

Loi de réciprocité quadratique

[CALDERO 1, p 319]

ÉNONCÉ :

Théorème :

Soient p , deux nombres premiers impairs distincts. Alors on a :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \quad \text{où} \quad \left(\frac{x}{p}\right) = \begin{cases} 1 & \text{si } x \in (\mathbb{F}_p^*)^2 \\ 0 & \text{si } x = 0 \\ -1 & \text{sinon} \end{cases}$$

DÉVELOPPEMENT :

LEMME :

Pour $a \in \mathbb{F}_q^*$, on a :

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

Démonstration. 1. Si $a \in (\mathbb{F}_q^*)^2$, alors il existe $b \in \mathbb{F}_q^*$ tel que $a = b^2$. Ainsi, on a : $a^{\frac{q-1}{2}} = b^{q-1} = 1 = \left(\frac{a}{q}\right)$. Comme on a $\frac{q-1}{2}$ carrés dans $\mathbb{F}_q^*$ et que le polynôme $X^{\frac{q-1}{2}} - 1$ a au plus $\frac{q-1}{2}$ racines dans $\mathbb{F}_q^*$. On en déduit que si a n'est pas un carré, alors $a^{\frac{q-1}{2}} = -1 = \left(\frac{a}{q}\right)$.

2. Si $a = b^2$ est un carré, alors $ax^2 = 1 \iff (bx)^2 = 1 \iff x = \pm b^{-1}$ donc on a bien 2 solutions (car $q \neq 2$). Sinon, on a, par le

premier point :

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

donc il n'y a pas de solutions (car 1 est un carré dans $\mathbb{F}_q^*$). □

Démonstration. Dénombrons $X = \{(x_1, \dots, x_p) \in \mathbb{F}_q^p \mid \sum_{i=1}^n x_i^2 = 1\}$ de deux manière différentes.

D'une part, considérons l'action de $\mathbb{F}_p$ sur X par permutation circulaire (considérée modulo p). Les orbites sous cette action divisant $p = |\mathbb{F}_p|$ et $|\mathcal{O}(x)| = 1 \iff |G_x| = p \iff x_1 = \dots = x_p$, l'équation aux classes nous donne :

$$|X| \equiv \sum_{\{x \in \mathbb{F}_q \mid px^2=1\}} 1 \quad [p]$$

En vertu du lemme, on en déduit que $|X| \equiv 1 + \left(\frac{p}{q}\right) \quad [p]$.

Considérons la matrice $A = \text{diag}(J_1, \dots, J_d, a)$ où , pour $i \in \{1, \dots, d\}$, $J_i = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $d = \frac{p-1}{2}$ et $a = (-1)^{\frac{p-1}{2}}$. Alors $\det(A) = \det(I_p) = 1$, $\text{rg}(A) = p = \text{rg}(I_p)$, donc A et I_p sont congruentes. Ainsi $A = {}^t P I_p P$, pour une matrice $P \in GL_p(\mathbb{F}_q)$. La bijection $u \mapsto P^{-1}u$ envoie bijectivement X sur l'ensemble :

$$\begin{aligned} X' &= \{u' \in \mathbb{F}_q^p \mid {}^t u' A u' = 1\} \\ &= \{(y_1, z_1, \dots, y_d, z_d, t) \in \mathbb{F}_q^q \mid 2 \left(\sum_{i=1}^d y_i z_i\right) + at^2 = 1\} \end{aligned}$$

Distinguons 2 types de points dans X' :

- Les points tels que $y_1 = \dots = y_d = 0$: chaque valeur de t telle que $at^2 = 1$ détermine q^d tels points soit :

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

- Les points pour lesquels au moins un des y_i n'est pas nul (il y a $q^d - 1$ possibilités pour les y_i) : une fois fixés $(y_1, \dots, y_d)$ et t , il reste à choisir un élément $(z_1, \dots, z_d)$ dans un hyperplan affine de $\mathbb{F}_q^d$: il y a :

$$(q^d - 1)qq^{d-1}$$

tels points en tout.

En faisant la somme des points de chaque type, on obtient :

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

En comparant les deux expressions trouvées de $|X|$, on a que :

$$|X| = \left(q^{\frac{p-1}{2}} + (-1)^{\frac{p-1}{2} \times \frac{q-1}{2}} \right) q^{\frac{p-1}{2}} \equiv \left(\frac{p}{q} \right) + 1 \quad [p]$$

D'où , en termes de symbole de LEGENDRE :

$$|X| = \left(\left(\frac{q}{p} \right) + (-1)^{\frac{p-1}{2} \times \frac{q-1}{2}} \right) \left(\frac{q}{p} \right) \equiv \left(\frac{p}{q} \right) + 1 \quad [p]$$

d'où, après simplification :

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

Mais comme p est impair et que les deux membres de l'égalité sont éléments de $\{-1, 1\}$, l'égalité demeure vraie sur $\mathbb{Z}$, d'où le résultat. □

Remarques :

- Il faut être capable d'appliquer ce résultat sur des exemples simples.
- On a en particulier : $\left(\frac{-1}{p} \right) = (-1)^{\frac{p-1}{2}}$.
- Pour le cas où $q = 2$: $\left(\frac{2}{p} \right) = (-1)^{\frac{p^2-1}{8}} \rightarrow$ pas trivial !