VH
29/04/15
1

Loi de réciprocité quadratique

121, 123, 150, 170, 190

Réf: CG

Si q est un nombre premier impair et $a \in \mathbb{F}_q$,

on définit le symbole de Legendre par $\left(\frac{a}{q}\right) = a^{\frac{q-1}{2}} = \begin{cases} 0 \text{ si } a=0 \\ 1 \text{ si } a \text{ est un carré dans } \mathbb{F}_q^\times \\ -1 \text{ sinon} \end{cases}$

On étend cette définition à $a \in \mathbb{Z}$.

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

dém : On va d'abord montrer le lemme suivant.

Lemme : q premier impair, $a \in \mathbb{F}_q^\times$,
alors $\{x \in \mathbb{F}_q \mid ax^2 = 1\}$ est de cardinal $1 + \left(\frac{a}{q}\right)$.

dém : a est un carré dans $\mathbb{F}_q^\times$ ssi a^{-1} l'est,

ssi $aX^2 - 1 \in \mathbb{F}_q[X]$ possède une racine dans $\mathbb{F}_q$.

ssi $aX^2 - 1$ possède deux racines distinctes dans $\mathbb{F}_q$ (car q impair)

Ainsi, le cardinal de $\{x \mid ax^2 = 1\}$ vaut $2 = 1 + \left(\frac{a}{q}\right)$ si a est un carré

$0 =$ —— sinon.

□

Ensuite, on considère

$$X = \{(x_1, \dots, x_p) \in \mathbb{F}_q^p \mid \sum_{i=1}^{p} x_i^2 = 1\}$$

modulo p

Dénombrons X de deux manières différentes.

1ère façon : $X = \{x \in \mathbb{F}_q^p \mid f(x) = 1\}$, où f est la forme quadratique associée à I_p dans la base canonique.

Soit $M = \begin{pmatrix} J & & 0 \\ & \ddots & \\ 0 & & J \\ & & & a \end{pmatrix} \in M_p(\mathbb{F}_q)$, où $J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ est répétée $d = \frac{p-1}{2}$ fois et $a = (-1)^d$.

Alors $\operatorname{rg}(M) = p = \operatorname{rg}(I_p)$

$\det M = (\det J)^d a = (-1)^d (-1)^d = 1 = \det I_p$.

Ainsi, M et I_p ont même rang et même discriminant,

donc d'après la classification des formes quadratiques sur $\mathbb{F}_q$, M et I_n sont congruentes. Soit q la forme quadratique associée à M dans la base canonique.

Ainsi, $|X| = |X'|$

où $X' = \{ x \in \mathbb{F}_q^n \mid q(x) = 1 \}$.

$= \{ (y_1, z_1, \dots, y_d, z_d, t) \in \mathbb{F}_q^n \mid 2\sum_{i=1}^{d} y_i z_i + at^2 = 1 \}$.

	Choix des $(y_i)_{1 \le i \le d}$	Choix de t	Choix des $(z_i)_{1 \le i \le d}$
Si $y_1 = \dots = y_d = 0$	1	D'après le lemme 1, $1 + \left(\frac{a}{q}\right)$	quelconque : q^d
Si l'un des $y_i \neq 0$	$q^d - 1$	quelconque q	(z_i) vérifie l'équation d'un hyperplan affine : q^{d-1}

Au total $|X| = |X'| = q^d \left[1 + \left(\frac{a}{q}\right) \right] + \left[q^d - 1 \right] q^{d-1}$.

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

$= \left(\frac{a}{n}\right) \left[(-1)^{\frac{n-1}{2} \frac{q-1}{2}} + \left(\frac{q}{n}\right) \right] \to \pmod n$ car $a = (-1)^{\frac{n-1}{2}}$.

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

2ème façon :

On fait agir $\mathbb{Z}/n\mathbb{Z}$ sur X :

$k \cdot (x_1, \dots, x_n) = (x_{k+1}, \dots, x_{k+n})$ (indices modulo n)

Le stabilisateur d'un élt x de X est

- soit $\mathbb{Z}/n\mathbb{Z}$, dans ce cas $x = (x_1, \dots, x_1) \in X$ donc $n x_1^2 = 1$
  → il y en a $1 + \left(\frac{1}{q}\right)$ d'après le lemme.
  → seuls dans leur orbite
- soit $\{1\}$, et alors l'orbite est de cardinal n.

à raccourcir

D'après l'équation aux classes,

$|X| = |X^{\mathbb{Z}/n\mathbb{Z}}| \pmod n$ donc $|X| = 1 + \left(\frac{1}{q}\right) \pmod n$.

VM
29/04/15
2

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

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

d'où $\quad \left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{2}} \pmod{p}$.

On les deux membres de l'égalité valent ± 1 dans $\mathbb{Z}$ donc l'égalité modulo p est vraie dans $\mathbb{Z}$: