Loi de réciprocité quadratique

Thm : Soient p et q premiers impairs distincts $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right)$.

Posons $X = \{(x_1, \dots, x_p) \in \mathbb{F}_q^p,\ \sum_{i=1}^{p} x_i^2 = 1\}$.
Calculons le cardinal de X (mod p) de deux manières.

* $\mathbb{F}_p$ agit sur X via $\mathbb{F}_p \longrightarrow \mathfrak{S}_X$
$k \longmapsto [(x_1, \dots, x_p) \mapsto (x_{k+1}, \dots, x_{k+p})]$.

Les orbites sont de deux sortes.
→ les orbites triviales, de stabilisateur $\mathbb{Z}/p\mathbb{Z}$, de la forme $\{(x, \dots, x)\}$ avec $x \in \mathbb{F}_q$ vérifiant $px^2 = 1$
→ les autres orbites, dont le stabilisateur (ss-gp de $\mathbb{Z}/p\mathbb{Z}$) est trivial $\{1\}$.
La formule des classes assure : $|X| = \sum_{px^2=1} 1 + \sum_{px^2 \neq 1} \frac{|\mathbb{Z}/p\mathbb{Z}|}{|\{1\}|}$

Lem : $\{x \in \mathbb{F}_q,\ ax^2 = 1\}$ est de cardinal $1 + \left(\frac{a}{q}\right)$ si $a \neq 0$.

> a est un carré de $\mathbb{F}_q$ ssi a^{-1} est un carré de $\mathbb{F}_q$: $a^{-1} = b^2$, $b \in \mathbb{F}_q$
> ssi $aX^2 - 1 = X^2 - a^{-1} = (X-b)(X+b)$ possède deux racines distinctes ($b = -b \Rightarrow a^{-1} = b^2 = -b^2 = -a^{-1} \Rightarrow a^{-1} = 0$)

Donc $|\{x \in \mathbb{F}_q,\ ax^2 = 1\}| = \begin{cases} 2 & \text{si } a \in \mathbb{F}_q^{*2} \\ 0 & \text{sinon} \end{cases} = 1 + \left(\frac{a}{q}\right)$.

Ainsi, $|X| \equiv 1 + \left(\frac{p}{q}\right) [p]$.

* $X = \{x \in \mathbb{F}_q^p,\ f(x) = 1\}$ où f est la forme quadratique de matrice I_p dans $\mathbb{F}_q^p$.
Soient $d = \frac{p-1}{2}$, $a = (-1)^d$, $J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Notons $M = \begin{pmatrix} J & & \\ & \ddots & \\ & & J \\ & & & a \end{pmatrix}$.
On a $\operatorname{rg}(M) = p = \operatorname{rg}(I_p)$ et $\det M = (\det J)^d a = 1 = \det I_p$
M et I_p ont même rang et det (donc diag modulo les carrés) donc sont congrues.

$|X| = |X'|$ où $X' = \{(y_1, z_1, \dots, y_d, z_d, t) \in \mathbb{F}_q^p,\ 2\sum_{i=1}^{d} y_i z_i + at^2 = 1\}$

→ si $y_1 = \dots = y_d = 0$, alors le choix des z_i est quelconque et on a $at^2 = 1$.
Il y a donc $\left(1 + \left(\frac{a}{q}\right)\right) q^d$ éléments dans X' de cette forme.
→ sinon, il y a $(q^d - 1)$ choix pour $(y_1, \dots, y_d)$, q choix pour t, et alors $(z_1, \dots, z_d)$ appartient à une hyperplan affine de $\mathbb{F}_q^d$, donc q^{d-1} choix.
Il y a $(q^d - 1) q^d$ éléments dans X' de cette forme.

Donc $|X'| = q^d \left(q^d + \left(\frac{a}{q}\right)\right) \equiv \left(\frac{q}{p}\right) \left[\left(\frac{q}{p}\right) + (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\right] [p]$.
car $\left(\frac{a}{q}\right) \equiv a^{\frac{q-1}{2}} \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}} [q]$ ce qui est donc vrai dans $\mathbb{Z}$, puis (mod p).
L'égalité $|X| = |X'|$ $[p]$ donne alors $\left(\frac{p}{q}\right) \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right) [p]$ puis dans $\mathbb{Z}$ car membres ± 1.