Réciprocité quadratique
(par les formes quadratiques)

Théorème: Soient p,q deux nombres premiers impairs distincts. On a $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{q}{p}\right)$.

Démonstration: On pose $X = \{(x_1,\dots,x_p) \in \mathbb{F}_q^p \;/\; \sum_{i=1}^{p} x_i^2 = 1\}$. On va calculer le cardinal de X de deux manières différentes.

- **1ère méthode:** On considère l'action de $\mathbb{F}_p$ sur X définie par $\mathbb{F}_p \longrightarrow \mathfrak{S}_X$
$k \longmapsto ((x_1,\dots,x_p) \mapsto (x_{\overline{k+1}},\dots,x_{\overline{k+p}}))$

Les orbites de cette action sont de deux types différents :

- les orbites triviales (i.e réduites à un élément), correspondant aux éléments $x \in \mathbb{F}_q$ tels que $px^2 = 1$. Ces orbites sont au nombre de $1 + \left(\frac{p}{q}\right)$.
- les autres orbites, dont le stabilisateur, qui est un sous-groupe strict de $\mathbb{F}_p$, est trivial.

Chacune de ces orbites est de cardinal p. La somme des cardinaux des orbites non triviales est donc nulle dans $\mathbb{F}_p$.

L'équation aux classes donne donc $|X| \equiv 1 + \left(\frac{p}{q}\right) \;(p)$.

- **2ème méthode:** On pose $d = \frac{p-1}{2}$ et $a = (-1)^d$.

On remarque que les matrices I_p et $A = \begin{pmatrix} \begin{smallmatrix}0&1\\1&0\end{smallmatrix} & & 0 \\ & \ddots & \\ 0 & & \begin{smallmatrix}0&1\\1&0\end{smallmatrix} \\ & & & a \end{pmatrix}$ sont congrues,

donc les formes quadratiques qu'elles définissent sont équivalentes.

L'ensemble X est donc de même cardinal que $Y = \{(y_1,\dots,y_d,z_1,\dots,z_d,t) \;/\; 2(y_1z_1+\dots+y_dz_d) + at^2 = 1\}$.

Les points $(y_1,\dots,y_d,z_1,\dots,z_d,t) \in Y$ sont de deux types :

- ceux pour lesquels $y_1 = \dots = y_d = 0$, qui donnent $q^d\left(1 + a^{\frac{q-1}{2}}\right)$ choix possibles pour $(z_1,\dots,z_d,t)$;

- ceux pour lesquels un des y_i est non nul : choisir $y_1, \dots, y_d$ non tous nuls donne $q^d - 1$ choix, choisir t donne q choix. Une fois $y_1, \dots, y_d, t$ fixés, il s'agit de prendre $(z_1, \dots, z_d)$ dans un hyperplan affine de $\mathbb{F}_q^d$, ce qui donne q^{d-1} choix. Les points de ce type sont donc au nombre de $(q^d - 1) q q^{d-1}$.

On a donc, par cette méthode, $|X| = q^d (1 + a^{\frac{q-1}{2}}) + q^d (q^d - 1)$

$$= q^d \left[q^d + a^{\frac{q-1}{2}} \right]$$

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

d'où, modulo p, $|X| \equiv \left(\frac{q}{p}\right) \left[\left(\frac{q}{p}\right) + (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \right] \quad (p)$

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

En rassemblant ce résultat et celui obtenu par la première méthode, on a :

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

donc $\left(\frac{p}{q}\right) \equiv (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{q}{p}\right) \quad (p)$. Les termes considérés étant dans $\{\pm 1\}$, l'égalité reste vraie dans $\mathbb{Z}$, ce qui donne $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{q}{p}\right)$,

ce qui achève la preuve.