Loi de réciprocité quadratique

Théorème 1. Soient p et q premiers impairs distincts.

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

Démonstration. Posons $X = \{(x_1, \dots, x_p) \in \mathbb{F}_q^p,\ x_1^2 + \cdots + x_p^2 = 1\}$. Calculons le cardinal de X modulo p de deux manières différentes.

Méthode 1 : $\mathbb{F}_p$ agit sur X via :

$$k \in \mathbb{F}_p \mapsto [(x_1, \dots, x_p) \mapsto (x_{k+1}, \dots, x_{k+p})] \in \mathfrak{S}_x.$$

Les orbites sous cette action sont de deux sortes :
- les orbites triviales, de stabilisateur $\mathbb{F}_p$, de la forme $\{(x, \dots, x)\}$ avec $x \in \mathbb{F}_q$ satisfaisant $px^2 = 1$.
- les autres orbites, dont le stabilisateur (sous-groupe de $\mathbb{F}_p$) est trivial.

La formule des classes donne donc, à l'aide du lemme ci-dessous :

$$|X| = \sum_{px^2=1} 1 + \sum_{px^2 \neq 1} \frac{|\mathbb{F}_p|}{|\{1\}|} = 1 + \left(\frac{p}{q}\right) \ [p].$$

Lemme 2. L'ensemble $\{x \in \mathbb{F}_q,\ ax^2 = 1\}$ est de cardinal $1 + \left(\frac{a}{q}\right)$ si $a \neq 0$.

Démonstration du lemme. L'élément a est un carré si et seulement si son inverse est un carré, i.e. si et seulement si $X^2 - a^{-1}$ (ou encore $aX^2 - 1$) possède deux racines distinctes. Donc le cardinal recherché vaut 2 si a est un carré (non nul), 0 sinon, d'où le résultat. □

Méthode 2 : $X = \{f = 1\}$, où f est la forme quadratique de matrice I_p dans $\mathbb{F}_q^p$. Posons maintenant

$$d = \frac{p-1}{2}, \quad a = (-1)^d, \quad J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{et} \quad M = \begin{pmatrix} J & & & \\ & \ddots & & \\ & & J & \\ & & & a \end{pmatrix}.$$

Puisque $\mathrm{rg}(M) = \mathrm{rg}(I_p)$ et $\det M = (\det J)^d a = 1 = \det I_p$, les matrices M et I_p sont congrues, donc :

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

- Si $y_1 = \cdots = y_d = 0$, alors le choix des z_i n'importe pas et par lemme, il y a $\left(1 + \left(\frac{a}{q}\right)\right) q^d$ éléments dans X' de cette forme.
- Sinon, il y a $(q^d - 1)$ choix possibles pour les y_i, q choix pour t, et les z_i vivent alors dans un hyperplan affine de $\mathbb{F}_q^d$ (de cardinal q^{d-1}). Il y a donc $(q^d - 1)q^d$ éléments de cette forme dans X'.

Ainsi, en reprenant ce qui précède :

$$|X'| = q^d \left(q^d + \left(\frac{a}{q}\right)\right) = \left(\frac{q}{p}\right) \left[\left(\frac{q}{p}\right) + (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\right] \ [p]$$

car $\left(\frac{a}{q}\right) = a^{\frac{q-1}{2}} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ $[q]$, ce qui est donc vrai dans $\mathbb{Z}$, puis modulo p.

En comparant les résultats donnés par les deux méthodes ci-dessus, on obtient :

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

ce qui est donc vrai dans $\mathbb{Z}$ car les quantités sont ± 1. □