Loi de réciprocité quadratique par les formes quadratiques

Lemme. *Soient a un entier non nul et q un nombre premier impair. Alors*

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

Démonstration : comme a est un carré modulo q si et seulement si a^{-1} en est un, il est équivalent de dire que a est un carré modulo q et que le polynôme $aX^2 - 1 \in \mathbb{F}_q[X]$ possède deux racines distinctes dans $\mathbb{F}_q$. Ainsi, le cardinal considéré vaut 0 si a n'est pas un carré modulo q, et 2 si a est un carré modulo q. Comme on peut encore écrire, de façon atrocement astucieuse, $0 = 1 - 1$ et $2 = 1 + 1$, le résultat suit. ■

Théorème. *Soient p et q deux nombres premiers impairs. On a*

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

Démonstration : considérons l'ensemble

$$X = \left\{(x_1, \ldots, x_p) \in \mathbb{F}_q^p, \sum_{i=1}^{p} x_i^2 = 1\right\}.$$

On va calculer son cardinal modulo p de deux façons différentes.

Tout d'abord, on peut le voir comme

$$X = \left\{x \in \mathbb{F}_q^p, f(x) = 1\right\},$$

où f est la forme quadratique dont la matrice dans la base canonique de $\mathbb{F}_q^p$ est I_p. Posons

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

et considérons la forme quadratique dont la matrice dans la base canonique de $\mathbb{F}_q^p$ est

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

On constate que $\mathrm{rg}(M) = p = \mathrm{rg}(I_p)$ 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, qui est le déterminant modulo les carrés du corps de base), elles sont congruentes. Ainsi $|X| = |X'|$, où

$$X' = \left\{x \in F_q^p, f'(x) = 1\right\},$$

et f' est la forme quadratique dont la matrice dans la base canonique de $\mathbb{F}_q^p$ est M ; autrement dit, on a

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

Il suffit donc de déterminer le cardinal de X'. Soit $(y_1, z_1, \ldots, y_d, z_d, t) \in X'$.

- si $y_1 = \ldots = y_d = 0$, alors le choix des z_i est quelconque, et t doit vérifier $at^2 = 1$. Ainsi, il y a q^d choix des z_i et $1 + \left(\frac{a}{q}\right)$ choix de t d'après le lemme. Il y a donc $q^d\left[1 + \left(\frac{a}{q}\right)\right]$ éléments de cette forme ;
- au contraire, s'il existe un y_i non nul, alors $(y_1, \ldots, y_d)$ est un vecteur non nul de $\mathbb{F}_q^d$, 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. Au total, il y a $(q^d - 1)qq^{d-1} = q^d(q^d - 1)$ éléments de cette forme

Par suite,

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

À présent, on fait agir $\mathbb{Z}/p\mathbb{Z}$ sur X par $k \cdot (x_1, \ldots, x_p) = (x_{k+1}, \ldots, x_{k+p})$, les indices étant vus modulo p. Il y a deux sortes d'orbites :

- celles dont le stabilisateur est $\mathbb{Z}/p\mathbb{Z}$, elles sont de la forme $\{(x, \ldots, x)\}$, où $x \in \mathbb{F}_q$ vérifie $f(x, \ldots, x) = 1$, c'est-à-dire $px^2 = 1$;
- les autres, dont le stabilisateur, étant un sous-groupe de $\mathbb{Z}/p\mathbb{Z}$, est forcément trivial.

L'équation aux classes nous donne alors

$$|X| = \sum_{px^2=1} \frac{|\mathbb{Z}/p\mathbb{Z}|}{|\mathbb{Z}/p\mathbb{Z}|} + \sum_{\text{autres orbites}} \frac{|\mathbb{Z}/p\mathbb{Z}|}{|\{1\}|} \equiv 1 + \left(\frac{p}{q}\right)[p]$$

grâce au lemme.

On en conclut que

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

Comme $q^d \equiv \left(\frac{q}{p}\right)[p]$ et que de même $\left(\frac{a}{q}\right) \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}}[p]$, on obtient en multipliant cette identité par $\left(\frac{q}{p}\right)$

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

Simplifiant par $\left(\frac{q}{p}\right)$, on obtient le résultat voulu modulo p. Mais comme chaque membre est un entier égal à ± 1, c'est en fait une égalité dans $\mathbb{Z}$. ■