Loi de réciprocité quadratique par les formes quadratiques.

Rémi Lajugie

Pour pouvoir présenter ce développement, il vaut mieux avoir travaillé la théorie des formes bilinéaires symétriques et des formes quadratiques. On rappelle un fait et deux propositions qui nous seront fort utiles.

Fait 1 *Le nombre de solutions à l'équation* $1+px^2=0$ *dans* $\mathbb{F}_q$ *est* $\left(\frac{p}{q}\right)+1$.

Proposition 1 *Le symbole de Legendre* $\left(\frac{p}{q}\right)$, *vérifie* $\left(\frac{p}{q}\right)=p^{\frac{q-1}{2}}$ *dans* $\mathbb{Z}/q\mathbb{Z}$.

Théorème 1 *Soit* p,q *deux nombres premiers impairs, alors on a* $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{(\frac{p-1}{2})(\frac{q-1}{2})}$.

Preuve :

L'idée est de compter de deux manières différentes le nombre d'éléments de la boule unité de $\mathbb{F}_q^p$.

Etape 1 : un premier comptage. On fait agir $\mathbb{Z}/p\mathbb{Z}$ sur les p-uplets constituant la boule unité B de $\mathbb{F}_q^p$ par permutation circulaire. Comme le groupe est simple car d'ordre premier, il n'y a que des stabilisateurs triviaux (égaux soit au singleton $\{1\}$ soit à $\mathbb{Z}/p\mathbb{Z}$). On peut alors distinguer deux types d'orbites :

1. Les singletons, de stabilisateur $\mathbb{Z}/p\mathbb{Z}$. Il y en a autant que de solutions à $px^2=1$ soit $\left(\frac{p}{q}\right)+1$ vu le fait.
2. Les autres dont le cardinal est forcément p.

Ainsi comme les orbites partitionnent B, on en déduit $|B|=1+\left(\frac{p}{q}\right)[p]$.

Etape 2 : un deuxième comptage.

Par la théorie des formes quadratiques sur les corps finis, les formes quadratiques associées aux matrices $I=\begin{pmatrix}1,0,\dots,0\\0,1,\dots,0\\0,0,\dots,0\\0,0,\dots,1\end{pmatrix}$, et $A=\begin{pmatrix}0,1,0,0,\dots,0\\1,0,0,0,\dots,0\\0,0,0,1,\dots,0\\0,0,1,0,\dots,0\\0,0,\dots,0,1,0\\0,0,\dots,1,0,0\\0,0,\dots,0,0,\delta\end{pmatrix}$, où $\delta=(-1)^{\frac{p-1}{2}}$, sont congruentes (elles ont le même déterminant donc même discriminant). Donc les boules unités sont en bijection et ont le même cardinal. Posons $d=\frac{p-1}{2}$, Comptons les éléments de la boule : on les écrit sous la forme $(y_1,z_1,\dots,y_d,z_d,t)$. Ils satisfont à $y_1z_1+\dots+\delta t^2=1$ et on compte le nombre d'éléments :

1. Si $y_1=\dots=y_d=0$, on compte $q^d(1+\left(\frac{p}{q}\right)^{(\frac{p-1}{2}})$.
2. Sinon, on a $q^d(q^d-1)$ éléments.

On additionne et on a donc $q^d(q^d-1+1+\left(\frac{p}{q}\right)^{(\frac{p-1}{2}})$.

Etape 3 : On égalise le tout

On remarque que, modulo p, $q^d=\left(\frac{p}{q}\right)$ et il vient immédiatement que $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{(p-1)}{2}\frac{(q-1)}{2}}$

Références

— H2G2.