

Li de réciproque quadratique via le PQ: Shermann p. 360 121-123-170

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

Démonstration: On va calculer de 2 manières différentes le cardinal de

$$B = \{(x_0, \dots, x_{p-1}) \in (\mathbb{F}_q)^p \mid \sum_{i=0}^{p-1} x_i^2 = 1\} \text{ modulo } p$$

Méthode 1: Soit l'action de groupe (2) $\mathbb{Z}/p\mathbb{Z} \times B \rightarrow B$ où $(k, (x_0, \dots, x_{p-1})) \mapsto (x_0, \dots, x_{p-1+k})$ indices sont pris modulo p

Pour $x \in B$, $\text{Stab}(x) \leq \mathbb{Z}/p\mathbb{Z}$ donc $|\text{Stab}(x)| = 1$ ou p . Comme $|\text{Orb}(x)| = \frac{|\mathbb{Z}/p\mathbb{Z}|}{|\text{Stab}(x)|}$ alors $|\text{Orb}(x)| = 1$ ou p .

Si $|\text{Orb}(x)| = 1$ alors $x_i = x_j \quad \forall i, j \in \{0, \dots, p-1\}$ donc $\exists y \in \mathbb{F}_q \mid x = (y, \dots, y)$ et donc $\sum_{i=0}^{p-1} y^2 = py^2 = 1$

La orbite triviale est donc en bijection avec $\{y \in \mathbb{F}_q \mid py^2 = 1\}$ qui a de cardinal $1 + \left(\frac{p}{q}\right)$. En effet: notons $K(a) = \{x \in \mathbb{F}_q \mid ax^2 = 1\}$ si $a \in \mathbb{F}_q^*$; q premier impair et $x \in \mathbb{F}_q$.

* Si a est un carré, $a = b^2$ et l'équation admet 2 solutions $x = b^{-1}$ et $-b^{-1}$. Comme $\mathbb{F}_q$ est un corps, $ax^2 - 1 \in \mathbb{F}_q[x]$ admet au plus 2 racines donc $|K(a)| = 2$ et comme a est un carré; $\left(\frac{a}{q}\right) = 1$ donc $1 + \left(\frac{a}{q}\right) = 2$

* Si a n'est pas un carré, a' non plus car $(b^{-1})^2 = (b^2)^{-1}$ donc $x^2 = a'$ n'a pas de solution d'où $|K(a)| = 0 = 1 + \left(\frac{a}{q}\right)$

$$\exists b \mid a = b^2 \Leftrightarrow a^{-1} = (b^{-1})^2 \\ \text{Si } \nexists b, a \neq b^2 \text{ alors } a^{-1} \neq (b^{-1})^2$$

Finalement: $1 + \left(\frac{a}{q}\right) = |\{x \in \mathbb{F}_q \mid ax^2 = 1\}|$

Enfin, par la formule de Gauss: $|B| = \sum_{x \in B} |\text{Orb}(x)| = |\{y \in \mathbb{F}_q \mid py^2 = 1\}| \text{ modulo } p = 1 + \left(\frac{p}{q}\right) \text{ modulo } p$

Méthode 2: Prenons $d = \frac{p-1}{2}$, $a = (-1)^d$, $J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. On définit les formes quadratiques q_1 et q_2 sur $(\mathbb{F}_q)^p$ par:

$$q_1(x_1, \dots, x_p) = \sum_{i=1}^p x_i^2 \text{ et } q_2(y_1, z_1, \dots, y_d, z_d, t) = 2 \sum_{i=1}^d y_i z_i + at^2$$

Les matrices amorcées sont : I_p et $A = \begin{pmatrix} J \\ J_a \end{pmatrix}$ $d+1$ blocs. (3)

$$\det(A) = \det(J)^d a = (-1)^d (-1)^d = 1$$

Les formes q_1, q_2 sont non dégénérées (4) et de même discriminant (5), donc elles sont congruentes (6). Ainsi : $|B| = |\{x \in (\mathbb{F}_q)^d \mid q_1(x) = 1\}| = |B'| = |\{x \in (\mathbb{F}_q)^d \mid q_2(x) = 1\}|$

énumérons les éléments de B' : soit $(y_1, z_1, \dots, y_d, z_d, t) \in B'$:

* Si $y_1 = \dots = y_d = 0$ alors $at^2 = 1$ donc on a $1 + \left(\frac{a}{q}\right)$ possibilités pour t et on est libre de choisir les z_i donc q^d possibilités pour les z_i . Donc il y a $q^d \left(1 + \left(\frac{a}{q}\right)\right)$ éléments de cette forme.

