

Rapport ENS

Yasser ALGHOUASS

Juin 2022

1 Introduction

On s'intéresse à l'ensemble des carrés dans le corps $\mathbb{F}_p$ p premier. On introduit le symbole de Legendre qui permet de caractériser les carrés et on développe les principales propriétés de ce symbole. On introduit aussi les sommes de Gauss pour obtenir le nombre de solutions d'une équation quadratique.

2 Résidus quadratiques modulo p .

Définition 2.1. Étant donné un nombre premier impair p , on dit qu'un entier a non divisible par p est un **résidu quadratique** modulo p s'il existe $x \in \mathbb{Z}$ tel que $x^2 \equiv a \pmod{p}$. Dans le cas contraire, on dit que a est 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 $(\mathbb{Z}/p\mathbb{Z})^*$.

Puisqu'on travaille modulo p et qu'on exclut les nombres divisibles par p , on étudie en fait essentiellement les nombres entre 1 et $p-1$. Cela ne dépend que de la classe de a modulo p . On ne distinguera plus dans la suite deux nombres égaux modulo p .

Exemple 2.1. Commençons par un exemple simple. La table des carrés dans $\mathbb{Z}/p\mathbb{Z}$ avec $p = 7$.

$x \bmod p$	0	1	2	3	4	5	6
$x^2 \bmod p$	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 2.1. 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 carrées.

En d'autres termes le théorème précédent affirme qu'étant donné un nombre premier impair p , il existe exactement $\frac{p-1}{2}$ résidus quadratiques et $\frac{p-1}{2}$ non-résidus quadratiques modulo p .

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

Théorème 2.2. Soit p un nombre premier impair et a un entier tel que p ne divise pas a . Alors

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

3 Le symbole de Legendre

Définition 3.1. Soient p un nombre premier impair et $a \in \mathbb{Z}$. On définit le **symbole de Legendre** par

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

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 3.1. Soient p un nombre premier impair et a un entier. On a

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

Théorème 3.1. Soient p un nombre premier impair, $a \in \mathbb{Z}$ et $m \in \mathbb{Z}$. On a

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

Le théorème précédent 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. Soient $a, b \in \mathbb{Z}$ et p un nombre premier impair. On a

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

Le théorème précédent implique qu 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 nombres 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 3.3. Soit p un nombre premier impair. Alors

$$\left(\frac{-1}{p}\right) = \begin{cases} +1 & \text{si } p \equiv 1 \pmod{4} \\ -1 & \text{si } p \equiv 3 \pmod{4} \end{cases}$$

De façon équivalente, on a

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

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

Théorème 3.4. Soit p un entier premier impair. On a

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

Lemme 3.1. On a

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

4 Les sommes de Gauss

Définition 4.1. 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 de K . Pour $x \in \mathbb{Z}$, l'élément ζ^x ne dépend que de $x \bmod p$ et donc il garde un sens pour $x \in \mathbb{F}_p$, on pose

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

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

Theorème 4.1. Soient K un corps de caractéristique q , soit p un nombre premier impair, $p \neq q$. Alors, on a les propriétés suivantes :

1. pour tout $a \in \mathbb{F}_p^*$,

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

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

3. si q est un nombre premier impair, pour tout $a \in \mathbb{F}_p^*$, on a

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

Dans le cas où le corps K est $\mathbb{Q}$, une racine primitive p -ième de l'unité est donnée par $\zeta = \frac{2i\pi}{p}$. On peut 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

$$\sum_{x \in \mathbb{F}_p} \exp\left(\frac{2i\pi xy}{p}\right) = \begin{cases} p & \text{si } y \equiv 0 \pmod{p} \\ -1 & \text{sinon} \end{cases} \quad (4.1)$$

Lemme 4.1. On a

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

5 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.

