{2i\pi a a_j x_j^2}{p}\right) \\
&= p^n + \sum_{a=1}^{p-1} \prod_{j=1}^{n} \tau(a a_j).
\end{aligned}$$

D'où en utilisant le théorème 3.3.1, on en déduit que

$$pN_p = p^n + \tau(1)^n \left(\frac{a_1 \dots a_n}{p}\right) \sum_{a=1}^{p-1} \left(\frac{a}{p}\right)^n.$$

Or $\det(Q) = a_1 \dots a_n$ et

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right)^n = \begin{cases} 0 & \text{si } n \text{ est impair} \\ p-1 & \text{si } n \text{ est pair.} \end{cases}$$

Donc si n est impair, on en déduit que $pN_p = p^n$, c'est-à-dire que $N_p = p^{n-1}$. Pour n pair, on obtient que

$$pN_p = p^n + \tau(1)^n \left(\frac{\det(Q)}{p}\right)(p-1),$$

et

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

D'où

$$N_p = p^{n-1} + (p-1)\left(\frac{(-1)^{\frac{n}{2}}\det(Q)}{p}\right) p^{\frac{n}{2}-1},$$

ce qui donne le résultat.

□

3.7 Exercices

Exercice 3.7.1 Soit p un nombre premier impair. Déterminer $\left(\frac{\frac{p+1}{2}}{p}\right)$ et $\left(\frac{\frac{p-1}{2}}{p}\right)$.

Exercice 3.7.2

1. Déterminer les p premiers pour lesquels l'équation $x^2 \equiv 3 \pmod{p}$ admet au moins une solution ?
2. Pour quels p premiers l'équation $x^2 \equiv 5 \pmod{p}$ a-t-elle des solutions ?

Exercice 3.7.3 131 et 263 sont premiers. Calculer $O_{263}(131)$ avec un minimum de calculs.

Exercice 3.7.4 Montrer que les diviseurs premiers de $4n^2 + 1$ sont de la forme $4k + 1$.

Exercice 3.7.5 Résoudre l'équation $x^2 + 3x + 7 \equiv 0 \pmod{115}$.

Exercice 3.7.6 (La méthode de Hensel) Soit p un nombre premier impair, $n \geq 1$ et $a \in \mathbb{Z}$ tel que $(a, p) = 1$.

(a) Montrer que $\bar{a} \in (\mathbb{Z}/p^n\mathbb{Z})^*$.

(b) On suppose que $x_1^2 \equiv a \pmod{p}$. Montrer que, pour tout entier $n \geq 1$, il existe un entier x_n, unique modulo p^n, qui vérifie

$$x_n \equiv x_1 \pmod{p}, \quad x_n^2 \equiv a \pmod{p^n}.$$

Indication : les x_n se construisent par récurrence, en cherchant x_{n+1} sous la forme

$$x_{n+1} = x_n + p^n u,$$

où u est un nombre entier à déterminer.

(c) En déduire que la congruence $x^2 \equiv a \pmod{p^n}$ admet des solutions si et seulement si $\left(\frac{a}{p}\right) = 1$, et dans ce cas, elle admet exactement deux solutions modulo p^n.

(d) **Application :** résoudre $x^2 + x + 3 \equiv 0 \pmod{125}$.

Exercice 3.7.7 (Résolution de $x^2 \equiv a \pmod{2^n}$ (a impair))

1. Soit $n \geq 3$, a un entier impair. Démontrer que si la congruence $x^2 \equiv a \pmod{2^n}$ a des solutions, alors $a \equiv 1 \pmod{8}$.
2. On suppose $a \equiv 1 \pmod{8}$. Démontrer que $x^2 \equiv a \pmod{8}$ admet exactement 4 solutions modulo 8.
3. Supposons que $a \equiv 1 \pmod{8}$ et supposons qu'il existe un entier x tel que $x^2 \equiv a \pmod{2^n}$.
   (a) Montrer que a est un carré modulo 2^{n+1}.
   Indication : on pourra calculer pour $y \in \mathbb{N}$, $(x + y2^{n-1})^2$.
   (b) En déduire que a possède au moins 4 racines carrés modulo 2^{n+1}.
4. Conclure par récurrence que, pour tout $n \geq 3$, si $a \equiv 1 \pmod{8}$, alors a possède exactement 4 racines carrées modulo 2^n.
   Indication : on pourra considérer $C_n = \{x \in (\mathbb{Z}/2^n\mathbb{Z})^* : x \equiv 1 \pmod{8}\}$ et

$$\begin{array}{rccc} \varphi : & (\mathbb{Z}/2^n\mathbb{Z})^* & \longrightarrow & C_n \\ & x & \longmapsto & x^2. \end{array}$$

Exercice 3.7.8 On s'intéresse à l'équation $x^2 + x + 1 \equiv 0 \pmod{n}$.

