

* Réciprocité quadratique (par les formes quadratiques): degrés 101, 170, 180, 221, 223 [NH₂G₂] V C

On rappelle l'énoncé (dans une autre version du développement):

Th:

Soient p et p' deux entiers premiers impairs distincts.

Alors:

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

démontre:

Soit p premier impair et $a \in \mathbb{F}_p^\times$.

Alors:

$$|\{x \in \mathbb{F}_p^\times, ax^2 = 1\}| = 1 + \left(\frac{a}{p}\right)$$

preuve du lemme:

$$\begin{aligned} \{x \in \mathbb{F}_p^\times, ax^2 = 1\} &= \{x \in \mathbb{F}_p^\times, x^2 = a^{-1}\} \\ &= \begin{cases} \pm \delta^{-1} & \text{si } a = \delta^2 \in (\mathbb{F}_p^\times)^2 \\ \emptyset & \text{sinon} \end{cases} \end{aligned}$$

On obtient bien le résultat car $\text{car}(\mathbb{F}_p) = p \neq 2$.

preuve du th:

On note dans la suite $d = \frac{p-1}{2}$ et $d' = \frac{p'-1}{2}$.

On note également $X = \{(x_1, \dots, x_p) \in \mathbb{F}_p^{\oplus p}, \sum_{i=1}^p x_i^2 = 1\}$ la "sphère unité" de $\mathbb{F}_p^{\oplus p}$.

On va calculer $|X|$ de deux manières différentes.

* d'q $|X| \equiv \left(\frac{p}{p'}\right) + 1 \pmod{p}$.

On fait agir $G = \mathbb{Z}/p\mathbb{Z}$ par permutation cyclique sur X : $h(x_1, \dots, x_p) = (x_2, \dots, x_p, x_1)$.

G est un p -groupe, donc par la formule du degré: $|X| \equiv |X^G| \pmod{p}$.

Soit $(x_1, \dots, x_p) \in X$. $(x_1, \dots, x_p) \in X^G \Leftrightarrow \forall k \in \mathbb{Z}/p\mathbb{Z}: k.(x_1, \dots, x_p) = (x_1, \dots, x_p)$

$$\Leftrightarrow x_1 = \dots = x_p.$$

Donc: $X^G = \{x \in \mathbb{F}_p^d, px^2 = 1\}$ et donc $|X^G| = 1 + \binom{d}{p}$ par le lemme.

↳ On a bien: $|X| = 1 + \binom{d}{p} (p)$ (*)

* d/q $|X| = (p^d + (-1)^{dd'}) (p')^d$:

Soit q la forme quadratique sur $\mathbb{F}_p^{2d'}$ associée à la matrice I_p .

On a: $X = \{u \in \mathbb{F}_p^{2d'}, q(u) = 1\}$

Soit maintenant $\tilde{q}$ la forme quadratique dont la matrice dans la base canonique est:

$$A = \begin{pmatrix} 0 & Id \\ Id & 0 \end{pmatrix} a \in M_p(\mathbb{F}_p) \quad \text{avec } a = (-1)^d.$$

En faisant d échanges de colonnes sur le bloc $\begin{pmatrix} 0 & Id \\ Id & 0 \end{pmatrix}$, on tombe sur Id .

Ainsi: $\det(A) = (-1)^d a = (-1)^{2d} = 1$

En particulier, A a le même rang et le même discriminant (réduit) que I_p . Par le

théorème de classification des formes quadratiques sur un corps fini, on a:

les espaces $(\mathbb{F}_p^{2d'}, q)$ et $(\mathbb{F}_p^{2d'}, \tilde{q})$ sont isomorphes.

En particulier, X est en bijection avec $\tilde{X} = \{u \in \mathbb{F}_p^{2d'}, \tilde{q}(u) = 1\}$
 $= \{u = (y_1, y_d, z_1, z_d, t) \in \mathbb{F}_p^{2d'}, y_1^2 + \dots + y_d^2 + z_1^2 + \dots + z_d^2 + at^2 = 1\}.$

• d/q $|\tilde{X} \cap \{y_1 = \dots = y_d = 0\}| = (p')^d (1 + (-1)^{dd'})$:

On a: $(0, \dots, 0, z_1, \dots, z_d, t) \in \tilde{X} \Leftrightarrow at^2 = 1$

Donc: $\tilde{X} \cap \{y_1 = \dots = y_d = 0\}$ est en bij. avec $\{t \in \mathbb{F}_p^x, at^2 = 1\} \times \mathbb{F}_p^{d'}$ qui est de cardinal $(p')^d (1 + \frac{a}{p}) = (p')^d (1 + (-1)^{dd'})$ grâce au lemme.

• d/q $|\tilde{X} \cap \{y_1 = \dots = y_d = 0\}^c| = (p')^d (p')^d - 1$:

Pour construire un élément de $\tilde{X} \cap \{y_1 = \dots = y_d = 0\}^c$, on choisit d'abord les y_i (on a $(p')^d - 1$ choix) et on choisit ensuite t (on a p' choix). Ensuite, on choisit $z_1, \dots, z_d$ dans l'hyperplan affine $\{y_1^2 + \dots + y_d^2 + z_1^2 + \dots + z_d^2 + at^2 = 1\}$ de $\mathbb{F}_p^{2d'}$ on a $(p')^{d-1}$ choix pour les z_i .

Ainsi, on a bien: $|\tilde{X} \cap \{y_1 = \dots = y_d = 0\}^c| = (p')^d ((p')^d - 1)$

→ Finalement, on a: $|X| = |\tilde{X}| = (p')^d (1 + (-1)^{dd'}) + (p')^d ((p')^d - 1) = (p')^d ((p')^d + (-1)^{dd'})$

Or, dans $\mathbb{F}_p$, on a $(p')^d = (p')^{\frac{p-1}{2}}$

$$= \left(\frac{p'}{p}\right) \quad \text{car } p' \in \mathbb{F}_p^\times$$

Donc: $|X| = \left(\frac{p'}{p}\right) \left(\left(\frac{p'}{p}\right) + (-1)^{dd'}\right) [p]$

Donc, par (*):

$$\left(\frac{p'}{p}\right) \left(\left(\frac{p'}{p}\right) + (-1)^{dd'}\right) = 1 + \left(\frac{p'}{p}\right) [p]$$

donc: $\left(\frac{p'}{p}\right) + (-1)^{dd'} = \left(\frac{p'}{p}\right) + \left(\frac{p'}{p}\right) \left(\frac{p'}{p'}\right) [p] \quad \text{car } \left(\frac{p'}{p'}\right) \in \{\pm 1\}$

donc: $(-1)^{dd'} = \left(\frac{p'}{p}\right) \left(\frac{p'}{p'}\right) [p]$

Or, les deux membres valent 1 ou -1 et $p \neq 2$ donc on peut élever l'égalité dans $\mathbb{Z}$.

On a bien: $\left(\frac{p'}{p}\right) \left(\frac{p'}{p'}\right) = (-1)^{dd'} = (-1)^{\frac{p-1}{2} \cdot \frac{p'-1}{2}}$