Theorème 5.1. 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 $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$

6 Nombre de solutions d'une équation quadratique

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

Theorème 6.1. Soit Q une forme quadratique en n variables non dégénérée à coefficients dans $\mathbb{F}_p$ où p est un nombre premier impair. Alors

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

où

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

7 Bibliographie

1. Problems in algebraic number theory, M.Ram Murty
2. Gauss and Jacobi sums, Bruce C.Berndt
3. Cours d'algèbre, Daniel Perrin
4. A classical introduction to modern number theory, Kenneth Ireland et Michael Rosen

8 Annexes

8.1 Preuve du théorème 2.1 :

Définition 8.1. Soit p un nombre premier et g un générateur du groupe $(\mathbb{Z}/p\mathbb{Z})^*$. Si $a \in (\mathbb{Z}/p\mathbb{Z})^*$, le **logarithme discret** de a en base g , noté $\log_g a$, est l'unique entier α tel que

$$0 \leq \alpha \leq p-2, a = g^\alpha$$

Lemme 8.1. Soient p un nombre premier, g un générateur du groupe $(\mathbb{Z}/p\mathbb{Z})^*$, $a \in (\mathbb{Z}/p\mathbb{Z})^*$ et n un entier tel que $a = g^n$. Alors, le logarithme discret de a en base g est le reste de la division euclidienne de n par $p-1$.

Preuve 1. Effectuons le reste de la division euclidienne de n par $p-1$. Alors il existe deux entiers q et r tels que

$$n = q(p-1) + r, 0 \leq r \leq p-2$$

On a alors $a = g^n = g^{q(p-1)+r} = g^{q(p-1)}g^r = g^r$ car $g^{p-1} = 1$. Par définition, on en déduit que $\log_g a = r$.

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

$$a = (g^l)^2$$

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 précédent, 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 qu'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 $\frac{p-1}{2}$ 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 $\mathbb{F}_p[X]$ étant de degré 2, il n'admet pas d'autres racines.

8.2 Preuve du théorème 2.2 :

Lemme 8.2. Soit p un nombre premier et d un entier naturel tel que $d|p-1$. Alors l'équation

$$x^d \equiv 1 \pmod{p}$$

a exactement d solutions modulo p .

Preuve 3. Ecrivons $p-1 = dk, k \in \mathbb{N}$. D'après le théorème de Fermat, l'équation

$$x^{p-1} \equiv 1 \pmod{p}$$

a exactement $p-1$ solutions modulo p . D'autre part,

$$x^{p-1} - 1 = x^{dk} - 1 = (x^d - 1)(x^{(k-1)d} + x^{(k-2)d} + \dots + 1)$$

D'où

$$x^{p-1} \equiv 1 \pmod{p} \iff x^d \equiv 1 \pmod{p} \text{ ou } x^{(k-1)d} + x^{(k-2)d} + \dots + 1 \equiv 0 \pmod{p}.$$

D'après le théorème de Lagrange, l'équation

$$x^{(k-1)d} + x^{(k-2)d} + \dots + 1 \equiv 0 \pmod{p}$$

a au plus $(k-1)d$ solutions modulo p et l'équation

$$x^d \equiv 1 \pmod{p}$$

a au plus d solutions modulo p . Comme au total, il y a $p - 1 = (k - 1)d + d$ solutions, on en déduit le résultat.

Preuve 4. D'après le théorème de Fermat, on a

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

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

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

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

$$a^{\frac{p-1}{2}} = b^{p-1} \equiv 1 \pmod{p}.$$

D'après le lemme précédent, l'équation

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

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

8.3 Preuve du théorème 3.1 :

Preuve 5. 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

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

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

8.4 Preuve du théorème 3.2 :

Preuve 6. En utilisant le critère d'Euler, on a

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

ce qui donne le résultat.

