Développement 28. La loi de réciprocité quadratique par les formes quadratiques

Lemme 1. Soient p un nombre premier impair et $a \in \mathbf{F}_p^\times$ un élément non nul. Alors
$$|\{x \in \mathbf{F}_p \mid ax^2 = 1\}| = 1 + \left(\frac{a}{p}\right).$$

Preuve Dans un premier temps, on suppose que l'élément a est un carré. Dans ce cas, on veut montrer que l'ensemble $S \coloneqq \{x \in \mathbf{F}_p \mid ax^2 = 1\}$ est de cardinal 2. On peut trouver un élément $b \in \mathbf{F}_p^\times$ tel que $a = b^2$. Pour tout élément $x \in \mathbf{F}_p$, on obtient alors
$$\begin{aligned} x \in S &\iff x^2 = b^{-2} \\ &\iff (x - b^{-1})(x + b^{-1}) = 0 \\ &\iff x = \pm b^{-1}. \end{aligned}$$
Ainsi l'ensemble S possède deux éléments.

Maintenant, on suppose que l'élément a n'est pas un carré. Montrons que l'ensemble S est vide. Raisonnons par l'absurde et supposons qu'il ait un élément $x \in S$. Comme l'élément a n'est pas nul, ce dernier élément x n'est pas nul. Par conséquent, on peut écrire $a = x^{-2} = (x^{-1})^2$ ce qui est impossible. Finalement, l'ensemble S est vide, c'est-à-dire de cardinal zéro. ◁

Théorème 2. Soient p et q deux nombres premiers impairs distincts. Alors
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)/2 \times (q-1)/2}.$$

Preuve On va calculer de deux façons le cardinal de l'ensemble
$$X \coloneqq \{(x_1, \dots, x_p) \in \mathbf{F}_q^p \mid x_1^2 + \dots + x_p^2 = 1\}.$$

D'une part, montrons que
$$|X| \equiv \left(\frac{p}{q}\right) + 1 \mod p. \tag{1}$$
On fait agir le groupe $\mathbf{Z}/p\mathbf{Z}$ sur l'ensemble $\mathbf{F}_q^p$ par l'action définie par l'égalité
$$k \cdot (x_1, \dots, x_p) \coloneqq (x_{1+k}, \dots, x_{p+k}), \qquad k \in \mathbf{Z}/p\mathbf{Z},\ (x_1, \dots, x_p) \in \mathbf{F}_q^p.$$
Le stabilisateur $\operatorname{Stab} u$ d'un élément $u \in \mathbf{F}_q^p$ est un sous-groupe de $\mathbf{Z}/p\mathbf{Z}$. Comme l'entier p est premier, le théorème de Lagrange assure que ce stabilisateur est soit le groupe trivial soit le groupe $\mathbf{Z}/p\mathbf{Z}$. Rappelons la formule
$$|\operatorname{Orb} u| = \frac{|\mathbf{Z}/p\mathbf{Z}|}{|\operatorname{Stab} u|}.$$
Distinguons les deux cas.

- Dans le second cas $\operatorname{Stab} u = \mathbf{Z}/p\mathbf{Z}$, l'orbite $\operatorname{Orb} u$ de l'élément u est un singleton et l'élément u est donc de la forme $(x, \dots, x)$ pour un élément $x \in \mathbf{F}_q$ vérifiant $px^2 = 1$. Réciproquement, l'orbite d'un tel élément $(x, \dots, x)$ est un singleton. Ainsi le nombre d'élément $u \in \mathbf{F}_q^p$ dont le stabilisateur n'est pas un singleton est le nombre de solutions de l'équation $px^2 = 1$.
- Dans le premier cas $\operatorname{Stab} u = \{1\}$, ceci est équivalent au fait que l'orbite $\operatorname{Orb} u$ est de cardinal p.

