Loi de réciprocité quadratique

Notation : $\mathbb{F}_p^{\times 2} = \{x \in \mathbb{F}_p^\times, \exists y \in \mathbb{F}_p, x = y^2\}$ désigne les carrés de $\mathbb{F}_p$.

Définition 1. *Soit p premier impair et $a \in \mathbb{F}_p$. On définit le symbole de Legendre de a par rapport à p par*

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & si\ a \in \mathbb{F}_p^{\times 2} \\ 0 & si\ a = 0 \\ -1 & si\ a \notin \mathbb{F}_p^{\times 2} \end{cases}$$

Lemme 2. *Soit p premier impair et $a \in \mathbb{F}_p^\times$. Alors*

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

Preuve. La démonstration se base sur le théorème de Fermat.

- Si $a \in \mathbb{F}_p^{\times 2}$,
  Alors il existe un $x \in \mathbb{F}_p^\times$ tel que $a = x^2$. Alors par le petit théorème de Fermat, $a^{\frac{p-1}{2}} = x^{p-1} = 1$ car $x \in \mathbb{F}_p^\times$.
- Réciproquement, si $a^{\frac{p-1}{2}} = -1$,
  Alors a ne peut pas être un carré : si on avait un $x \in \mathbb{F}_p^\times$ tel que $a = x^2$ alors on aurait $x^{p-1} = -1$ ce qui est impossible d'après le théorème de Fermat.

On en déduit le théorème par définition du symbole de Legendre. □

Théorème 3 (Loi de réciprocité quadratique)**.** *Soient p et q deux nombres premiers impairs distincts. Alors*

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

Preuve. L'idée est de calculer le cardinal de la "sphère" de $\mathbb{F}_q$, $\{(x_1, \ldots, x_p) \in (\mathbb{F}_q)^p, \sum_{i=1}^{p} x_i^2 = 1\}$

Etape 1 : On calcule le cardinal à l'aide du lemme suivant :

Lemme 4. $\forall a \in \mathbb{F}_p^\times$, $Card\left(\{x \in \mathbb{F}_p, ax^2 = 1\}\right) = 1 + \left(\frac{a}{p}\right)$.

Preuve du lemme. On distingue les cas suivant la valeur de $\left(\frac{a}{p}\right)$, c'est à dire si a est un carré modulo p ou non. On remarque que chercher les x vérifiant $ax^2 = 1$ revient à chercher les racines du polynôme $X^2 - a$. Ce polynôme a au plus deux racines, et :

- Si $a \in \mathbb{F}_p^{\times 2}$,
  Alors il existe un $y \in \mathbb{F}_p^\times$ tel que $a = y^2$. On a alors deux racines pour $(X^2 - a)$ que sont y et $-y$. On a bien sûr $y \neq y$ car sinon $y = 0$ ce qui est exclu car $a \in \mathbb{F}_p \setminus \{0\}$.
- Réciproquement, si $a \notin \mathbb{F}_p^{\times 2}$,
  Alors $X^2 - a$ est irréductible comme polynôme de degré deux sans racine (les racines sont les y tels que $y^2 = a$, soit $\emptyset$ ici).

Ainsi, en regroupant les deux résultats on a bien $Card\left(\{x \in \mathbb{F}_p, ax^2 = 1\}\right) = 1 + \left(\frac{p}{q}\right)$. □

L'idée est maintenant de faire agir le groupe additif $(\mathbb{F}_p, +)$ sur l'ensemble $A := \{(x_1, \dots, x_p) \in (\mathbb{F}_q)^p, \sum_{i=1}^{p} x_i^2 = 1\}$, donnée par l'action de ce groupe sur $(\mathbb{F}_q)^p$ définie par $n \cdot (x_1, \dots, x_p) := (x_{n+1}, \dots, x_{n+p})$ où les indices sont vus modulo p. Intéressons-nous aux orbites et au stabilisateurs pour cette action. On remarque déjà que les stabilisateurs étant des sous-groupes de $\mathbb{F}_p$, le théorème de Lagrange assurequ'ils sont ou bien $\{0\}$ ou bien $\mathbb{F}_p$ tout entier.

- Si $(x_1, \dots, x_p)$ a un stabilisateur non trivial, alors cela signifie par définition que $\forall n \in \mathbb{F}_p$, $(x_1, \dots, x_p) = (x_{n+1}, \dots, x_{n+p})$ et donc que $\forall i \in [\![1, p]\!]$, $x_i = x_1$.
- Si $(x_1, \dots, x_p)$ a un stabilisateur trivial, on trouve au contraire que tous les x_i sont nécessairement différents. [1]

Ainsi, pour le premier cas il y a autant d'orbites différentes pour l'action que d'éléments $x \in \mathbb{F}_p$ vérifiant $\sum_{i=1}^{p} x^2 = px^2 = 1$, soit $1 + \left(\frac{p}{q}\right)$ possibilités d'après le lemme. Par la relation orbite-stabilisateur, pour le second cas on a

$$Card(Orb((x_1, \dots, x_p))) = Card(\mathbb{F}_p)/Card(Stab((x_1, \dots, x_p)) = Card(\mathbb{F}_p)/1 = Card(\mathbb{F}_p)$$

et en particulier l'orbite a un cardinal nul lorsque l'on réduit modulo p.

