Loi de réciprocité quadratique

Théorème . Soient $p,q \geq 3$ deux nombres premiers. Alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ avec la notation pour le symbole de Legendre $\left(\frac{x}{q}\right) = \begin{cases} 1 & \text{si } x \in \left(\mathbb{F}_q^\times\right)^2 \\ 0 & \text{si } x \equiv 0 \quad [q] \\ -1 & \text{sinon} \end{cases}$.

Preuve :
Nous allons compter l'ensemble

$$X := \left\{ \ (x_1,\dots,x_p) \in \mathbb{F}_q^p \ ; \ x_1^2+\dots+x_p^2 = 1 \ \right\}$$

modulo p de deux manières différentes.
On remarque que $\mathbb{Z}/p\mathbb{Z}$ agit par permutation circulaire sur X via $(x_1,\dots,x_p) \mapsto (x_{1+n},\dots,x_{p+n})$ où les indices sont pris modulo p. D'après la relation orbite-stabilisateur, il y a deux types d'orbites

- celles de taille p dont le stabilisateur est trivial.
- les orbites de la forme $\{(x,\dots,x)\}$, avec $px^2 = 1$ dans $\mathbb{F}_q$, de stabilisateur $\mathbb{Z}/p\mathbb{Z}$. Il y en a donc autant que de solutions à cette équation, c'est-à-dire $1+\left(\frac{p}{q}\right)$.

Donc $|X| \equiv 1+\left(\frac{p}{q}\right) \quad [p]$.

On pose $d = \dfrac{p-1}{2}$ et $a = (-1)^d$ et on considère maintenant l'ensemble

$$X' := \left\{ \ (x_1,\dots,x_p) \in \mathbb{F}_q^p \ ; \ Q(x_1,\dots,x_p) := 2\Big(x_1x_2+x_3x_4+\dots+x_{p-2}x_{p-1}\Big)+ax_p^2 = 1 \ \right\}.$$

Alors la matrice de Q dans la base canonique est

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

On sait que la matrice de Q dans une bonne base est I_p ou $\mathrm{diag}(1,\dots,1,\alpha)$ avec $\alpha \in \mathbb{F}_q$ qui n'est pas un carré. Or le discriminant de Q est 1 par construction. On en déduit que sa matrice est I_p dans une bonne base, et donc que $|X| = |X'|$.

Nous allons maintenant compter X' modulo p et en déduire le résultat. Soit $(x_1,\dots,x_p) \in X'$.

· Cas 1 : $(x_1,x_3,\dots,x_{p-2}) = (0,\dots,0)$.
La condition devient alors $ax_p^2 = 1$. Il y a $1+\left(\frac{a}{q}\right)$ solutions pour x_p, et q^d pour $(x_2,\dots,x_{p-1})$ ce qui donne $q^d\left(1+\left(\frac{a}{q}\right)\right)$.

· Cas 2 : $(x_1, x_3, \ldots, x_{p-2}) \neq (0, \ldots, 0)$.
On considère alors $(x_1, x_3, \ldots, x_{p-2})$ fixés, et soit $x_p \in \mathbb{F}_q$ fixé. L'équation devient celle d'un hyperplan affine dans un espace vectoriel de dimension d sur un corps de cardinal q, il y a q^{d-1} possibilités pour $(x_2, \ldots, x_{p-1})$. De plus, il y a $q^d - 1$ choix pour $(x_1, x_3, \ldots, x_{p-2})$ et q choix pour x_p, ce qui fait au total $q^d(q^d - 1)$ possibilités pour $(x_1, \ldots, x_p)$.

Donc $|X'| = q^d(1 + \left(\frac{a}{q}\right)) + q^d(q^d - 1) = q^{p-1} + q^d \left(\frac{a}{q}\right)$. On regarde alors l'égalité entre $|X|$ et $|X'|$ modulo p

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

Or $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}$ dans $\mathbb{F}_p$ donc

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

et ainsi

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

Or de même les termes valent $1, 0$ ou -1, on a donc l'égalité en tant qu'entier et non seulement modulo p.

□