Loi de réciprocité quadratique

Réf:
- Histoires hédonistes de groupes et de géométries tome 1 J. Caldero

Leçons: 101, 121, 170, 190.

Lemme

Soient p un nombre premier impair et $a \in \mathbb{F}_p^\times$.
Alors on a

$$\#\left\{x \in \mathbb{F}_p / \; ax^2 = 1\right\} = 1 + \left(\frac{a}{p}\right)$$

Preuve:

L'élément a est un carré dans $\mathbb{F}_p$ si et seulement si a^{-1} en est un. (par exemple car $x \longmapsto \left(\frac{x}{p}\right)$ est un morphisme de groupes entre $\mathbb{F}_p^\times$ et $\{-1, 1\}$)

Ainsi si a est un carré dans $\mathbb{F}_p$ alors il existe $x \in \mathbb{F}_p^\times$ tel que $x^2 = a^{-1}$. Comme $p \neq 2$, x et $-x$ sont distincts.
Donc $aX^2 - 1$ admet 2 racines dans $\mathbb{F}_p$.

Si a n'est pas un carré alors a^{-1} non plus et donc le polynôme $aX^2 - 1$ n'a pas de racine dans $\mathbb{F}_p$.

Cela conclut ∎

Théorème

Soient p et q des nombres premiers impairs distincts.
Alors on a

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

Preuve:

Notons X l'ensemble $\left\{(x_1, \dots, x_p) \in \mathbb{F}_q^p \; / \; \sum_{i=1}^{p} x_i^2 = 1\right\}$.

Idée : on calcule le cardinal de X de deux façons différentes

Etape 1 : avec une action de $\mathbb{F}_p$ sur $\mathbb{F}_q^p$.

On considère l'action par permutation cyclique de $\mathbb{F}_p$ sur $\mathbb{F}_q^p$ définie par

$$\forall k \in \mathbb{F}_p \ \forall (x_1, \dots, x_p) \in \mathbb{F}_q^p \quad k \cdot (x_1, \dots, x_p) = (x_{1+k}, \dots, x_{p+k})$$

où les indices sont les représentants modulo p dans $[\![1, p]\!]$.

Le sous-ensemble X est stable par cette action donc on considère celle-ci en restriction à X.

Soit $x \in X$.

Si $\mathrm{Stab}(x) = \mathbb{F}_p$ alors il s'en suit

$$\forall i \in [\![1, p]\!] \quad x_1 = x_i$$

et donc, comme $x \in X$, $p x_1^2 = \sum_{i=1}^{p} x_i^2 = 1$.

Si $\mathrm{Stab}(x) \neq \mathbb{F}_p$ alors comme $\mathrm{Stab}(x)$ est un sous-groupe de $\mathbb{F}_p$ et comme p est premier, on a par théorème de Lagrange $\#\mathrm{Stab}(x) = 1$.

Par la formule des classes, on obtient alors

$$|X| = \sum_{\substack{x_1 \in \mathbb{F}_p \\ a x_1^2 = 1}} 1 + \sum_{i=1}^{N} p = \#\{x \in \mathbb{F}_q / p x^2 = 1\} + Np$$

où N est le nombre d'orbites distinctes non réduites à 1 élément.

Il s'en suit par le lemme précédent $|X| \equiv 1 + \left(\frac{p}{q}\right) \bmod p$

Etape 2 : avec une forme quadratique.

Les matrices symétriques I_p et

$$A = \begin{pmatrix} 0 & 1 & & & \\ 1 & 0 & & & \\ & & \ddots & & \\ & & & 0 & 1 \\ & & & 1 & 0 \\ & & & & a \end{pmatrix} \in M_p(\mathbb{F}_q)$$

où $a = (-1)^{\frac{p-1}{2}}$, sont de même rang p et on a

$$\det(A) = \det(I_p) = 1$$

Par classification des formes quadratiques sur $\mathbb{F}_q$, ces matrices sont congruentes.

Ainsi les ensembles X et

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

ont le même cardinal, où $d = \frac{p-1}{2}$.

Soit $(y_1, \dots, y_d, z_1, \dots, z_d, t)$ dans X'.

Si on a $y_1 = \dots = y_d = 0$ alors chaque valeur $t \in \mathbb{F}_q$ vérifiant

$$at^2 = 1$$

détermine q^d points de cet acabit (on choisit $z_1, \dots, z_d$ comme on veut dans $\mathbb{F}_q$)

S'il existe $i \in [\![1, d]\!]$ tel que $y_i \neq 0$ alors $(y_1, \dots, y_d)$ est un vecteur non nul de $\mathbb{F}_q^d$, soit $q^d - 1$ choix possibles

Puis pour un choix de t dans $\mathbb{F}_q$, le vecteur $(z_1, \dots, z_d)$ est un élément d'un hyperplan affine de $\mathbb{F}_q^d$, c-à-d on a $\#\mathbb{F}_q^{d-1}$ choix possible pour ce vecteur.

On en déduit l'égalité

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

$$" \quad = q^d \left(\left(\frac{a}{q}\right) + q^d\right)$$

Etape 3 : conclusion.

On obtient en combinant les deux égalités obtenues

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

Par ailleurs, on a

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

et $$q^d \equiv q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right) \bmod p .$$

Donc on a

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

c-à-d $$\left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \equiv \left(\frac{p}{q}\right) \bmod p$$

Comme chacun des côtés de l'égalité modulo p sont soit 1 soit -1, et comme p est différent de 2, on a une égalité.

Cela conclut ■