I.B Loi de la réciprocité quadratique

Théorème 2: Loi de la réciprocité quadratique

Pour tous p et q nombre premiers impairs distaincts, on a :

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

Démonstration. On calcule de deux manières différentes le cardinal de : $X = \{x = (x_1, \dots, x_p) \in \mathbb{F}_q \quad / \quad x_1^2 + \cdots + x_p^2 = 1\}$.

1. On fait agir $\mathbb{Z}/p\mathbb{Z}$ sur X par translation. On a une action naturelle de $\mathbb{Z}/p\mathbb{Z}$ sur $\mathbb{F}_q$ par translation, on restreint alors simplement cette action. La relation stabilisateur orbite fournit que le cardinal d'une orbite divise le cardinal du groupe qui agit, i.e. p. Les orbites ont donc 1 élément ou p.

   On s'intéresse aux orbites à 1 élément. Il y a $1 + \left(\frac{p}{q}\right)$ orbite(s) à 1 élément. En effet les orbites à 1 élément vérifient $x_1 = x_2 = \cdots = x_p$ et $px_1^2 = 1$. Or cette dernière équation a 0 solution si p n'est pas un carré modulo q et en a 2 sinon.

   Alors l'équation aux classes nous donne que $\#X = 1 + \left(\frac{p}{q}\right) \mod p$

2. On considère maintenant les deux matrices suivantes :

$$A = \begin{pmatrix} 0 & 1 & & & & \\ 1 & 0 & & & & \\ & & \ddots & & & \\ & & & 0 & 1 & \\ & & & 1 & 0 & \\ & & & & & a \end{pmatrix} \in \mathcal{M}_p(\mathbb{F}_q) \qquad \text{et} \qquad I_p = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix} \in \mathcal{M}_p(\mathbb{F}_q)$$

   où $a = (-1)^{p-1}$.

   Elles sont toutes deux symétriques donc représentent deux forment quadratiques sur $\mathbb{F}_q$. Or elles ont même rang et même déterminant (donc a fortiori même discriminant). Par le théorème de classification des forment quadratiques sur les corps finis, les deux matrices sont congruentes.

   Soit alors $P \in \mathrm{GL}_p(\mathbb{F}_q)$ tel que $I_p = {}^tPAP$.
   On peut alors écrire :

$$\begin{aligned} X &= \{x \in \mathbb{F}_q \quad / \quad {}^txx = 1\} \\ &= \{x \in \mathbb{F}_q \quad / \quad {}^txI_px = 1\} \\ &= \{P^{-1}x \in \mathbb{F}_q \quad / \quad {}^tx\,{}^tPI_pPx = 1\} \\ &= \{P^{-1}x \in \mathbb{F}_q \quad / \quad {}^txAx = 1\} \\ &= P^{-1}\{x \in \mathbb{F}_q \quad / \quad {}^txAx = 1\} \end{aligned}$$

   Donc X est en bijection avec

   $\{x \in \mathbb{F}_q \quad / \quad {}^txAx = 1\} = \{x = (y_1, z_1, y_2, z_2, \dots, y_q, z_d, t) \in \mathbb{F}_q \quad / \quad 2(y_1z_1 + \cdots + y_dz_d) + at^2 = 1\}$

   où $d = \frac{p-1}{2}$

   On compte le nombre d'élément de ce dernier ensemble.

— Si tous les y_i sont nuls, alors on choisit les z_i comme on veut dans $\mathbb{F}_q$ (il y a q^q choix) et l'équation $at^2 = 1$ a $1 + \left(\frac{a}{q}\right) = 1 + a^{\frac{q-1}{2}} = 1 + (-1)^{\frac{q-1}{2}\frac{p-1}{2}}$ solutions.

— l'un au moins des y_i est non nul (il y a $q^d - 1$ choix) et on fixe t (il y a q choix). Alors on obtient l'équation d'un hyperplan de $\mathbb{F}_q^d$. Il y a donc q^{d-1} choix pour les z_i.

Au total, on obtient :

$$\begin{aligned}\#X &= q^d \times \left(1 + (-1)^{\frac{q-1}{2}\frac{p-1}{2}}\right) + \left(q^d - 1\right) \times q \times q^{d-1} \\ &= q^d \times \left(q^d + (-1)^{\frac{q-1}{2}\frac{p-1}{2}}\right) \\ &= q^{p-1} + (-1)^{\frac{q-1}{2}\frac{p-1}{2}} \times q^d\end{aligned}$$

3. Au total :

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

Or $q^{p-1} = 1 \mod p$. Et part la formule d'Euler, on a : $q^{\frac{p-1}{2}} = \left(\frac{q}{p}\right)$.

On obtient donc ainsi le résultat annoncé mais modulo p. Or comme $p \neq 2$ et que les deux membres de l'égalité valent ± 1 dans $\mathbb{Z}$, on peut remonter cette égalité dans $\mathbb{Z}$, ce qui conclut.

■