Loi de réciprocité quadratique

Caldero
Histoires Reconstruites 1

Recasages: 120, 121, 170

Définition: Pour p un nombre premier impair et $a \in \mathbb{F}_p$, on définit le symbole de Legendre de a par:

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} = \begin{cases} 1 \text{ si } a \text{ est un carré dans } \mathbb{F}_p^* \\ -1 \text{ si } a \text{ n'est pas un carré dans } \mathbb{F}_p^* \\ 0 \text{ si } a = 0 \end{cases}$$

Lemme: Soit p premier impair et $a \in \mathbb{F}_p^*$. On a:

$$\#\{x \in \mathbb{F}_p \mid ax^2 = 1\} = 1 + \left(\frac{a}{p}\right).$$

Preuve: a est un carré dans $\mathbb{F}_q$ si et seulement si a^{-1} en est un donc: (a est un carré dans $\mathbb{F}_q$) $\Leftrightarrow$ ($aX^2 - 1 \in \mathbb{F}_q[X]$ possède deux racines distinctes dans $\mathbb{F}_q$).
Le cardinal considéré vaut donc 0 si a n'est pas un carré dans $\mathbb{F}_q$, et 2 si a est un carré dans $\mathbb{F}_q$, d'où le résultat.

Théorème: Soient p et q deux nombres premiers impairs distincts. Alors:

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

Preuve: L'idée est de calculer de deux manières différentes le cardinal de l'ensemble:

$$X = \left\{(x_1, \dots, x_p) \in \mathbb{F}_q^p \mid \sum_{i=1}^{p} x_i^2 = 1\right\} \quad \text{On pose } f : x \in \mathbb{F}_q^p \mapsto \sum_{i=1}^{p} x_i^2.$$

- On fait agir $\mathbb{Z}/p\mathbb{Z}$ sur X par: $k \cdot (x_1, \dots, x_p) = (x_{k+1}, \dots, x_{k+p})$ où les indices sont vus modulo p: $x_{k+p} = x_k$ pour tout k. Il y a deux sortes d'orbite:
  - celles dont le stabilisateur est $\mathbb{Z}/p\mathbb{Z}$, elles sont de la forme $\{(x, \dots, x)\}$ où $x \in \mathbb{F}_q$ vérifie $f(x, \dots, x) = 1$ c'est-à-dire $px^2 = 1$
  - les autres, dont le stabilisateur est trivial (sous-groupe de $\mathbb{Z}/p\mathbb{Z}$)

L'équation aux classes donne:

$$\#X = \sum_{x, px^2 = 1} \frac{\#\mathbb{Z}/p\mathbb{Z}}{\#\mathbb{Z}/p\mathbb{Z}} + \sum_{\text{autres orbites}} \frac{\#\mathbb{Z}/p\mathbb{Z}}{\#\{1\}} = 1 + \left(\frac{p}{q}\right) \bmod p \text{ (lemme)}$$

* $\exists P \in GL_n(\mathbb{F}_q)$, $M = {}^tP I_q P$. $u \mapsto P^t u$ est bijective donc :

$\#X = \#\{u \in \mathbb{F}_q^p \mid {}^t u M u = 1\} = \#\{u' \in \mathbb{F}_q^p \mid {}^t u' I_q u' = 1\}$

$= \#\tilde{X}$

• D'autre part, f est la forme quadratique dont la matrice dans la base canonique de $\mathbb{F}_q^p$ est I_p. On pose :

$$d = \frac{p-1}{2}, \quad a = (-1)^d, \quad J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathcal{M}_2(\mathbb{F}_q)$$

On considère la forme quadratique dont la matrice dans la base canonique de $\mathbb{F}_q^p$ est :

$$M = \begin{pmatrix} J & & (0) \\ & \ddots & \\ (0) & & J \\ & & & a \end{pmatrix} \in \mathcal{M}_p(\mathbb{F}_q)$$

On a $\mathrm{rg}(M) = p$ et $\det(M) = \det(J)^d a = (-1)^d (-1)^d = 1 = \det(I_p)$.

D'après la classification des formes quadratiques sur les corps finis, M et I_p ayant même rang et même déterminant (donc même discriminant), M et I_p sont congruentes. Ainsi, $\#X = \#\tilde{X}$ où $\tilde{X} = \{x \in \mathbb{F}_q^p \mid \tilde{f}(x) = 1\}$ où $\tilde{f}$ est la forme quadratique dont la matrice dans la base canonique de $\mathbb{F}_q^p$ est M. Autrement dit,

$$X' = \left\{(y_1, z_1, \dots, y_d, z_d, t) \in \mathbb{F}_q^p, \ 2\sum_{i=1}^{d} y_i z_i + at^2 = 1\right\}$$

Soit $(y_1, z_1, \dots, y_d, z_d, t) \in X'$.

- Si $y_1 = \dots = y_d = 0$, alors le choix des z_i est quelconque, et t doit vérifier $at^2 = 1$. Il y a donc q^d choix des z_i et $1 + \left(\frac{a}{q}\right)$ choix de t. Il y a donc $q^d\left[1 + \left(\frac{a}{q}\right)\right]$ éléments de cette forme.

- S'il existe y_i non nul, $(y_1, \dots, y_d)$ est non nul dans $\mathbb{F}_q^d$ pour lequel il y a $q^d - 1$ choix. Le choix de t est quelconque, et alors les z_i vivent dans un hyperplan affine de $\mathbb{F}_q^d$, il y a donc q^{d-1} choix pour eux. Il y a au total $(q^d - 1) q q^{d-1} = q^d(q^d - 1)$ éléments de cette forme.

Ainsi, $\#X' = q^d\left[1 + \left(\frac{a}{q}\right) + q^d - 1\right] = q^d\left[q^d + \left(\frac{a}{q}\right)\right]$.

On conclut que : $q^d\left(q^d + \left(\frac{a}{q}\right)\right) \equiv 1 + \left(\frac{f}{q}\right) \bmod p$

$\mapsto d = \frac{p-1}{2}$

Or, $\left(\frac{a}{p}\right) \equiv a^d \bmod p$ et $\left(\frac{a}{q}\right) \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \bmod p$, on obtient en multipliant cette identité par $\left(\frac{q}{p}\right)$:

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

On simplifie par $\left(\frac{a}{p}\right)$ et on obtient le résultat mod p. Mais comme chaque membre est un entier égal à ± 1, c'est une égalité dans $\mathbb{Z}$.