Titre : **Loi de réciprocité quadratique.**
Recasages : 120,121,123,126
Thème : Arithmétique, calculatoire, polynômes et corps.
Références : Serre - Cours d'arithmétique (p. 14)

Théorème 1. *(Loi de réciprocité quadratique)*
Soient p, q deux nombres premiers impairs distincts, alors

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

Lemme 2. *Soit $x \in \mathbb{F}_p^*$, on a que x est un carré dans $\mathbb{F}_p^*$ si et seulement si $x^{\frac{p-1}{2}} = 1$.*

Démonstration. Notons

$$A = \{\text{carrés dans } \mathbb{F}_p^*\} \quad \text{et} \quad B = \{x \in F_p^* \mid x^{\frac{p-1}{2}} = 1\}$$

Soit $x \in A$, il existe alors $y \in \mathbb{F}_p^*$ tel que $y^2 = x$, on a alors $x^{\frac{p-1}{2}} = y^{p-1} = 1$ par le théorème de Lagrange sur le groupe $(\mathbb{F}_p^*, \times)$, donc $x \in B$ et $A \subset B$.
Considérons ensuite le morphisme de groupes

$$\begin{array}{rccc} \varphi : & \mathbb{F}_p^* & \longrightarrow & A \\ & x & \longmapsto & x^2 \end{array}$$

Il s'agit d'un morphisme surjectif (par définition de A), or, son noyau est donné par $\{\pm 1\}$, donc $|A| = \frac{|\mathbb{F}_p^*|}{2} = \frac{p-1}{2}$.
Enfin, B est constitué des racines du polynômes $X^{\frac{p-1}{2}} - 1 \in \mathbb{F}_p[X]$, il est donc au plus de cardinal $\frac{p-1}{2}$. On obtient bien $B = A$ par inclusion et égalité des cardinaux. $\square$

Considérons maintenant p, q premiers impairs distincts, et Ω une clôture algébrique de $\mathbb{F}_p$. On pose $\omega \in \Omega$ une racine q-ème de l'unité dans Ω avec $\omega \neq 1$ et

$$y := \sum_{x \in \mathbb{F}_q} \left(\frac{x}{q}\right) \omega^x \in \Omega$$

Ceci a bien un sens, l'application $\mathbb{Z} \to \Omega$ envoyant k sur ω^k passe au quotient par $q\mathbb{Z}$ car $\omega^q = 1$ (c'est une racine q-ème de l'unité.
Calculons y^2 :

$$\begin{aligned} y^2 &= \left(\sum_{x \in \mathbb{F}_q} \left(\frac{x}{q}\right) \omega^x\right)\left(\sum_{x \in \mathbb{F}_q} \left(\frac{x}{q}\right) \omega^x\right) \\ &= \sum_{(x,z) \in \mathbb{F}_q} \left(\frac{xz}{q}\right) \omega^{x+z} \\ &= \sum_{u \in \mathbb{F}_q} \omega^u \sum_{t \in \mathbb{F}_q} \left(\frac{t(u-t)}{q}\right) \end{aligned}$$

Comme $\left(\frac{0}{q}\right) = 0$, on a

$$\sum_{t\in\mathbb{F}_q} \left(\frac{t(u-t)}{q}\right) = \sum_{t\in\mathbb{F}_q^*} \left(\frac{t(u-t)}{q}\right) = \sum_{t\in\mathbb{F}_q^*} \left(\frac{-1}{q}\right)\left(\frac{t^2}{q}\right)\left(\frac{1-ut^{-1}}{q}\right) = (-1)^{\frac{q-1}{2}} \sum_{t\in\mathbb{F}_q^*} \left(\frac{1-ut^{-1}}{q}\right)$$

D'où

$$(-1)^{\frac{q-1}{2}} y^2 = \sum_{u\in\mathbb{F}_q} \omega^u C_u$$

en posant $C_u = \sum_{t\in\mathbb{F}_q^*} \left(\frac{1-ut^{-1}}{q}\right)$. Si $u = 0$, alors $C_0 = \sum_{t\in\mathbb{F}_q^*} \left(\frac{1}{q}\right) = q-1$, sinon $s = 1 - ut^{-1}$ décrit $\mathbb{F}_q \setminus \{1\}$ quand t décrit $\mathbb{F}_q^*$, d'où

$$C_u = \sum_{s\in\mathbb{F}_q\setminus\{1\}} \left(\frac{s}{q}\right) = \sum_{s\in\mathbb{F}_q} \left(\frac{s}{q}\right) - \left(\frac{1}{q}\right) = (-1) \times \frac{q-1}{2} + \frac{q-1}{2} - \left(\frac{1}{q}\right) = -\left(\frac{1}{q}\right) = -1$$

Ainsi, on obtient

$$(-1)^{\frac{q-1}{2}} y^2 = q - 1 - \sum_{u\in\mathbb{F}_q^*} \omega^u = q - 1 + 1 = q$$

car ω est une racine q-ème de l'unité (polynôme cyclotomique : $\Phi_q = 1 + X + \cdots + X^{q-1}$). Montrons ensuite que $y^{p-1} = \left(\frac{p}{q}\right)$: on a (morphisme de Frobenius)

$$\begin{aligned} y^p = \left(\sum_{x\in\mathbb{F}_p} \left(\frac{x}{q}\right)\omega^x\right)^p &= \sum_{x\in\mathbb{F}_q} \left(\frac{x}{q}\right)\omega^{xp} \\ &= \sum_{z\in\mathbb{F}_q} \left(\frac{zp^{-1}}{q}\right)\omega^z \\ &= \sum_{z\in\mathbb{F}_q} \left(\frac{z}{q}\right)\left(\frac{p^{-1}}{q}\right)\omega^z \\ &= \sum_{z\in\mathbb{F}_q} \left(\frac{z}{q}\right)\left(\frac{p}{q}\right)\omega^z \\ &= \left(\frac{p}{q}\right) y \end{aligned}$$

Donc $y^{p-1} = \left(\frac{p}{q}\right)$, on obtient enfin

$$\begin{aligned} \left(\frac{p}{q}\right) = y^{p-1} &= (y^2)^{\frac{p-1}{2}} \\ &= \left((-1)^{\frac{q-1}{2}} q\right)^{\frac{p-1}{2}} \\ &= (-1)^{\frac{(q-1)(p-1)}{4}} q^{\frac{p-1}{2}} \\ &= (-1)^{\frac{(q-1)(p-1)}{4}} \left(\frac{q}{p}\right) \end{aligned}$$

Ce qui clos la démonstration.