8.5 Preuve du théorème 3.3 :

Preuve 7. Observons que

$$(-1)^{\frac{p-1}{2}} = \begin{cases} +1 & \text{si } p \equiv 1 \pmod{4} \\ -1 & \text{si } p \equiv 3 \pmod{4} \end{cases}$$

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

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

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

8.6 Preuve du théorème 3.4 :

Preuve 8. Considérons le produit $A = \prod_{k=1}^{\frac{p-1}{2}} 2k = 2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!$

Raisonnons modulo p de sorte que $A \equiv \left(\frac{p-1}{2}\right)! \left(\frac{2}{p}\right) \pmod{p}$

On observe une certaine symétrie du produit car, modulo p , on a

$-(2k - p) \equiv -2k \pmod{p}$ et le terme $p - 2k$ est un entier positif impair qu'on réécrit $p - 2k = 2l - 1$.

1. Cas où $p \equiv 1 \pmod{4}$

Pour k parcourant $\llbracket \frac{p+3}{4}, \frac{p-1}{2} \rrbracket$, les l correspondants parcourent $\llbracket 1, \frac{p-1}{4} \rrbracket$. On a alors

$$\begin{aligned} A &= \left(\prod_{k=1}^{\frac{p-1}{4}} 2k\right) \left(\prod_{k=\frac{p+3}{4}}^{\frac{p-1}{2}} 2k\right) \\ &\equiv \left(\prod_{k=1}^{\frac{p-1}{4}} 2k\right) \left(\prod_{l=1}^{\frac{p-1}{4}} p - (2l - 1)\right) \pmod{p} \\ &\equiv (-1)^{\frac{p-1}{4}} \left(\prod_{k=1}^{\frac{p-1}{4}} 2k\right) \left(\prod_{l=1}^{\frac{p-1}{4}} (2l + 1)\right) \pmod{p} \\ &\equiv (-1)^{\frac{p-1}{4}} \left(\frac{p-1}{2}\right)! \pmod{p} \end{aligned}$$

Comme $\left(\frac{p-1}{2}\right)!$ est inversible modulo p , on en déduit dans ce cas que $\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{4}}$. Ainsi, par le critère d'Euler, on en déduit que 2 est carré modulo p si et seulement si $p \equiv 1 \pmod{8}$.

2. Cas où $p \equiv 3 \pmod{4}$

Pour k parcourant $\llbracket \frac{p+1}{4}, \frac{p-1}{2} \rrbracket$, les l correspondants parcourent $\llbracket 1, \frac{p+1}{4} \rrbracket$. On a alors

$$\begin{aligned} A &= \left(\prod_{k=1}^{\frac{p-3}{4}} 2k\right) \left(\prod_{k=\frac{p+1}{4}}^{\frac{p-1}{2}} 2k\right) \\ &\equiv \left(\prod_{k=1}^{\frac{p-3}{4}} 2k\right) \left(\prod_{l=1}^{\frac{p+1}{4}} p - (2l - 1)\right) \pmod{p} \\ &\equiv (-1)^{\frac{p+1}{4}} \left(\prod_{k=1}^{\frac{p-3}{4}} 2k\right) \left(\prod_{l=1}^{\frac{p+1}{4}} (2l + 1)\right) \pmod{p} \\ &\equiv (-1)^{\frac{p+1}{4}} \left(\frac{p-1}{2}\right)! \pmod{p} \end{aligned}$$

Comme $\left(\frac{p-1}{2}\right)!$ est inversible modulo p , on en déduit dans ce cas que $\left(\frac{2}{p}\right) = (-1)^{\frac{p+1}{4}}$. Ainsi, par le critère d'Euler, on en déduit que 2 est carré modulo p si et seulement si $p \equiv -1 \pmod{8}$.

8.7 Preuve du lemme 3.1 :

Preuve 9. Il suffit de se rappeler qu'il y a autant de carrés que de non-carrés dans $\mathbb{F}_p^*$.