1. Soit $S(n)$ la fonction arithmétique qui associe à l'entier $n \geq 1$ le nombre de solutions modulo n de l'équation $x^2 + x + 1 \equiv 0 \pmod{n}$. Démontrer que la fonction S est une *fonction arithmétique multiplicative* c'est à dire que $S(mn) = S(m)S(n)$ chaque fois que m et n sont premiers entre eux.

2. Pour quels p premiers l'équation $x^2+x+1=0 \pmod p$ a-t-elle des solutions, c'est à dire tels que $S(p)>0$.
3. Pour chacun de ces nombres premiers, discuter selon la valeur de $\alpha \geq 1$ la valeur de $S(p^\alpha)$.
4. Quels sont les entiers n pour lesquels $x^2+x+1 \equiv 0 \pmod n$ a des solutions ?
5. Quel est le nombre de solutions de

$$x^2+x+1 \equiv 0 \pmod{2457}.$$

Exercice 3.7.9 1. Pour quels p premiers l'équation $x^2+6x+1=0 \pmod p$ a-t-elle des solutions ?
2. Pour chacun de ces nombres premiers, discuter selon la valeur de $\alpha \geq 1$ le nombre de solutions de

$$x^2+6x+1 \equiv 0 \pmod{p^\alpha}$$

3. Quels sont les entiers n pour lesquels $x^2+6x+1 \equiv 0 \pmod n$ a des solutions ?

Exercice 3.7.10 On appelle $n^{\text{ième}}$ nombre de Fermat le nombre $2^{2^n}+1$.

1. Montrer que si un nombre premier est de la forme 2^k+1 alors c'est un nombre de Fermat.
2. Soit $F_n = 2^{2^n}+1$ un nombre de Fermat. Montrer que les diviseurs premiers de F_n sont tous de la forme $k2^{n+1}+1$ (si p est un diviseur premier de F_n, on considèrera l'ordre de 2 modulo p et on montrera qu'il est exactement 2^{n+1}).
3. En considérant le caractère quadratique de 2 modulo p montrer qu'on a un peu mieux : les diviseurs premiers de F_n sont tous de la forme $k2^{n+2}+1$.
4. En marchant sur les traces d'Euler, en déduire que $F_5 = 2^{32}+1 = 4294967297$ n'est pas premier.

Exercice 3.7.11 Soit $p = F_n = 2^{2^n}+1$, avec $n \geq 1$.

1. On suppose que p est premier.
   (a) Montrer que g est un générateur $(\mathbb{Z}/p\mathbb{Z})^*$ si et seulement si $\left(\frac{g}{p}\right) = -1$.
   (b) Montrer que 3 est un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$.
2. Ici on ne suppose pas p premier, mais seulement que

$$3^{\frac{p-1}{2}} \equiv -1 \pmod p.$$

Montrer que p est premier. Ce test de primalité pour les nombres de Fermat est le test de Pepin.

Exercice 3.7.12 (Calcul d'une racine carrée modulo p) On donne dans cet exercice un algorithme efficace de calcul des racines carrées de a dans $\mathbb{Z}/p\mathbb{Z}$ lorsque p est premier impair.

1. Dans la cas ou $p \equiv 3 \pmod 4$ cet algorithme est particulièrement simple. Soit a un carré modulo p. Démontrer que $a^{\frac{p+1}{4}}$ est un racine carrée de a.
2. A partir de maintenant p est un nombre premier impair quelconque. Expliquer comment, en pratique, on peut trouver rapidement un entier b qui ne soit pas un carré modulo p. On choisit un tel entier. On considère alors l'ensemble E des couples (e_1, e_2) satisfaisant

$$a^{e_1} b^{e_2} \equiv 1 \bmod p. \tag{3.3}$$

3. Montrer que $\left(\frac{p-1}{2}, 0\right) \in E$
4. Montrer que si $(e_1, e_2) \in E$ alors e_2 est pair.
5. Montrer que si $(e_1, e_2) \in E$ et si e_1 est impair alors

$$x = a^{\frac{e_1+1}{2}} b^{\frac{e_2}{2}}$$

est une racine carrée de a modulo p.

6. Soit $(e_1, e_2) \in E$ avec e_1 pair. Soit $u = a^{\frac{e_1}{2}} b^{\frac{e_2}{2}}$. Que pouvez vous dire de u^2 ? En déduire un couple $(e_1', e_2') \in E$ avec $e_1' = e_1/2$.
7. En déduire un algorithme de calcul d'une racine carrée de a modulo p. Analyser la complexité de cet algorithme dans le pire des cas, c'est-à-dire le nombre maximum d'opérations à effectuer pour obtenir ainsi une racine carrée de a. Que se passe-t-il lorsque p est de la forme $p = 4k + 3$?.