

Def (symbole de LEGENDRE) : Soit p un nombre premier impair. Pour $x \in \mathbb{Z}$, on définit le symbole de LEGENDRE de x en p comme
$$\left(\frac{x}{p}\right) = \begin{cases} 1 & \text{si } x \text{ est un carré non nul modulo } p \\ 0 & \text{si } x \equiv 0 \pmod{p} \\ -1 & \text{sinon} \end{cases}$$
. On remarque que la valeur de $\left(\frac{x}{p}\right)$ ne dépend que de la classe de x modulo p : on définit alors pour $x \in \mathbb{F}_p$:
$$\left(\frac{x}{p}\right) = \begin{cases} 1 & \text{si } x \in \mathbb{F}_p^{\times(2)} := \{y^2 : y \in \mathbb{F}_p^{\times}\} \\ 0 & \text{si } x = 0 \\ -1 & \text{sinon} \end{cases}$$
.

Lemme : Soit q un entier premier impair. Pour tout $a \in \mathbb{F}_q^{\times}$:

$$1 \triangleright \left(\frac{a}{q}\right) \bmod q = a^{\frac{q-1}{2}}$$

$$2 \triangleright \#\{x \in \mathbb{F}_q^{\times} \mid ax^2 = 1\} = 1 + \left(\frac{a}{q}\right)$$

Thm (loi de réciprocité quadratique) : Soient p et q deux entiers premiers impairs. Alors
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}.$$

Preuve du lemme : 1 $\triangleright$ Remarquons que $a^{\frac{q-1}{2}}$ est racine de $X^2 - 1$ d'après le théorème de LAGRANGE, donc $a^{\frac{q-1}{2}} \in \{\pm 1\}$.
S'il existe $b \in \mathbb{F}_q^{\times}$ tel que $a = b^2$, alors $a^{\frac{q-1}{2}} = b^{q-1} = 1 = \left(\frac{a}{q}\right) \bmod q$. Réciproquement, si $a^{\frac{q-1}{2}} = 1$, alors a est racine de $X^{\frac{q-1}{2}} - 1$, lequel a au plus $\frac{q-1}{2}$ racines. Or les $\frac{q-1}{2}$ carrés de $\mathbb{F}_q^{\times}$ (*) sont racines de $X^{\frac{q-1}{2}} - 1$, donc on a trouvé toutes les racines de ce polynôme, et donc a est un carré. Ainsi, si a n'est pas un carré, i.e. $\left(\frac{a}{q}\right) = -1$, alors $a^{\frac{q-1}{2}} = -1 = \left(\frac{a}{q}\right) \bmod q$.

2 $\triangleright$ S'il existe $b \in \mathbb{F}_q^{\times}$ tel que $a = b^2$, alors $\forall x \in \mathbb{F}_q^{\times}, ax^2 = 1 \Leftrightarrow (bx)^2 = 1 \Leftrightarrow bx = \pm 1 \Leftrightarrow x = \pm b^{-1}$, et $q \neq 2$ donc $-b^{-1} \neq +b^{-1}$, donc $\#\{x \in \mathbb{F}_q^{\times} \mid ax^2 = 1\} = 2 = 1 + 1 = 1 + \left(\frac{a}{q}\right)$.

Sinon, pour tout $x \in \mathbb{F}_q^{\times}$, $\left(\frac{ax^2}{q}\right) \bmod q = (ax^2)^{\frac{q-1}{2}} = a^{\frac{q-1}{2}} x^{q-1} = a^{\frac{q-1}{2}} = \left(\frac{a}{q}\right) \bmod q = -1 \bmod q$, donc $\left(\frac{ax^2}{q}\right) = -1$ et donc ax^2 n'est pas un carré, a fortiori $ax^2 \neq 1$. Ainsi, $\#\{x \in \mathbb{F}_q^{\times} \mid ax^2 = 1\} = 0 = 1 - 1 = 1 + \left(\frac{a}{q}\right)$.

Preuve du Thm : Posons $X := \{x = (x_1, \dots, x_p) \in \mathbb{F}_p^p \mid \sum_{k=1}^p x_k^2 = 1\}$.