8.8 Preuve du théorème 4.1 :

Preuve 10. 1. l'application $x \mapsto ax$ est une bijection de $\mathbb{F}_p^*$ sur $\mathbb{F}_p^*$. On a donc

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

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

2. pour simplifier, nous noterons $\tau = \tau(1)$. En utilisant le théorème 3.2, on a

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

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

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

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

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

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

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

Ainsi

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

Il reste à appliquer le lemme 3.1 pour conclure la preuve du (2).

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

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

Or comme q est impair, on a

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

d'où

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

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

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

Or d'après (2), $\tau \neq 0$, d'où on en tire $\tau^{q-1} = \left(\frac{q}{p}\right)$.

8.9 Preuve du lemme 4.1

Preuve 11. On vérifie facilement que l'équation $y^2 = x$ admet $1 + \left(\frac{x}{p}\right)$ solutions. On en déduit, en utilisant la formule (4.1) que

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

8.10 Preuve du théorème 5.1 :

Preuve 12. Soit ζ une racine primitive p -ième de l'unité sur $\mathbb{F}_p$ et soit $\tau = \tau(1)$ la somme de Gauss associée dans $\sum_p(\mathbb{F}_p)$. En utilisant le corollaire 3.1 et le théorème 4.1, on obtient les égalités suivantes dans $\sum_p(\mathbb{F}_p)$:

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

ce qui donne le résultat.

8.11 Preuve du théorème 6.1 :

Preuve 13. Etape 1 : On se ramène au cas où Q est diagonale, c'est-à-dire de la forme

$$Q(x) = a_1 x_1^2 + a_2 x_2^2 + \dots + a_n x_n^2$$

Ecrivons $Q(x) = {}^t x A x$ Comme

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

On peut supposer que la matrice A est symétrique (quitte à changer A en $\frac{1}{2}(A + {}^t A)$). 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 $a_1, a_2, \dots, a_n \in F_p$ tels que si $x = Uy$, alors

$$Q(x) = Q^\#(y) = a_1 y_1^2 + \dots + a_n y_n^2$$

De plus, comme ${}^t x A x = {}^t y {}^t U A U y$, la matrice $A^\# = {}^t U A U$ est la matrice associée à $Q^\#$. Il reste à remarquer alors que:

$$\deg(Q^\#) = \det(A^t) = \det(U)^2 \det(Q)$$

ce qui implique:

$$\frac{\deg(Q^\#)}{P} = \frac{\deg(Q)}{P}$$

et on achève de prouver l'étape 1. Etape 2: on prouve le résultat dans le cas où Q est diagonale. Notons:

$$N_p = \text{card}\{x \in F_p^n : Q(x) = 0\}$$

et montrons que

$$pN_p = \sum_{a=0}^{p-1} \sum_{x \in F_p^n} \exp\left(\frac{2i\pi a Q(x)}{p}\right)$$

On a tout d'abord,

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

D'autre part en utilisant (3.1) on a

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

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

$$\begin{aligned} pN_p &= p^n + \sum_{a=0}^{p-1} \sum_{x \in F_p^n, Q(x) \neq 0} \exp\left(\frac{2i\pi a Q(x)}{p}\right) \\ &= p^n + \sum_{a=0}^{p-1} \sum_{x_1, x_2, \dots, x_n \in F_p} \exp\left(\frac{2i\pi a (a_1 x_1^2 + a_2 x_2^2 + \dots + a_n x_n^2)}{p}\right) \\ &= p^n + \sum_{a=0}^{p-1} \prod_{j=1}^n \sum_{x_j \in F_p} \exp\left(\frac{2i\pi a a_j x_j^2}{p}\right) \\ &= p^n + \sum_{a=0}^{p-1} \prod_{j=1}^n \tau(a a_j) \end{aligned}$$

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

$$pN_p = p^n + \tau(1)^n \left(\frac{a_1 a_2 \dots a_n}{p}\right) \sum_{a=0}^{p-1} \left(\frac{a}{p}\right)^n$$

Or $\det(Q) = a_1 a_2 \dots a_n$ et

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

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

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

et

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

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.