* Si $\exists y_i \neq 0$; à $y_1, \dots, y_d, t$ fixés, les z_i doivent vérifier :

$q_2(y_1, \dots, t) = 1$ qui est l'équation d'un hyperplan affine de $\mathbb{F}_q^d$ qui a de dimension $|\mathbb{F}_q^d| - 1 = q^d - 1$ donc il y a q^{d-1} choix pour les y_i , $q^{d-1} - 1$ pour les z_i , et q choix pour t . Donc il y a $q^{d-1} (q^{d-1} - 1) q$ éléments de cette forme.

$$\begin{aligned} \text{Finalement : } |B'| &= q^d \left(1 + \left(\frac{a}{q}\right)\right) + q^{d-1} (q^{d-1} - 1) q \\ &= q^d \left(1 + \left(\frac{a}{q}\right) + q^{d-1} - 1\right) = q^d \left(\left(\frac{a}{q}\right) + q^{d-1}\right) \end{aligned}$$

$$\begin{aligned} \text{Conclusion : } 1 + \left(\frac{p}{q}\right) &= q^d \left(\left(\frac{a}{q}\right) + q^{d-1}\right) \pmod{p} & \left(\frac{q}{p}\right) &= q^{p-1/2} \\ &= q^d \left(\left(\frac{(-1)^d}{q}\right) + q^{d-1}\right) \pmod{p} & &= q^d \end{aligned}$$

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

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

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

+ et aussi
① p premier impair ; $n \in \mathbb{N}$. On dit que n est un résidu quadratique de p s'il existe $a \in \mathbb{N} \mid n = a^2 \pmod{p}$ car $\left(\frac{p}{p}\right), \left(\frac{q}{p}\right) = 0, \pm 1$

$\& 1, 1 \neq 2$

On définit le symbole de Legendre $\left(\frac{n}{p}\right)$ par :

$$\left(\frac{n}{p}\right) = \begin{cases} 0, & \text{si } n \equiv 0 \pmod{p} \\ 1, & \text{si } n \not\equiv 0 \pmod{p} \text{ et } n \text{ est un résidu quadr. de } p \\ -1, & \text{sinon} \end{cases}$$

Si $p \nmid n = 1$ alors $\left(\frac{n}{p}\right) = n^{p-1/2} \pmod{p}$

lem p. 75 On a la suite exacte $1 \rightarrow \mathbb{F}_q^{\times 2} \xrightarrow{i} \mathbb{F}_q^{\times} \xrightarrow{1 \pm 1} 1$
 $a \mapsto a^{q-1/2}$

Suite exacte: $0 \rightarrow N \xrightarrow{i} G \xrightarrow{p} K \rightarrow 0$; N, G, K groupes

Si i est injective (homom de gp)
 p surjectif

$\text{Im}(i) = \text{Ker}(p)$

Si $a \in \mathbb{F}_q^{\times}$, alors
 $(a^{q-1/2})^2 = a^{q-1} = 1$
 donc $a^{q-1/2} = \pm 1$

p impair premier:

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

?

* $-1 \not\equiv 0 \pmod{p} \forall p$

* $-1 = x^2 \pmod{p} \Leftrightarrow p = 2 \text{ ou } p \equiv 1 \pmod{4}$

lem p. 58

Si $p \equiv 1 \pmod{4}$ alors $p = 4m + 1$
 donc $(-1)^{4m+1-1/2} = (-1)^{2m} = 1$

* Si $-1 \not\equiv 0 \pmod{p}$ et n'est pas un carré alors $p \equiv 3 \pmod{4}$
 $p = 4m + 3$, $(-1)^{4m+3-1/2} = (-1)^{4m+2(2)} = (-1)^{2m+1} = -1$

② $\mathbb{Z}[p\mathbb{Z}] \times B \rightarrow B$

action?

$(k, (a_0, \dots, a_{p-1})) \mapsto (a_0, \dots, a_{p-1} + k)$

* $0 \cdot (a_0, \dots, a_{p-1}) = (a_0, \dots, a_{p-1})$

* $k \cdot (l \cdot (a_0, \dots, a_{p-1})) = k \cdot (la_0, \dots, la_{p-1})$

$$= (x_{k+l}, \dots, x_{l+k+l}) = (l+l) \cdot (x_0, \dots, x_{p-1}).$$

$$(3) \quad q_2(y_1, z_1, \dots, y_d, z_d, t) = 2 \sum y_i z_i + a t^2$$

$$\text{FP: Lemme p. 131} \quad (q(x+y) - q(x) - q(y)) \times \frac{1}{2} = \mathcal{Q}(x, y)$$

$$\begin{aligned} q_2(y_1 + y_1', \dots, z_d + z_d', t + t') &= 2 \sum (y_i + y_i') (z_i + z_i') + a (t + t')^2 \\ &= 2 \sum (y_i z_i + y_i z_i' + y_i' z_i + y_i' z_i') \\ &\quad + a t^2 + 2 a t t' + a t'^2 \end{aligned}$$

