

Bd NHGG 1
121
120
123
101?
190?
120

Loi de réciprocité quadratique

Théorème: Soient p et q deux nombres premiers impairs distincts.

Alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}$ ou $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} = \begin{cases} 1 & \text{si } a \text{ est carré dans } \mathbb{F}_p^* \\ -1 & \text{si } a \text{ n'est pas carré dans } \mathbb{F}_p^* \\ 0 & \text{si } a=0 \end{cases}$

Lemme: Soit p un nombre premier impair et $a \in \mathbb{F}_p^*$.

On a $|\{x \in \mathbb{F}_p, ax^2 = 1\}| = 1 + \left(\frac{a}{p}\right)$.

- plan:
- 1) preuve du lemme
 - 2) Introduction de $X = \{(x_1, \dots, x_p) \in \mathbb{F}_q^p, \sum_{i=1}^p x_i^2 = 1\}$
 - 3) Action de $\mathbb{Z}/p\mathbb{Z}$ sur $\mathbb{F}_q^p$
 - 4) Utilisation de matrices pour $|X|$
 - 5) Conclusion.

L'idée est de calculer 1) Soit $x \in \mathbb{F}_p, ax^2 = 1$ m $x^2 = a^{-1}$.
Or a est un carré si a^{-1} en est un

1^{er} cas $a \notin (\mathbb{F}_p^*)^2$: $|\{x \in \mathbb{F}_p, ax^2 = 1\}| = 0 = 1 + \left(\frac{a}{p}\right) = -1$.

2^e cas car $a \in (\mathbb{F}_p^*)^2$: $x^2 = a^{-1} = 0$ donc x est sol $x = y^2, y \neq 0$
 $ax^2 = 1$ m $(yx)^2 = 1$
 m $yx = 1$ m $yx = -1$ car $x^2 = 1$ deux sols dans un corps (car $p \neq 2$)
 m $x = y^{-1}$ m $x = -y^{-1}$.

Or $y \neq -y$ car $\text{Car}(\mathbb{F}_p) \neq 2$.

Donc $|\{x \in \mathbb{F}_p, ax^2 = 1\}| = 2 = 1 + \left(\frac{a}{p}\right) = 1$.

2) L'idée est de calculer de deux façons différentes le cardinal modulo p de la sphère $\rightarrow$ définie sur $\mathbb{F}_q$: $X = \{(x_1, \dots, x_p) \in \mathbb{F}_q^p, \sum_{i=1}^p x_i^2 = 1\}$

D'une part, on fait agir le groupe cyclique $\mathbb{Z}/p\mathbb{Z}$ m X

D'autre part, on remplace la forme quadratique $\sum x_i^2$ par une forme qui lui est congruente, pour laquelle le cardinal de X est facile.

3) D'une part, on a: en faisant agir $\mathbb{Z}/p\mathbb{Z}$ par permutation cyclique sur $\mathbb{F}_q^p$:

$\forall h \in \mathbb{Z}/p\mathbb{Z} \quad \forall (x_1, \dots, x_p) \in \mathbb{F}_q^p, \quad h \cdot (x_1, \dots, x_p) = (x_{1+h}, \dots, x_{p+h})$
 où les indices sont pris modulo p : $x_{i+p} = x_i \quad \forall i$.

Les orbites de $\mathbb{Z}/p\mathbb{Z}$ dans X sont de deux types:

- les singletons $\{(x, \dots, x)\}$, où $x \in \mathbb{F}_q$ qui ont un stabilisateur trivial.
- Les autres orbites qui ont un stabilisateur non trivial, nécessairement égal à $\mathbb{Z}/p\mathbb{Z}$ (car $\text{Stab}(x)$ sous groupe de $\mathbb{Z}/p\mathbb{Z}$).

Le nombre d'orbites à stabilisateur trivial est le nombre de solutions x à l'équation $px^2 = 1$ dans $\mathbb{F}_q$

D'après le lemme, cela vaut $1 + \left(\frac{p}{q}\right)$

Le cardinal des autres orbites est divisible par p car $|X| \approx \frac{q}{p}$

Donc $|X| = \left(\frac{p}{q}\right) + 1 \pmod{p}$.

4) D'autre part, ~~on a~~ $|X| = (q^d + (-1)^{\frac{p-1}{2} \frac{q-1}{2}}) q^d$ ou $d = \frac{p-1}{2}$.

En effet, les matrices $p \times p$ à coefficients dans $\mathbb{F}_q$:

$$I_p = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ et } A = \begin{pmatrix} \boxed{0} & \boxed{0} & \dots & \boxed{0} \\ \boxed{0} & \boxed{0} & \dots & \boxed{0} \\ \vdots & \vdots & \ddots & \vdots \\ \boxed{0} & \boxed{0} & \dots & \boxed{0} \end{pmatrix} \left. \vphantom{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}} \right\} \frac{p-1}{2} \text{ blocs } 2 \times 2$$

et $\alpha := (-1)^{\frac{p-1}{2}} = (-1)^d$.

I_p et A sont symétriques et ont même rang p et même déterminant 1.

Elles ont donc même discriminant (classification FQ sur corps fins; discriminant = det mod carrés du corps de base).

Comme on travaille sur $\mathbb{F}_p$, cela signifie qu'elles sont congruentes.

C'est à dire qu'il y a un changement linéaire de variable qui identifie X à

$$X' = \{(y_1, \dots, y_d, z_1, \dots, z_d, t) \in \mathbb{F}_q^p, 2(y_1 z_1 + \dots + y_d z_d) + t + t^2 = 1\}$$

Distinguons deux types de points $(y_1, \dots, y_d, z_1, \dots, z_d, t)$ de X' :

- les points tels que $y_1 = \dots = y_d = 0$: chaque valeur de t telle que $t + t^2 = 1$ détermine q^d tels points; d'après le lemme, il y en a $q^d (1 + \alpha^{\frac{q-1}{2}})$ points en tout.

- Les points pour lesquels au moins un des y_i n'est pas nul: une fois fixés $(y_1, \dots, y_d)$ et t , il reste à choisir un élément $(z_1, \dots, z_d)$ dans un hyperplan affine $\mathbb{F}_q^d$, il y a $(q^d - 1) q^{d-1}$ tels points en tout.

Par somme $|X| = q^d (q^d - 1 + 1 + \alpha^{\frac{q-1}{2}}) = q^d (q^d + (-1)^{\frac{p-1}{2} \frac{q-1}{2}})$.

5) Par 3) et 4),

$$|X| = q^{\frac{p-1}{2}} \left(q^{\frac{p-1}{2}} + (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \right) = \left(\frac{p}{q}\right) + 1 \pmod{p}.$$

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

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

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

Donc $\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}$ car les éléments valent ± 1 .