15. Loi de réciprocité quadratique

[Rom17, §13.6-7, p429–435]

ÉNONCÉ

THÉORÈME. [LOI DE RÉCIPROCITÉ QUADRATIQUE]
Soient $p \neq q$ des nombres premiers impairs. Alors :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \quad \text{où} \quad \left(\frac{x}{p}\right) = \begin{cases} 1 & \text{si } x \text{ est un carré dans } \mathbb{F}_p^* \\ 0 & \text{si } x = 0 \\ -1 & \text{sinon} \end{cases}$$

DÉVELOPPEMENT

Soient p et q des entiers premiers impairs. Montrons d'abord le lemme suivant ;

LEMME. *Pour $a \in \mathbb{F}_q^*$, on a $\overline{\left(\frac{a}{q}\right)} = a^{\frac{q-1}{2}}$ dans $\mathbb{F}_q^*$ et $|\{x \in \mathbb{F}_q^* \mid ax^2 = 1\}| = 1 + \left(\frac{a}{q}\right)$.*

En effet si $a = b^2$ est un carré, alors nécessairement $a^{\frac{q-1}{2}} = b^{q-1} = \overline{1} = \overline{\left(\frac{a}{q}\right)}$.
Comme on a $\frac{q-1}{2}$ carrés [1] dans $\mathbb{F}_p^*$ et que $X^{\frac{q-1}{2}} - 1$ a au plus $\frac{q-1}{2}$ solutions dans F_q^*, on en déduit que si a n'est pas un carré, alors $a^{\frac{q-1}{2}} = \overline{-1} = \overline{\left(\frac{a}{q}\right)}$.

Ensuite, si $a = b^2$ est un carré, alors $ax^2 = 1 \iff (bx)^2 = 1 \iff x = \pm b^{-1}$ et donc puisque $q \neq 2$, on a bien deux solutions. Sinon, il n'y a pas de solutions puisque le produit d'un carré c par un non carré d est un non carré. En effet $\overline{\left(\frac{cd}{q}\right)} = (cd)^{\frac{q-1}{2}} = c^{\frac{q-1}{2}} d^{\frac{q-1}{2}} = \overline{\left(\frac{c}{q}\right)} \times \overline{\left(\frac{d}{q}\right)} = \overline{1} \times \overline{-1} = \overline{-1}$ et puisque $q \neq 2$, $\left(\frac{cd}{q}\right) = -1$.

Soit maintenant $X = \{x = (x_1, \dots, x_p) \in \mathbb{F}_q^p \mid \sum_{i=1}^p x_i^2 = 1\}$. On va dénombrer X modulo p de deux manières différentes :

- Considérons d'abord l'action de $\mathbb{F}_p$ sur X définie par [2] $\overline{k}.(x_1, \dots, x_p) = (x_{1+k}, \dots, x_{p+k})$.
  Le cardinal de l'orbite d'un élément divise $p = |\mathbb{F}_p|$, donc est égal à 1 ou p.
  L'orbite de x est réduite à lui-même si et seulement si $x_1 = \dots = x_p$. Le nombre de tels x dans X est le nombre de solutions de $px_1^2 = 1$, c'est-à-dire $1 + \left(\frac{p}{q}\right)$ d'après le Lemme.
  Ainsi $|X| \equiv 1 + \left(\frac{p}{q}\right) \mod p$.
- On a $X = \{x \in \mathbb{F}_q^p \mid f(x) = 1\}$ où f est la forme quadratique associée à Id_p dans la base canonique. Notons $d = \frac{p-1}{2}$.
  Soit $M = \mathrm{diag}(J, J, \dots, J, a)$ où $J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ est répétée d fois et $a = (-1)^d$.
  On a $\mathrm{rg}(M) = p$ et $\det(M) = a \det(J)^d = (-1)^d(-1)^d = 1$. La forme quadratique g associée à M dans la base canonique est donc non dégénérée et par classification des formes quadratiques [3] sur $\mathbb{F}_q$, on a que f et g sont congruentes.
  Soit $X' = \{x \in \mathbb{F}_q^p \mid g(x) = 1\} = \{x \in \mathbb{F}_q^p \mid 2\sum_{k=1}^d x_{2k}x_{2k-1} + ax_p^2 = 1\}$.
  Alors $|X| = |X'|$ et si $x \in X'$:
  - soit pour tout $k \leq d$, $x_{2k+1} = 0$ et $ax_p^2 = 1$: on a alors $1 + \left(\frac{a}{q}\right)$ possibilités pour x_p et q^d pour les $(x_{2k})_{1 \leq k \leq d}$,
  - soit il existe un $x_{2k+1} \neq 0$: on choisit $(x_{2k+1})_{1 \leq k \leq d}$ et x_p avec $q(q^d - 1)$ possibilités, puis on choisit $(x_{2k})_{1 \leq k \leq d}$ satisfaisant $2\sum_{k=1}^d x_{2k-1}x_{2k} = 1 - ax_p^2$, équation d'un hyperplan affine de cardinal q^{d-1}.

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

Ainsi par le Lemme :

$$\begin{aligned} & 1 + \left(\frac{p}{q}\right) \equiv \left(\frac{q}{p}\right)\left(\left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right) + \left(\frac{q}{p}\right)\right) \mod p \\ \iff & \left(\frac{q}{p}\right) + \left(\frac{q}{p}\right)\left(\frac{p}{q}\right) \equiv \left(\frac{q}{p}\right) + ((-1)^{\frac{p-1}{2}})^{\frac{q-1}{2}} \mod p \\ \iff & \left(\frac{q}{p}\right)\left(\frac{p}{q}\right) \equiv (-1)^{\frac{(p-1)(q-1)}{2}} \mod p \end{aligned}$$

On obtient alors le résultat puisque les deux membres de la congruence sont égaux à ± 1 dans $\mathbb{Z}$ et que $p \neq 2$.

COMMENTAIRES

Il y a pas mal de choses à maitriser sur les formes quadratiques : classification, égalité des cardinaux de X et X', expression de la forme quadratique à partir de sa matrice …

Il faut savoir ce qu'il se passe dans le cas $p = 2$. La loi de réciprocité quadratique sert notamment à résoudre des équations diophantiennes. Savoir si un élément est un carré dans $\mathbb{F}_q$ permet aussi dans le cas des formes quadratiques, de classifier une forme quadratique (connaissant un déterminant, il suffit de savoir si c'est un carré).

1. car $\phi : \mathbb{F}_q^* \longrightarrow \mathbb{F}_q^*, a \longmapsto a^2$ est un morphisme de groupes et $|\mathrm{Im}(\phi)| = |\mathbb{F}_q^*| / |\ker(\phi)| = (q-1)/2$
2. les indices des éléments sont modulo p
3. valable pour un corps de caractéristique différente de 2 : c'est bien le cas ici puisque $q \geq 3$