Par conséquent, la formule des classes et le lemme donnent alors
$$|X| \equiv \sum_{px^2=1} \frac{|\mathbf{Z}/p\mathbf{Z}|}{|\mathbf{Z}/p\mathbf{Z}|} \equiv 1 + \left(\frac{p}{q}\right) \mod p.$$

D'autre part, montrons que
$$|X| = (q^d + (-1)^{(p-1)/2 \times (q-1)/2})q^d \quad \text{avec} \quad d \coloneqq \frac{p-1}{2}. \tag{2}$$
Considérons le matrice
$$A \coloneqq \begin{pmatrix} 0 & 1 & & & & \\ 1 & 0 & & & & \\ & & \ddots & & & \\ & & & 0 & 1 & \\ & & & 1 & 0 & \\ & & & & & a \end{pmatrix} \in \mathscr{M}_p(\mathbf{F}_q) \quad \text{avec} \quad a \coloneqq (-1)^d.$$
Les matrices I_p et A à coefficients dans $\mathbf{F}_q$ sont symétriques, de même rang et de même déterminant $1 = (-1)^{(p-1)/2}a$, donc elles sont congruentes. Soit $P \in \mathrm{GL}_p(\mathbf{F}_q)$ une matrice inversible telle que $A = {}^{\mathrm{t}}PI_pP$. Grâce à la bijection $u \longmapsto P^{-1}u$, l'ensemble $X = \{u \in \mathbf{F}_q^p \mid {}^{\mathrm{t}}uu = 1\}$ est de même cardinal que l'ensemble
$$\begin{aligned} X' &\coloneqq \{u' \in \mathbf{F}_p^q \mid {}^{\mathrm{t}}(Pu')(Pu') = 1\} \\ &= \{u' \in \mathbf{F}_p^q \mid {}^{\mathrm{t}}u'Au' = 1\} \\ &= \{(y_1, z_1, \dots, y_d, z_d, t) \in \mathbf{F}_p^q \mid 2(y_1z_1 + \dots + y_dz_d) + at^2 = 1\}. \end{aligned}$$
Dénombrons cet ensemble X'.

- Pour les éléments du type $(0, z_1, \dots, 0, z_d, t) \in X'$, il y a $1 + (\frac{a}{q})$ choix pour les éléments $t \in \mathbf{F}_p$ vérifiant $at^2 = 1$ d'après le lemme et il y a q^d choix pour les éléments z_d, donc le nombre de choix pour de tels éléments est
$$q^d\left(1 + \left(\frac{a}{q}\right)\right) = q^d(1 + a^{(q-1)/2}).$$
- Pour les éléments du type $(y_1, z_1, \dots, y_d, z_d, t) \in X'$ avec un élément non nul y_i, il y a $q^d - 1$ choix pour le vecteur $(y_1, \dots, y_d)$, il y a q choix pour t et il reste à choisir un vecteur $(z_1, \dots, z_d)$ tel que $y_1z_1 + \dots + y_dz_d = 1 - at^2$. Cette dernière équation définit un hyperplan affine, donc il y a q^{d-1} choix pour le vecteur $(z_1, \dots, z_d)$. Finalement, le nombre de choix pour de tels éléments est
$$(q^d - 1)qq^{d-1}.$$

Ainsi, on trouve l'égalité (2)

Concluons. Avec les égalités (1) et (2), on trouve
$$\left(\frac{p}{q}\right) + 1 \equiv (q^{(p-1)/2} + (-1)^{(p-1)/2 \times (q-1)/2})q^{(p-1)/2} \mod p,$$

c'est-à-dire
$$\left(\frac{p}{q}\right) + 1 \equiv \left(\left(\frac{q}{p}\right) + (-1)^{(p-1)/2\times(q-1)/2}\right)\left(\frac{q}{p}\right) \mod p.$$
En multipliant par $\left(\frac{q}{p}\right)$ et en soustrayant $\left(\frac{p}{q}\right)$ de chaque côté, on obtient
$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) \equiv (-1)^{(p-1)/2\times(q-1)/2} \mod p.$$
Comme le nombre premier p est impair, on a $1 \neq -1$ dans $\mathbf{F}_p$ et cette dernière congruence est en fait une égalité dans $\mathbf{Z}$ ce qui conclut. ◁

Recasage

123 Corps finis. Applications

[1] Philippe Caldero et Jérôme Germoni. *Nouvelles histoires hédonistes de groupes et de géométries*. T. Tome premier. Calvage & Mounet, 2017.