Loi de réciprocité quadratique

Pierron Théo

10 juin 2014

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

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

Théorème *Soient p, q premiers impairs. Alors*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

Démonstration. Soit

$$X = \{(x_1, \ldots, x_p) \in \mathbb{F}_q^p, q(x_1, \ldots, x_p) := x_1^2 + \ldots + x_p^2 = 1\}$$

la boule unité de $\mathbb{F}_q$. On dénombre X de deux manières.

$\mathbb{Z}/p\mathbb{Z}$ agit sur X par permutation circulaire des coordonnées. Par la relation orbite-stabilisateur, comme p est premier, les orbites et les stabilisateurs sont de taille 1 ou p. Il y a deux types d'orbites :

- Celles de la forme $\{(x, \ldots, x)\}$ qui sont de taille 1 et sont stabilisées par tout le monde.
- Les autres, de taille p et de stabilisateur trivial.

Le nombre d'orbites de la première catégorie est le nombre de x tels que $px^2 = 1$ dans $\mathbb{F}_q$, i.e. $1 + \left(\frac{p}{q}\right)$. X est la réunion disjointe des orbites pour cette action donc, pour k le nombre d'orbites de la seconde catégorie, on a

$$|X| = 1 + \left(\frac{p}{q}\right) + kp$$

Donc modulo p, $|X| = 1 + \left(\frac{p}{q}\right)$.

Soit q' la forme quadratique

$$(y_1, z_1, \ldots, y_d, z_d, t) \mapsto 2(y_1 z_1 + \ldots y_d z_d) + at^2$$

où on a posé $d = \frac{p-1}{2}$ et $a = (-1)^d$. Sa matrice est

$$\begin{pmatrix} 0 & 1 & & & & \\ 1 & 0 & & & & \\ & & \ddots & & & \\ & & & 0 & 1 & \\ & & & 1 & 0 & \\ & & & & & a \end{pmatrix}$$

de déterminant $(-1)^d a = 1$ donc q' est équivalente à q. Alors

$$|X| = |\{x, q(x) = 1\}| = |\underbrace{\{x, q'(x) = 1\}}_{X'}|$$

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

- Si $y_1 = \ldots, y_d = 0$ alors $at^2 = 1$ donc on a q^d choix pour les z_i et $1 + \left(\frac{a}{q}\right)$ pour t.
- Sinon, il existe un y_i non nul. Alors, si les y_i et t sont fixés,

$$f \quad : \quad (z_1, \ldots, z_d) \mapsto 2(y_1 z_1 + \ldots + y_d z_d) + at^2 - 1$$

est une forme linéaire non nulle donc son noyau est un hyperplan de $\mathbb{F}_q^d$ qui contient donc q^{d-1} éléments. Il y a donc $(q^d - 1)$ possibilités pour les y_i, q^{d-1} pour les z_i et q pour t.

Ainsi,

$$|X| = |X'| = q^d \left(1 + \left(\frac{a}{q}\right)\right) + q^d(q^d - 1) = q^{p-1} + q^d \left(\frac{a}{q}\right)$$

En regroupant les deux méthodes, on a, modulo p,

$$1 + \left(\frac{p}{q}\right) = q^{p-1} + q^d \left(\frac{a}{q}\right) = 1 + q^d a^{\frac{q-1}{2}} = 1 + \left(\frac{q}{p}\right)(-1)^{\frac{(p-1)(q-1)}{4}}$$

En simplifiant, on a finalement

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \mod p$$

Comme tout ce beau monde vaut 1 ou -1, l'égalité est en fait vraie dans $\{\pm 1\}$, ce qui conclut. ■