

* Formule de réciprocité quadratique: leçons 121, 123; (104; 120)

[Gozard] II 2

p et p' deux entiers premiers impairs distincts

def (plutôt dans le plan):

Soit K un corps de caractéristique $\text{car}(K) \notin \{p, 2\}$ et contenant un élément $\omega \in K^\times$ d'ordre p .

finaloges de la transformée de Fourier:

la somme de Gauss associée à $a \in \mathbb{F}_p^\times$ est: $s(a) = \sum_{x \in \mathbb{F}_p^\times} \left(\frac{x}{p}\right) \omega^{ax}$

symbole de Legendre

On a $s(a) = \left(\frac{a}{p}\right) s(1)$ et $s(1)^2 = \left(-\frac{1}{p}\right) p = (-1)^{\frac{p-1}{2}} p$. (*)

démontre: group fin

$\chi: G \rightarrow M^\times$ un caractère non trivial, alors:

$$\sum_{g \in G} \chi(g) = 0.$$

rq: Si M corps fini:

2 groupes naturels: $(M, +)$ et $(M^\times, \cdot)$

Th:

$$1) \left(\frac{p}{p'}\right) \left(\frac{p'}{p}\right) = (-1)^{\frac{(p-1)(p'-1)}{4}}$$

(on distingue selon les congruences de p et q modulo 4).

$$2) \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

preuve:

lemme:

χ non trivial donc $\exists g_0 \in G, \chi(g_0) \neq 1$

$$\text{Alors: } \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(g_0 g) = \chi(g_0) \left(\sum_{g \in G} \chi(g) \right) \rightsquigarrow \sum_{g \in G} \chi(g) = 0 \text{ car } M \text{ intègre}$$

* preuve de (*):

car $\mathbb{F}_p^\times \xrightarrow{x \mapsto x^{-1}} \mathbb{F}_p^\times$ morphisme

$$\bullet s(a) = \sum_{x \in \mathbb{F}_p^\times} \left(\frac{x}{p}\right) \omega^{ax} = \sum_{x \in \mathbb{F}_p^\times} \left(\frac{a^{-1}x}{p}\right) \omega^x = \sum_{x \in \mathbb{F}_p^\times} \left(\frac{a}{p}\right) \left(\frac{x}{p}\right) \omega^x = \left(\frac{a}{p}\right) s(1)$$

$$\begin{aligned} \bullet s(1)^2 &= \sum_{x, y \in \mathbb{F}_p^\times} \left(\frac{xy}{p}\right) \omega^{x+y} \\ &= \sum_{x, t \in \mathbb{F}_p^\times} \left(\frac{xt}{p}\right) \omega^{x+t} \\ &= \sum_{x, t \in \mathbb{F}_p^\times} \underbrace{\left(\frac{x}{p}\right)^2}_{=1} \left(\frac{t}{p}\right) \omega^{x(1+t)} \\ &= \sum_{t \in \mathbb{F}_p^\times} \left(\frac{t}{p}\right) \underbrace{\sum_{x \in \mathbb{F}_p^\times} \omega^{x(1+t)}}_{=0} \end{aligned}$$

Dev. Alg 3.

Si $t = -1$: $\sum_{x \in \mathbb{F}_p^*} w^{x(1+t)} = \sum_{x \in \mathbb{F}_p^*} 1 = p-1$

Si $t \neq -1$: $w^{1+t} \neq 1$ car w racine primitive p -ème donc $\mathbb{F}_p \rightarrow \mathbb{L}^*$ est

un caractère non trivial et donc, par le lemme:

$$\sum_{x \in \mathbb{F}_p^*} w^{x(1+t)} = -w^{0(1+t)} = -1$$

Donc:

$$s(1)^2 = (p-1) \left(\frac{-1}{p} \right) - \sum_{t \in \mathbb{F}_p^* \setminus \{-1\}} \left(\frac{t}{p} \right)$$

