

Loi de réciprocité quadratique

Léçons: 101, 121, 123, 170

Réf.: Calhene, H2G2 p 303

Lemme:

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

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

Th.:

Soient p et q premiers impairs distincts.

Alors: $\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$

Lemme:

$a \in \mathbb{F}_p^{*2} \Leftrightarrow a^{-1} \in \mathbb{F}_p^{*2} \Leftrightarrow aX^2 - 1 \in \mathbb{F}_p[X]$ a deux racines distinctes

donc $|\{x \in \mathbb{F}_p, ax^2 = 1\}| = \begin{cases} 0 = 1 - 1 = 1 + \left(\frac{a}{p}\right) & \text{si } a \notin \mathbb{F}_p^{*2} \\ 2 = 1 + 1 = 1 + \left(\frac{a}{p}\right) & \text{si } a \in \mathbb{F}_p^{*2} \end{cases}$

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

Th.:

On va calculer de deux manières différentes le cardinal de

$$X = \{u = (u_1, \dots, u_p) \in \mathbb{F}_q^p, \sum_{i=1}^p u_i^2 = 1\}$$

1) Par une action de groupe

On considère l'action $(\mathbb{F}_p \times X \longrightarrow X)$ s'en convaincre...

$$(k, u) \longmapsto k \cdot u = (u_{1+k}, \dots, u_{p+k})$$

où $i+k$ est vu modulo p , i.e. $u_{i+p} = u_i$

$\forall u \in \mathbb{F}_q^p$, $\text{Stab}_u \trianglelefteq \mathbb{F}_p$ $\mathbb{F}_p$ est abélien

On a donc deux possibilités:

• $\text{Stab}_u = \mathbb{F}_p$

$\forall k \in \mathbb{F}_p$, $k \cdot u = (u_{1+k} \dots u_{p+k}) = (u_1 \dots u_p) = u$ donc

$u = (x, \dots, x)$ où $x \in \mathbb{F}_q$.

Donc $\left\{ \begin{array}{l} u \in X \\ \text{Stab}_u = \mathbb{F}_p \end{array} \right\} \iff u = (x, \dots, x), x \in \mathbb{F}_q / p x^2 = 1 \text{ (dans } \mathbb{F}_q)$
↖ s'en convaincre

Le cardinal de ces éléments est donc $1 + \left(\frac{p}{q}\right)$

• $\text{Stab}_u = \{0\}$ (non a' dire)

L'équation aux classes s'écrit alors

$$|X| = \sum_{\substack{x \in \mathbb{F}_q \\ p x^2 = 1}} \frac{|\mathbb{F}_p|}{|\mathbb{F}_p|} + \sum_{\text{autres}} \frac{|\mathbb{F}_p|}{|\{0\}|} = p$$

donc $|X| = 1 + \left(\frac{p}{q}\right) [p]$ (1)

2) Par les formes quadratiques

On considère dans $\text{GL}_p(\mathbb{F}_q)$ les matrices suivantes:

$I_p = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$ et $A = \begin{pmatrix} \begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix} & & 0 \\ & \ddots & \\ 0 & & \begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix} & a \end{pmatrix}$ où $a = (-1)^{\frac{p-1}{2}}$
 $\frac{p-1}{2}$ blocs
 a
 $= (-1)^d$

Alors $\det A = (-1)^{\frac{p-1}{2}} \times a = 1 = \det I_p$.

donc A et I_p ont même rang (p)

A et I_p ont même déterminant donc même discriminant (module $\mathbb{F}_q^{*2}$)

donc A et I_p sont congruentes

classification formes quad. sur corps fini car p, q impairs! (car $\neq 2$)

donc $\exists P \in \text{GL}_p(\mathbb{F}_q) / A = {}^t P I_p P = {}^t P P$.

