Loi de réciprocité quadratique

Leçons 120,121,170

Dans tout ce qui suit, p et q sont deux nombres premier supérieurs ou égaux à 3, tels que p ne soit pas congru à 0 modulo q et vice-versa.

Définition (Symbole de Legendre)

On définit le **symbole de Lgendre** de p et q, noté $\left(\frac{p}{q}\right)$ par:

$$\left(\frac{p}{q}\right) = \begin{cases} 1 & \text{si} \quad x \in \left(\mathbb{F}_q^\times\right)^2 \ (\text{est un carré modulo } q) \\ 0 & \text{si} \quad x \equiv 0 \ [q] \\ -1 & \text{sinon} \end{cases}$$

Théorème (Loi de réciprocité quadratique)

Le symbole de Legendre vérifie cette propriété, dite **loi de réciprocité quadratique**:

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

Voici le plan de la démonstration:

1. Compter l'ensemble:
$$X = \left\{(x_1, \cdots, x_p) \in \mathbb{F}_q^p : x_1^2 + \cdots + x_p^2 = 1\right\}$$
modulo q via l'action de $\frac{\mathbb{Z}}{p\mathbb{Z}}$ sur X.

2. Compter l'ensemble:
$$X' = \left\{(x_1, \cdots, x_p) \in \mathbb{F}_q^p : 2(x_1x_2 + x_3x_4 + \cdots + x_{p-2}x_{p-1}) + ax_p^2 = 1\right\}$$
où $a = (-1)^{\frac{p-1}{2}}$, en utilisant les propriétés des formes quadratiques, après avoir montré que $X = X'$.

3. Comparer $|X|$ et $|X'|$ modulo p puis conclure.

Démonstration. *1. $\frac{\mathbb{Z}}{p\mathbb{Z}}$ agit sur X par permutation circulaire via l'action:*

$$\begin{array}{ccc} \frac{\mathbb{Z}}{p\mathbb{Z}} \times X & \longrightarrow & X \\ (\overline{n}, (x_{\overline{1}}, \cdots, x_{\overline{p}})) & \longmapsto & (x_{\overline{1+n}}, \cdots, x_{\overline{p+n}}) \end{array}$$

D'après la relation orbite-stabilisateur, il y a deux types d'orbites, puisque $|\mathcal{O}_x| \cdot |Stab_x| = \left|\frac{\mathbb{Z}}{p\mathbb{Z}}\right| = p \Rightarrow |\mathcal{O}_x| \in \{1, p\}$:

⋆ *Les orbites de taille p, dont le stabilisateur est trivial.*

⋆ *Les orbites de taille 1, i.e. de la forme $(x, \cdots, x)$ avec $px^2 = 1$ dans $\mathbb{F}_q$, de stabilisateur $\frac{\mathbb{Z}}{p\mathbb{Z}}$.*

Il y a autant d'orbites de taille 1 que de solutions à l'équation $px^2 = 1$ dans $\mathbb{F}_q$, soit $1 + \left(\frac{p}{q}\right)$.

En vertu de l'équation aux classes, on a: $|X| \equiv 1 + \left(\frac{p}{q}\right) \quad [p]$.

2. *On pose $a = (-1)^{\frac{p-1}{2}}$ et on considère notre ensemble X' donné par:*

$$X' = \left\{(x_1, \cdots, x_p) \in \mathbb{F}_q^p : Q(x_1, \cdots, x_p) := 2(x_1x_2 + \cdots + x_{p-2}x_{p-1}) + ax_p^2 = 1\right\}$$

La matrice de Q dans la base canonique est donnée par:

$$\begin{bmatrix} 0 & 1 & & & & \\ 1 & 0 & & & (0) & \\ & & \ddots & & & \\ & (0) & & 0 & 1 & \\ & & & 1 & 0 & \\ & & & & & a \end{bmatrix}$$

La classification des formes quadratiques non-dégénérées sur un corps fini assure que la matrice de Q dans une bonne base est I_p ou diag $\{1, \cdots, 1, \alpha\}$ où $\alpha \in \mathbb{F}_q$ n'est pas un carré. Or, le discriminant de Q vaut 1 par construction (le déterminant de la matrice vaut $(-1)^{\frac{p-1}{2}} \cdot a = (-1)^{p-1} = 1$), donc on en déduit que la matrice de Q est I_p dans une bonne base, d'où $X = X'$.

On va maintenant dénombrer X'. Soit $(x_1, \cdots, x_p) \in X'$:

⋆ ***Cas 1:** $(x_1, x_3, \cdots, x_{p-2}) = (0, \cdots, 0)$, la condition devient alors $ax_p^2 = 1$, et il y a $1 + \left(\frac{a}{q}\right)$ solutions pour x_p, et $q^{\frac{p-1}{2}}$ pour $(x_2, x_4, \cdots, x_{p-1})$, donc, en multipliant, on a $q^{\frac{p-1}{2}}\left(1 + \left(\frac{a}{q}\right)\right)$ solutions.*

⋆ ***Cas 2:** $(x_1, x_3, \cdots, x_{p-2}) \neq (0, \cdots, 0)$. On fixe alors $(x_1, x_3, \cdots, x_{p-2})$ ($q^{\frac{p-1}{2}} - 1$ solutions, le vecteur nul étant exclu, d'où le "-1") et on fixe également x_p (q solutions). L'équation $Q(x_1, x_2, \cdots, x_{p-2}, x_{p-1}, x_p) = 1$ devient celle d'un hyperplan affine dans un espace vectoriel de dimension $\frac{p-1}{2}$ sur un corps de cardinal q, donnant ainsi $q^{\frac{p-1}{2}-1}$ solutions. Finalement, en multipliant tous les nombres de solutions, on obtient $q \cdot \left(q^{\frac{p-1}{2}-1}\right) \cdot \left(q^{\frac{p-1}{2}} - 1\right) = q^{\frac{p-1}{2}} \cdot \left(q^{\frac{p-1}{2}} - 1\right)$ solutions.*

Ainsi, pour calculer $|X'|$, on additionne le nombre de solutions pour chaque cas et on en déduit que:

$$|X'| \;=\; q^{\frac{p-1}{2}}\left(1 + \left(\frac{a}{q}\right)\right) + q^{\frac{p-1}{2}} \cdot \left(q^{\frac{p-1}{2}} - 1\right)$$

3. On étudie $|X|$ et $|X'|$ modulo p:

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

$$\textit{Donc:} \quad q^{\frac{p-1}{2}}\left(1 + \left(\frac{a}{q}\right)\right) + q^{\frac{p-1}{2}} \cdot \left(q^{\frac{p-1}{2}} - 1\right) \equiv 1 + \left(\frac{p}{q}\right) \quad [p]$$

Or, pour tout $x \in \mathbb{F}_q$, $\left(\frac{x}{q}\right) = x^{\frac{q-1}{2}}$ (résultat donné par le théorème de Lagrange)

$$\textit{D'où:} \quad q^{\frac{p-1}{2}}\left(1 + a^{\frac{q-1}{2}}\right) + \underbrace{q^{p-1}}_{\equiv 1 \ [p] \ (\textit{Th. de Lagrange})} - q^{\frac{p-1}{2}} \equiv 1 + \left(\frac{p}{q}\right) \quad [p]$$

Puisque $a = (-1)^{\frac{p-1}{2}}$, on a:

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

$$\textit{D'où:} \quad \left(\frac{q}{p}\right)(-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)} \equiv \left(\frac{p}{q}\right) \quad [p]$$

Les entiers en question valant -1, 0 ou 1, le résultat est valable de manière générale (et plus seulement modulo p), donnant ainsi:

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

■