$$q_2(x + x') - q(x) - q(x') = 2 \sum_{i=1}^d (y_i z_i' + y_i' z_i) + 2 a t t'$$

$$\text{Donc } \mathcal{Q}(x, x') = \sum_{i=1}^d (y_i z_i' + y_i' z_i) + a t t'$$

$$\text{Mat}(\mathcal{Q}) = \begin{bmatrix} \mathcal{Q}(e_1, e_1) & \mathcal{Q}(e_1, e_1') \\ \mathcal{Q}(e_1, e_1') & \mathcal{Q}(e_1, e_1') \\ & & \ddots & \\ & & & \mathcal{Q}(e, e) \end{bmatrix} = A$$

$$\mathcal{Q}(e_1, e_1) = 1 \times 0 + 0 \times 1 + a \times 0 = 0$$

$$\mathcal{Q}(e_1, e_1') = 1 \times 1 + 0 \times 0 + 0 = 1$$

$$\mathcal{Q}(e, e) = 0 + a \times 1 \times 1 = a$$

$$x = \begin{pmatrix} y_1 \\ z_1 \\ \vdots \\ y_d \\ z_d \\ t \end{pmatrix}$$

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \quad e_1' = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

$$e_2 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad \dots \quad e_d = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \\ 0 \end{pmatrix} \quad \{d\}$$

$$e_d' = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad \{d+1\}$$

$$e = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$$

$$(4) \text{ Lemme p. 126} \quad \text{FB non dégénérée} \Leftrightarrow \text{Mat}(\mathcal{Q}) \text{ inversible}$$

$$\text{Sci: } \text{rg}(A) = 2d+1 = p-1+1 = p$$

$$\text{D Lemme p. 118} \quad \text{le déterminant de } A \text{ est un déterminant de } \mathcal{Q} \\ \text{si on change de base, } \text{Mat}(\mathcal{Q}) = {}^t P A P$$

$$A'$$

$$\det(A') = \det({}^t P) \det(A) \det(P) = \delta^2 \det(A) \quad (\delta \neq 0)$$

le discriminant est défini à un carré près.

$$\text{Donc, } \det(A) = \det(S)^d \times a = (-1)^d \times (-1)^d = 1 = \det(T_f).$$

⑥ Pour 11.130 Soit $K = \mathbb{F}_q$ un corps fini de caractéristique $\neq 2$ alors et E un K -ev de dim n .

$$\text{Soit } \alpha \in \mathbb{F}_q \setminus (\mathbb{F}_q^*)^2$$

Il y a 2 classes d'eq de $\mathbb{F}_q$ non dégénérées sur E ; de nature:

$$Q_1 = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix}, \quad Q_2 = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 & \alpha \end{pmatrix}$$

Une matrice Q est congruente à Q_1 ou Q_2 selon que son discriminant est un carré ou non de $\mathbb{F}_q^*$

Lemme: Il y a en n, y de $ax^2 + by^2 = 1$; $a, b \in \mathbb{F}_q^*$ a des solutions dans $\mathbb{F}_q$.

On sait qu'il y a $\frac{q+1}{2}$ carrés dans $\mathbb{F}_q$ donc qd y décrit $\mathbb{F}_q$, la quantité $\frac{1-by^2}{a}$ prend $\frac{q+1}{2}$ valeurs donc prend nécessairement une valeur qui est un carré car $\frac{q+1}{2} + \frac{q+1}{2} > q$

Lemme: Soit $n \geq 2$, une FQ Q sur E a une nature du type unnaire. Par rec:

$$* n=2, \text{ BO pour } Q \text{ dans laquelle } ax^2 + by^2 = c(x, y)$$

$$\text{Par le lemme: } \exists e_1 = (x, y) \mid \varphi(e_1) = 1$$

$$\text{Soit } e_2 \perp e_1, \text{ si } |\varphi(e_2)| = 1^2 \in \mathbb{F}_q^{*2}, \text{ on remplace } e_2 \text{ par}$$

$$\frac{1}{1} e_2, \text{ si } |\varphi(e_2)| \in \mathbb{F}_q^* \setminus \mathbb{F}_q^{*2}, \text{ comme } \mathbb{F}_q^{*2} \text{ est d'indice 2 dans } \mathbb{F}_q^*, \text{ on a } |\varphi(e_2)| = 1^2 \alpha \text{ et on remplace } e_2 \text{ par } \frac{1}{1} e_2$$

$$* n > 2, \text{ on prend une BO } (e_1, \dots, e_n). \text{ Le lemme nous donne } \exists e_2 \in$$

par $\langle e_1, e_2 \rangle$ / $Q(e_1) = 1$, par orthogonalité par $K = \langle e_1 \rangle^\perp$,
on obtient la mat voulue.

Sur $\mathbb{Q}[T]^{+2}$, le 2 forms ne sont pas eq car leur discriminant
ne sont pas égaux mod $\mathbb{Q}^{+2}$ donc il y a bien deux formes d'eq de
forme sur $\mathbb{Q}$