Loi de réciprocité quadratique (via les FQ)

Réf : H2G2, Tome 1er (p185) ou NH2G2 Tome 1 (p304)

Leçons : 101, 120, 121, 123, 126, 170, 190

Thm : $p,q \in \mathbb{P}$ impairs, $p \neq q$: $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

Déf : Pour $p \in \mathbb{P}$ impair, $a \geq 1$ $\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \text{ est un carré dans } \mathbb{F}_p^* \\ -1 & \text{si } a \text{ n'est pas un carré dans } \mathbb{F}_p^* \\ 0 & \text{si } p \mid a \end{cases}$.

Lm : Si $p \in \mathbb{P}$ impair, $a \in \mathbb{F}_p^*$ alors $\left|\{x \in \mathbb{F}_p,\ ax^2 = 1\}\right| = 1 + \left(\frac{a}{p}\right)$

Dem : a est un carré modulo p ssi a^{-1} est un carré mod p. Si a n'est pas un carré → pas de sol. Si a est un carré, cela vient du fait que si b est un carré alors le polynôme $X^2 - b$ admet deux racines distinctes dans $\mathbb{F}_p$. ✓

Dem du Thm : Calculons de 2 manières différentes $|X| = \left|\{(x_1,\dots,x_p) \in \mathbb{F}_q^p,\ \sum_{i=1}^p x_i^2 = 1\}\right|$

① Calcul par action :

$\mathbb{Z}/p\mathbb{Z} \curvearrowright X$ par $k \cdot (x_1,\dots,x_p) = (x_{1+k},\dots,x_{p+k})$ où les indices sont mod p

On étudie les orbites de cette action. $\mathbb{Z}/p\mathbb{Z}$ n'a pas $\{1\}$ et l'inclusion comme ss-gp donc $\mathrm{Stab}(y) = \{1\}$ ou $\mathbb{Z}/p\mathbb{Z}$. Si $\mathrm{Stab}(y) = \mathbb{Z}/p\mathbb{Z}$ alors $x_1 = x_2 = \dots = x_p =: x$ et donc $\sum_{i=1}^p x_i^2 = 1 = px^2$, $x \in \mathbb{F}_q$.

$\rightsquigarrow$ les orbites dont le stab est $\mathbb{Z}/p\mathbb{Z}$ sont les singletons $\{(x,\dots,x),\ x \in \mathbb{F}_q,\ px^2 = 1\}$.

Par le Lm, il y en a $1 + \left(\frac{p}{q}\right)$.

Par la relation orbite-stabilisateur, les orbites dont le stab est $\{1\}$, sont de cardinal $|\mathbb{Z}/p\mathbb{Z}| / |\{1\}| = p$. Par la formule des classes, $|X| = \sum_{\substack{x \\ \text{représentant}}} |\mathrm{orb}(x)|$ on a mod p :

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

② Calcul par FQ : Notons $f(x) = \sum_{i=1}^p x_i^2$. Sa matrice dans la base canonique est I_p.

Posons $A = \begin{pmatrix} 0 & 1 & & (0) \\ 1 & 0 & & \\ & & \ddots & \\ (0) & & & a \end{pmatrix}$ où $a = (-1)^d$ et $d = \frac{p-1}{2}$. A et I_p sont de rang p et même déterminant (en effet, A est diag par blocs avec $\det(b_k) = -1$). Donc A et I_p ont même discriminant donc elles définissent 2 FQ équivalentes donc $\exists P \in GL_p$, $I_p = {}^tPAP$.

Et $X = \{x = (x_1,\dots,x_p) \in \mathbb{F}_q^p,\ {}^txx = 1\} = \{x,\ {}^tx{}^tPAPx = 1\} = \{y,\ {}^tyAy = 1\} = X'$ (via $y = Px$)

donc $|X| = |X'| = |\{(y_1,\dots,y_d,z_1,\dots,z_d,t) \in \mathbb{F}_q^p;\ 2(y_1z_1 + \dots + y_dz_d) + at^2 = 1\}|$.

On a 2 cas :

1) Soit $\forall i\ y_i = 0$: Le choix des z_i est donc quelconque et donne q^d possibilités.
On a donc $at^2 = 1$, le lemme fournit qu'il y a $1 + \left(\frac{a}{q}\right)$ possibilités
soit $\underline{q^d\left(1 + \left(\frac{a}{q}\right)\right) \text{ possibilités}}$

2) Soit $\exists i, y_i \neq 0$. On choisit un vecteur de $\mathbb{F}_q^d$ non nul : $q^d - 1$ possibilités,
t quelconque dans $\mathbb{F}_q$: q possibilités
Il reste à choisir $(z_1, \dots, z_d)$ dans l'hyperplan affine d'eq : $2(y_1 z_1 + \dots + y_d z_d) + at^2 - 1 = 0$
il y a donc q^{d-1} possibilités donc $\underline{(q^d - 1)\, q^d \text{ possibilités}}$.

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

(3) Conclusion :

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

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

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

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

Donc $\left(\frac{a}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \ [p]$. On a des éléments en jeu sont égaux à ± 1 donc l'égalité est vraie dans $\mathbb{Z}$. CQFD.