1. Mais cela importe peu dans la suite.

Ainsi, en regroupant les résultats précédents, on obtient par équation aux classes

$$Card(A) \equiv \sum_{\text{Orbites triviales}} Card(\{1\}) + 0[p] \equiv 1 + \left(\frac{p}{q}\right)[p].$$

Etape 2 : On va maintenant considérer le cardinal précédent à l'aide des formes quadratiques.
On remarque en effet que $Card(A) = \{(x_1, \ldots, x_p), f((x_1, \ldots, x_p)) = 1\}$ où f désigne la forme quadratique $(x_1, \ldots, x_p) \mapsto \sum_{i=1}^{p} x_i^2$ définie sur $(\mathbb{F}_q)^p$. La matrice de f dans la base canonique du $\mathbb{F}_q$-espace vectoriel $(\mathbb{F}_q)^p$ est I_q. On va maintenant montrer

$$Card(A) = \{(x_1, \ldots, x_p), g((x_1, \ldots, x_p)) = 1\} \tag{0.1}$$

avec g une autre forme quadratique bien choisie afin de simplifier le dénombrement de A. On considère donc l'unique forme quadratique g dont la matrice dans la base canonique de $(\mathbb{F}_q)^p$ est

$$M := \begin{pmatrix} J & & & \\ & \ddots & & \\ & & J & \\ & & & a \end{pmatrix} \in \mathcal{M}_p(\mathbb{F}_q)$$

où $J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ et où on a posé $d = \dfrac{p-1}{2}$ et $a = (-1)^d$. Pour montrer que f et g sont équivalentes, d'après la classification des formes quadratiques sur $\mathbb{F}_p$ il suffit de montrer que leurs matrices associées ont même déterminant et même rang. Le dernier point est vérifié car les deux formes quadratiques sont ici non dégénérées, ou de manière équivalente, I_q et M sont toutes deux de rang p. Le premier point est assuré par le calcul du déterminant de M :

$$\det(M) = (det(J))^d \times a = (-1)^{2d} = 1 = det(I_q).$$

Ainsi, on a bien (0.1), c'est à dire plus précisément $Car(A) = \{(x_1, \ldots, x_d), (y_1, \ldots, y_d), t \in (\mathbb{F}_q)^p, \sum_{i=1}^{d} 2x_i y_i + at^2 = 1\}$. Pour calculer ce cardinal, on peut distinguer deux types de points :

- Les points tels que tous les y_i sont nuls, qui sont au nombre de $Card(\{(x,t) \in \mathbb{F}_q^d \times \mathbb{F}_q, at^2 = 1\}) =$

$\left(1+\left(\frac{a}{q}\right)\right)q^d$.

- Les points pour lequel au moins y_i n'est pas nul. Pour compter ce nombre de points, on peut fixer un tel y_i, puis choisir d'une part les $d-1$ valeurs y_i restantes ($q \times q^{d-1}$ choix) et d'autre par les x_i restants, choisis dans un hyperplan (affine) de $\mathbb{F}_q^d$ (soit $q^d - 1$ choix).

Ainsi, en regroupant ces deux résultats (c'est à dire en effectuant la somme), on obtient

$$Card(A) = \left(1+\left(\frac{a}{q}\right)\right)q^d + q^d \times (q^d - 1) = q^d\left(\left(\frac{a}{q}\right) + q^d\right)$$

Or on remarque que $q^d = \left(\frac{q}{p}\right)$ et que $\left(\frac{a}{q}\right) = \left(\frac{(-1)^d}{q}\right) = \left(\frac{-1}{q}\right)^d = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. Ainsi, en reprenant l'expression obtenue à l'étape 1, il vient

$$1+\left(\frac{p}{q}\right) \equiv \left(\frac{q}{p}\right) \times \left((-1)^{\frac{p-1}{2}\frac{q-1}{2}} + \left(\frac{q}{p}\right)\right)[p]$$

Puisque les symboles de Legendre sont égaux à 1 ou -1 ici, leur carré vaut 1, donc en particulier en multipliant cette équation par $\left(\frac{q}{p}\right)$ on obtient

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

c'est à dire encore

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

Finalement, on a bien le résultat souhaité (les éléments ici valent 1 ou -1 donc l'galité est bien une égalité sur $\mathbb{Z}$). □