On écrit $X = \{u \in \mathbb{F}_q^p / {}^t u u = 1\}$ (2)
 $X = \{u' \in \mathbb{F}_q^p / {}^t u' A u' = 1\}$ $\leftarrow u = P u'$ où $P \in GL_p(\mathbb{F}_q)$

donc $X = \{u = (y_1, z_1, \dots, y_d, z_d, t) \in \mathbb{F}_q^p / (*) \sum_{i=1}^d y_i z_i + a t^2 = 1\}$

On distingue deux types d'éléments de X

• si $y_1 = \dots = y_d = 0$:

on peut alors choisir n'importe quelle valeur pour $z_1, \dots, z_d \Rightarrow q^d$ choix

(*) $\Leftrightarrow a t^2 = 1$ donc $1 + \left(\frac{a}{q}\right)$ valeurs possibles pour t

On a donc $\boxed{q^d \left(1 + \left(\frac{a}{q}\right)\right)}$ éléments dans X de cette forme

• si $\exists 1 \leq i \leq d / y_i \neq 0$: $q^d - 1$ possibilités. $\rightarrow q$ possibilités

On peut alors choisir n'importe quelle valeur pour t , et

$\{z = (z_1, \dots, z_d) \in \mathbb{F}_q^d / \sum_{i=1}^d y_i z_i + a t^2 = 1\}$ est un hyperplan

affine de $\mathbb{F}_q^d$, donc de dimension $d-1$ donc de cardinal q^{d-1}

On a donc $\boxed{(q^d - 1) q q^{d-1} = q^d (q^d - 1)}$ éléments

D'où $|X| = q^d \left(1 + \left(\frac{a}{q}\right)\right) + q^d (q^d - 1)$

soit $\boxed{|X| = q^d \left(q^d + \left(\frac{a}{q}\right)\right)} \quad (2)$

3) Conclusion

On écrit (2) $[p]$, et d'après (1).

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

soit $\boxed{q^{2d} + q^d \left(\frac{a}{q}\right) = 1 + \left(\frac{p}{q}\right) [p]}$

Or, $q^{2d} = q^{p-1}$ et $p \nmid q$ donc $q \in \mathbb{F}_p^*$ donc $q^{2d} = 1 [p]$

On a donc $q^d \left(\frac{a}{q} \right) = \left(\frac{p}{q} \right) [p]$

$\downarrow \times q^d$

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

et $q^d = q^{\frac{p-1}{2}} = \left(\frac{q}{p} \right) ; \left(\frac{a}{q} \right) = a^{\frac{q-1}{2}} = (-1)^{\frac{p-1}{2} \times \frac{q-1}{2}}$

donc $(-1)^{\frac{p-1}{2} \times \frac{q-1}{2}} = \underbrace{\left(\frac{q}{p} \right)}_{=\pm 1} \underbrace{\left(\frac{p}{q} \right)}_{=\pm 1} [p]$

et l'égalité est donc vraie dans $\mathbb{Z}$, d'où

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

Rq: l'hyperplan affine...

On a : $y_1 \dots y_d$ non tous nuls, ops $y_1 \neq 0$.

• $t \in \mathbb{F}_q$ quelconque

On cherche $F = \{ z = (z_1 \dots z_d) \in \mathbb{F}_q^d / 2 \sum_{i=1}^d y_i z_i = 1 - at^2 \}$

• Soit $f : \mathbb{F}_q^d \rightarrow \mathbb{F}_q$
 $z = (z_1 \dots z_d) \mapsto 2 \sum_{i=1}^d y_i z_i$

Alors f est une forme linéaire sur l'espace $\mathbb{F}_q^d$, non identiquement nulle, donc $H = \text{Ker } f$ est un hyperplan de $\mathbb{F}_q^d$.

• Soit $z = (z_0, 0 \dots 0) \in \mathbb{F}_q^d$ où $z_0 = \frac{1 - at^2}{2y_1}$

On a alors $f(z) = 2 y_1 z_0 = 1 - at^2$

• Enfin, $F = z + H$ est bien un hyperplan affine.