Loi de réciprocité quadratique

Théorème 1 (Réciprocité quadratique)**.** *Soient p et q deux premiers distincts impairs, alors :*

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

Démonstration.

Soit Ω une clôture algébrique de $\mathbb{F}_p$, et soit $\omega \in \Omega$ une racine primitive q-ième de l'unité.
On peut donc définir :

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

Calculons y^2 :

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

$$y^2 = \sum_{u\in\mathbb{F}_q}\omega^u\sum_{t\in\mathbb{F}_q^\star}\left(\frac{t(u-t)}{q}\right) = \sum_{u\in\mathbb{F}_q}\omega^u\sum_{t\in\mathbb{F}_q^\star}\left(\frac{-t^2(1-ut^{-1})}{q}\right) = \sum_{u\in\mathbb{F}_q}\omega^u\sum_{t\in\mathbb{F}_q^\star}\underbrace{\left(\frac{-1}{q}\right)}_{=(-1)^{\frac{q-1}{2}}}\underbrace{\left(\frac{t^2}{q}\right)}_{=1}\left(\frac{1-ut^{-1}}{q}\right)$$

Finalement : $y^2 = (-1)^{\frac{q-1}{2}}\sum_{u\in\mathbb{F}_q}\omega^u\sum_{t\in\mathbb{F}_q^\star}\left(\frac{1-ut^{-1}}{q}\right)$.
Ainsi, en posant $c_u = \sum\limits_{t\in\mathbb{F}_q^\star}\left(\frac{1-ut^{-1}}{q}\right)$, on a $y^2 = \sum\limits_{u\in\mathbb{F}_q}\omega^u c_u$.

Calculons maintenant c_u :

$$c_0 = \sum_{t\in\mathbb{F}_q^\star}\left(\frac{1}{q}\right) = |\mathbb{F}_q^\star| = q-1$$

De plus, pour $u \neq 0$, posons $s = 1-ut^{-1} \in \mathbb{F}_q \setminus \{1\}$, alors :

$$c_u = \sum_{s\in\mathbb{F}_q\setminus\{1\}}\left(\frac{s}{q}\right) = \sum_{s\in\mathbb{F}_q}\left(\frac{s}{q}\right) - \left(\frac{1}{q}\right) = \sum_{s\in\mathbb{F}_q^\star}\left(\frac{s}{q}\right) - 1 = -1$$

En effet, il y a $\frac{p-1}{2}$ éléments de $\mathbb{F}_q^\star$ qui sont des carrés, et autant qui ne le sont pas.
La somme est donc nulle par définition du symbole de Legendre.

On obtient donc :

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

Ainsi, $y^2 = (-1)^{\frac{q-1}{2}}q$.

Calculons maintenant y^{p-1} :

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

$$y^{p-1} = y^{-1}\sum_{z\in\mathbb{F}_q}\left(\frac{z}{q}\right)\left(\frac{p^{-1}}{q}\right)\omega^z = y^{-1}\left(\frac{p}{q}\right)^{-1}\sum_{z\in\mathbb{F}_q}\left(\frac{z}{q}\right)\omega^z = y^{-1}\left(\frac{p}{q}\right)y = \left(\frac{p}{q}\right)$$

Ainsi :

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

On obtient alors le résultat voulu :

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

□

Références

[Ser] Jean-Pierre Serre. *Cours d'Arithmétiques.* PUF