$\triangleright$ On fait agir $\mathbb{F}_p$ sur X par $\bar{1} \cdot x = (x_2, x_3, \dots, x_p, x_1)$. D'après la relation orbite-stabilisateur, pour tout $x \in X$, $p = \#\mathbb{F}_p = \#\text{Orb}(x) \#\text{Stab}(x)$, donc $\#\text{Orb}(x) \in \{1, p\}$. Or $\text{Orb}(x) = \{x\}$ si, et seulement si $x_1 = \dots = x_p$ et $\sum_{k=1}^p x_k^2 = 1$, i.e. $px_1^2 = 1$. D'après le Lemme, il y a $1 + \left(\frac{p}{q}\right)$ tels $x \in X$. Or $\#X^{\mathbb{F}_p} \equiv \#X \bmod p$ (†), et $X^{\mathbb{F}_p} = \{x \in X \mid \text{Orb}(x) = \{x\}\}$, donc $\#X \equiv 1 + \left(\frac{p}{q}\right) \bmod p$.

$\triangleright$ Notons $f : (x_1, \dots, x_p) \mapsto \sum_{k=1}^p x_k^2$ la forme quadratique de matrice I_p dans la base canonique. Posons $d = \frac{p-1}{2}$.
Posons $M = \text{Diag}(J, \dots, J, a) \in \mathcal{M}_p(\mathbb{F}_q)$ par blocs, où $J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ est répétée d fois, et $a = (-1)^d$. On en déduit que $\text{rg}(M) = dx + 1 = p$ et $\det(M) = a \det(J)^d = (-1)^d (-1)^d = 1$. Notons g la forme quadratique de matrice M dans la base canonique : d'après la classification des formes quadratiques non dégénérées sur $\mathbb{F}_q$ (†), f et g sont congruentes, i.e. il existe $\varphi \in GL(\mathbb{F}_q^p)$ telle que $f = g \circ \varphi$. De là, $X = f^{-1}(\{1\}) = (g \circ \varphi)^{-1}(\{1\}) = \varphi^{-1}(g^{-1}(\{1\}))$, et φ^{-1} étant bijective, $\#X = \#X'$ où $X' = g^{-1}(\{1\}) = \{x = (x_1, \dots, x_p) \in \mathbb{F}_q^p \mid 2 \sum_{k=1}^d x_{2k} x_{2k-1} + ax_p^2 = 1\}$. Pour tout $x \in X'$,
 $\triangleright$ Soit $(x_{2k-1})_{1 \leq k \leq d} = (0, \dots, 0)$ et $ax_p^2 = 1$, alors il y a d'après le Lemme $1 + \left(\frac{a}{q}\right)$ possibilités pour x_p et q^d choix pour $(x_{2k})_{1 \leq k \leq d}$. Il y a donc $q^d \left[1 + \left(\frac{(-1)^d}{q}\right)\right]$ possibilités pour x .

$\triangleright$ Soit $(x_{2k-1})_{1 \leq k \leq d} \neq (0, \dots, 0)$, alors il y a $(q^d - 1)$ possibilités pour $(x_{2k-1})_{1 \leq k \leq d}$, q choix pour x_p ,

et $(x_{2k})_{1 \leq k \leq d}$ doit être pris dans l'hyperplan affine d'équation $2 \sum_{k=1}^d x_{2k-1} x_{2k} = 1 - \alpha x_p^2$: il y a donc q^{d-1} possibilités. In fine, il y a $q^{d-1} \cdot q(q^d-1) = q^d(q^d-1)$ possibilités pour x .

Ainsi, $\#X' = q^d \left(1 + \left(\frac{(-1)^d}{q}\right)\right) + q^d(q^d-1) = q^d \left(q^d + \left(\frac{(-1)^d}{q}\right)\right) = \#X$. Finalement, en rappelant que $\left(\frac{x}{p}\right) \equiv x^{\frac{p-1}{2}} \equiv x^d \pmod{p}$:

$$1 + \left(\frac{p}{q}\right) \equiv q^d \left(q^d + \left(\frac{(-1)^d}{q}\right)\right) \equiv (q^2)^d + \left(\frac{q}{p}\right) \left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right) \equiv \left(\frac{q^2}{p}\right) + \left(\frac{q}{p}\right) \left[(-1)^{\frac{p-1}{2}}\right]^{\frac{q-1}{2}} \stackrel{q \not\equiv 0 [p]}{=} 1 + \left(\frac{q}{p}\right) (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \pmod{p}$$

donc $\left(\frac{p}{q}\right) \equiv \left(\frac{q}{p}\right) (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \pmod{p}$, donc $\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) \equiv \left(\frac{q}{p}\right)^2 (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \equiv \left(\frac{q^2}{p}\right) (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \equiv 1 \cdot (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \pmod{p}$.

Or $\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) \in \{\pm 1\}$, donc $\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}$.

ANNEXE:

(*) : (Montrons un tout petit peu plus, parce que c'est vraiment gratuit.)

