leçons :
121 : Nombres premiers
123 : Corps finis
170 : Formes quadratiques
190 : Méthodes combinatoires. Pb de dénombrement

# Réciprocité quadratique par les formes quadratiques

(41)

Références :
Caldero-Germoni "$H_2 G_2$"

**Théorème :** Soient $p, q$ premiers impairs distincts.
Alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

preuve :

① On pose $X = \{(x_1, \dots, x_p) \in \mathbb{F}_q^p \mid x_1^2 + \dots + x_p^2 = 1\}$. MQ $\#X = \left(\frac{p}{q}\right) + 1 \ [p]$

- $\mathbb{Z}/p\mathbb{Z}$ agit sur $\mathbb{F}_q^p$ par permutation des coordonnées :
$\forall k \in \mathbb{Z}/p\mathbb{Z}$ $\forall x = (x_1, \dots, x_p) \in \mathbb{F}_q^p$ $k \cdot x = (x_{1+k}, \dots, x_{p+k})$ (indices modulo p)

X est stable sous l'action de $\mathbb{Z}/p\mathbb{Z}$, étudions donc les orbites de cette action.

(i) l'orbite de $(x, \dots, x) \in \mathbb{F}_q^p$ où $x \in \mathbb{F}_q$ est triviale, c'est le singleton $\{(x, \dots, x)\}$
et toutes les orbites triviales sont de cette forme là.
Il y a autant d'orbites triviales que d'éléments $x \in \mathbb{F}_q$ tels que $px^2 = 1$
et $\#\{x \in \mathbb{F}_q \mid px^2 = 1\} = 1 + \left(\frac{p}{q}\right)$

(ii) Les orbites non triviales sont en bijection avec $(\mathbb{Z}/p\mathbb{Z})/\{Id\}$ donc sont de cardinal p.

D'où $\#X = 1 + \left(\frac{p}{q}\right) \ [p]$

② Les matrices $p \times p$ à coefficients dans $\mathbb{F}_q$ $I_p = \begin{pmatrix} 1 & & (0) \\ & \ddots & \\ (0) & & 1 \end{pmatrix}$ et $A = \begin{pmatrix} 0 & 1 & & & \\ 1 & 0 & & & \\ & & 0 & 1 & \\ & & 1 & 0 & \\ & & & & a \end{pmatrix}$
où $a = (-1)^{\frac{p-1}{2}}$ sont congruentes.
En effet, $\operatorname{rg} I_p = \operatorname{rg} A = p$ et $\det I_p = 1 = (-1)^{\frac{p-1}{2}} (-1)^{\frac{p-1}{2}} = \det A$
donc le théorème de classification(*) sur $\mathbb{F}_q$ s'applique. On pose $d = \frac{p-1}{2}$
[(*) des formes quadratiques !]

Par changement de variables linéaire, X est en bijection avec $X' = \{(y_1, z_1, \dots, y_d, z_d, t) \in \mathbb{F}_q^p \mid 2(y_1 z_1 + \dots + y_d z_d) + (-1)^d t^2 = 1\}$

Distinguons deux types de points dans $X'$ :

(i) Si $(y_1, \dots, y_d) = (0, \dots, 0)$ :

On a $q^d$ choix pour les $q$-uplets $(z_1, \dots, z_d)$

puis on a $1 + a^{\frac{q-1}{2}}$ choix pour $t \in \mathbb{F}_q$ tel que $at^2 = 1$

D'où $q^d\left(1 + a^{\frac{q-1}{2}}\right)$ éléments de $X'$ tels que $y_1 = y_2 = \dots = y_d = 0$

(ii) Si $(y_1, \dots, y_d) \neq (0, \dots, 0)$ :

Fixons $(y_1, \dots, y_d) \neq (0, \dots, 0)$ et $t \in \mathbb{F}_q$ ( $q(q^d - 1)$ choix)

Les $(z_1, \dots, z_d)$ qui conviennent sont exactement les points d'un hyperplan affine de $\mathbb{F}_q^d$ donc il y a $q^{d-1}$ choix.

D'où $q^d(q^d - 1)$ éléments de $X'$ tels que $(y_1, \dots, y_d) \neq (0, \dots, 0)$

(3) D'après (1) et (2), on a

$$\#X = 1 + \left(\frac{a}{q}\right) \quad [p] \quad \text{et} \quad \#X = \#X' = q^d\left(1 + a^{\frac{q-1}{2}}\right) + q^d\left(q^d - 1\right)$$

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

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

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

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

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

Les deux termes sont dans $\{-1, 1\}$ donc l'égalité a lieu dans $\mathbb{Z}$.