

Théorème: p, q premiers impairs, $p \neq q$

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

preuve: Double dénombrement

on compte de deux manières $|X|$ où $X = \{(x_1, \dots, x_p) \in \mathbb{F}_q^p \mid \sum_{i=1}^p x_i^2 = 1\}$

• Par action de $\mathbb{Z}/p\mathbb{Z}$ sur X

$$h(x_1, \dots, x_p) \rightarrow (x_{1+p}, \dots, x_{p+p}) \text{ indice mod } p$$

$\forall z \in X$ $\text{Stab}(z)$ ss grp de $\mathbb{Z}/p\mathbb{Z}$, p premier donc

Soit $\text{Stab}(z) = \mathbb{Z}/p\mathbb{Z}$ et dans ce cas $O(z)$ est de la forme $\{(x, \dots, x)\}$ où $x \in \mathbb{F}_q$

Soit $\text{Stab}(z) = \{1\}$

D'après la formule des classes

$$|X| = \sum_{\substack{x \in X \\ x \text{ mod } \mathbb{Z}/p\mathbb{Z}}} \frac{|\mathbb{Z}/p\mathbb{Z}|}{|\text{Stab}(x)|} = \alpha p + \sum_{\substack{x \in X \\ \text{Stab}(x) = \mathbb{Z}/p\mathbb{Z}}} 1$$

nb de sol à $px^2 = 1$

||

$$\left(\frac{p}{q}\right) + 1$$

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

• par les formes quadratiques

$$A = \begin{pmatrix} 0 & 1 & & \\ 1 & 0 & & \\ & & \ddots & \\ & & & 0 \end{pmatrix} \quad \text{à bloc}$$

$$I_p = \begin{pmatrix} 1 & & & \\ & a & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}$$

$$\text{où } a = (-1)^d$$

$$d = \frac{p-1}{2}$$

A et I_p sont de même rang (p) et de même déterminant

$$\det(A) = (-1)^d a = ((-1)^d)^2 = 1 = \det(I_p)$$

A et I_p ont donc le même déterminant et ainsi sont congrues.
(sur $\mathbb{F}_q$)

$\exists P \in GL_p(\mathbb{F}_q) / A = {}^t P J_p P$
 et dans la bijection $u \rightarrow P^{-1}u$ identifie
 $C = \{u, {}^t u u = 1\}$ à $X' = \{u' \in \mathbb{F}_q^p / {}^t u' A u' = 1\}$
 $= \{(y_1, z_1, y_2, z_2, \dots, y_d, z_d, t) \in \mathbb{F}_q^p /$
 $2(y_1 z_1 + \dots + y_d z_d) + a t^2 = 1\}$

On a alors deux cas possibles:

$\triangleright$ Soit $y_1 = y_2 = \dots = y_d = 0$ et dans ce cas
 pour chaque $t / a t^2 = 1$ on a q choix pour chaque z_i
 donc chaque t donne q^d choix
 et on a donc $q^d (1 + \binom{a}{q}) = q^d (1 + a^{\frac{q-1}{2}})$
 $= q^d (1 + (-1)^{\frac{p-1}{2} \frac{q-1}{2}})$
 def de a

$\triangleright \exists i / y_i \neq 0, \Rightarrow q^{d-1}$ choix pour les y_j
 q choix pour t . une fois les y_j et t fixés les z_i
 sont quelconque dans l'hyperplan affine
 $L^{-1}(1 - a t^2)$ ou L est la forme linéaire

$$(z_1, \dots, z_d) \rightarrow 2(y_1 z_1 + \dots + y_d z_d)$$

C'est une s.e.u. de dim $d-1$ on a alors q^{d-1} choix pour
 les z_i ce qui donne au final
 $(a^d - 1) q q^{d-1}$ choix
 $- (q^d - 1) q^d$

(conclusion: $|X| = q^d + q^d (-1)^{\frac{p-1}{2} \frac{q-1}{2}} + q^{d^2} - q^d$
 $= q^d (1 + (-1)^{\frac{p-1}{2} \frac{q-1}{2}}) + q^{d^2} - q^d = q^d (q^d + (-1)^{\frac{p-1}{2} \frac{q-1}{2}})$

et $|X| = \binom{p}{p} + 1 \binom{p}{p} = \binom{p}{q} + 1 \binom{p}{p}$

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

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

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

les deux membres sont ± 1 et $p > 2$ donc

on peut éliminer l'égalité à $\neq$