Posons $c: \mathbb{F}_q^* \rightarrow \mathbb{F}_q^*$, $x \mapsto x^2$ et $l: \mathbb{F}_q^* \rightarrow \mathbb{F}_q^*$, $x \mapsto x^{\frac{q-1}{2}}$. D'après le théorème de LAGRANGE, $\text{col} = \text{loc} = 1$, donc $\text{Im}(c) \subseteq \text{Ker}(l)$ et $\text{Im}(l) \subseteq \text{Ker}(c)$. On a justifié dans le développement que $\text{Im}(l) = \{\pm 1\}$, $\text{Ker}(c) = \{\pm 1\}$ et $\#\text{Im}(c) = \frac{q-1}{2}$. Comme $q-1 = \#\mathbb{F}_q^* = \#\text{Ker}(c) + \#\text{Im}(c) = \#\text{Ker}(l) + \#\text{Im}(l)$, on en déduit que $\#\text{Ker}(l) = \#\text{Im}(c) = \frac{q-1}{2}$ (et en particulier, $\text{Ker}(c) = \text{Im}(l)$ et $\text{Ker}(l) = \text{Im}(c)$). Or les carrés de $\mathbb{F}_q^*$ sont les éléments de $\text{Im}(c)$: on a bien montré qu'il y en a $\frac{q-1}{2}$.

(†) : D'après l'équation aux classes et la relation orbite-stabilisateur,

$$\#X = \sum_{i=1}^r \#\text{Orb}(x_i) = \sum_{\substack{i=1 \\ \text{Orb}(x_i) = \{x_i\}}}^r \#\{x_i\} + \sum_{\substack{i=1 \\ \#\text{Orb}(x_i) > 1}}^r \frac{\#\mathbb{F}_p}{\#\text{Stab}(x_i)} \equiv \#X^{\mathbb{F}_p} + 0 \pmod{p}$$

Car $\text{Stab}(x_i)$ est un sous-groupe de $\mathbb{F}_p$, donc d'après le théorème de LAGRANGE, $\#\text{Stab}(x_i) \mid \#\mathbb{F}_p = p$, mais $\#\text{Orb}(x_i) > 1 \Leftrightarrow \#\text{Stab}(x_i) < \#\mathbb{F}_p \Leftrightarrow \#\text{Stab}(x_i) = 1$.

(‡) : Deux formes quadratiques non dégénérées (i.e. de rang maximal) sont congruentes si, et seulement si elles ont le même discriminant.

COMMENTAIRES:

► Cas $p=2, q>2$: on a $q \equiv 1 [2]$ donc $\left(\frac{q}{2}\right) = 1$. Montrons que $\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}}$: soit K le corps de décomposition de X^4+1 sur $\mathbb{F}_q$. On note σ une racine de X^4+1 dans K . En particulier, $\sigma^4+1=0$ donc $\sigma^2+\sigma^{-2}=0$, donc $(\sigma+\sigma^{-1})^2=2$. Posons $\tau = \sigma + \sigma^{-1}$, de sorte que $\tau^{p-1} = (\tau^2)^{\frac{p-1}{2}} = 2^{\frac{p-1}{2}} = \left(\frac{2}{p}\right)$. Or $\text{car}(K)=p$, $\tau^p = \sigma^p + \sigma^{-p}$.

► Si $p \equiv \pm 1 [8]$, alors $\tau = \tau^p = \tau \left(\frac{2}{p}\right)$ donc $\left(\frac{2}{p}\right) = 1 = (-1)^{\frac{p^2-1}{8}}$.

► Si $p \equiv \pm 3 [8]$, alors $-\tau = \tau^p = \tau \left(\frac{2}{p}\right)$ donc $\left(\frac{2}{p}\right) = -1 = (-1)^{\frac{p^2-1}{8}}$.

► La loi de réciprocité quadratique, à quoi ça sert ?

► À déterminer si un entier est premier dans un anneau d'entiers de corps de nombres

(exemple: p est premier dans $\mathbb{Z}[i] \Leftrightarrow \frac{\mathbb{Z}[i]}{\langle p \rangle}$ est intègre $\Leftrightarrow \frac{\mathbb{F}_p[X]}{\langle X^2+1 \rangle}$ est intègre $\Leftrightarrow X^2+1$ est premier dans $\mathbb{F}_p[X] \Leftrightarrow X^2+1$ est irréductible dans $\mathbb{F}_p[X] \Leftrightarrow -1$ n'est pas un carré mod $p \Leftrightarrow \left(\frac{-1}{p}\right) = -1$)

► À tester la non-primauté d'un entier (mais c'est très peu efficace...)

► À résoudre des équations diophantiennes (il paraît)

► À connaître le discriminant d'une forme quadratique (selon si son déterminant est un carré mod p).