Or, $\mathbb{F}_p^* \rightarrow \{\pm 1\}$ est un caractère non trivial donc, par le lemme: $\sum_{t \in \mathbb{F}_p^*} \left(\frac{t}{p} \right) = 0$

Donc $s(1)^2 = s(1)^2 + \sum_{t \in \mathbb{F}_p^*} \left(\frac{t}{p} \right)$

$$= (p-1) \left(\frac{-1}{p} \right) + \left(\frac{-1}{p} \right)$$

$$= p \left(\frac{-1}{p} \right) = p(-1)^{\frac{p-1}{2}} \quad (\text{donc } s(1) \neq 0)$$

* preuve du théorème:

$p' \nmid p-1$ donc $p'^{p-1} \equiv 1 \pmod{p}$, donc $p \mid p'^{p-1} - 1$ et donc $\exists w \in \mathbb{F}_{p'^{p-1}}$ d'ordre p

On peut donc considérer $s(1)$ la somme de Gauss pour w . On a.

$$s(1)^{p'} = \left(\sum_{x \in \mathbb{F}_p^*} \left(\frac{x}{p} \right) w^x \right)^{p'}$$

$$= \sum_{x \in \mathbb{F}_p^*} \left(\frac{x}{p} \right)^{p'} w^{p'x}$$

(morphisme de Frobenius)

$$= \sum_{x \in \mathbb{F}_p^*} \left(\frac{x}{p} \right) w^{p'x}$$

car $\left(\frac{x}{p} \right) \in \{\pm 1\}$ et p' impair

$$= s(p')$$

car $p' \in \mathbb{F}_p^*$

$$= \left(\frac{p'}{p} \right) s(1)$$

donc: $\left(\frac{p'}{p} \right) = s(1)^{p'-1} = (s(1)^2)^{\frac{p'-1}{2}} = \prod_{x \in \mathbb{F}_p^*} (-1)^{\frac{(p-1)(p'-1)}{4}} = \left(\frac{p}{p'} \right) (-1)^{\frac{(p-1)(p'-1)}{4}}$

donc: $\left(\frac{p}{p'} \right) \left(\frac{p'}{p} \right) = (-1)^{\frac{(p-1)(p'-1)}{4}}$

2) Soit n un entier impair, on a $n^2 - 1 = (n-1)(n+1)$ et $n-1, n+1$ sont deux entiers pairs successifs donc l'un au moins est divisible par 4. Ainsi: $8 \mid n^2 - 1$

Posons: $\chi: (\mathbb{Z}/8\mathbb{Z})^\times \longrightarrow \{\pm 1\}$ C'est bien défini et c'est un caractère non trivial

$$\bar{x} \longmapsto (-1)^{\frac{x^2-1}{8}}$$

de $(\mathbb{Z}/8\mathbb{Z})^\times =: G$. On a: $\chi(1) = \chi(\bar{7}) = 1$ et $\chi(\bar{3}) = \chi(\bar{5}) = -1$.

On peut également définir la somme de Gauss sur G :

p est impair donc $8 \mid p^2 - 1$ donc, comme $\mathbb{F}_p^\times$ est cyclique, $\exists w \in \mathbb{F}_p^\times$ d'ordre 8

On pose: $\forall \bar{a} \in G$: $s(\bar{a}) := \sum_{\bar{x} \in G} \chi(\bar{x}) w^{ax}$, bien défini dans $\mathbb{F}_p$ car $w^8 = 1$.

Encore une fois: $s(\bar{a}) = \chi(\bar{a}) s(\bar{1})$

$$\text{et } s(\bar{1})^p = \sum_{\bar{x} \in G} \chi(\bar{x}) w^{p^x} \\ = \chi(\bar{p}) s(\bar{1})$$

(morphisme de Frobenius)

Par ailleurs: $s(\bar{1}) = w - w^3 - w^5 + w^7$

$$= w(1 - w^2 - w^4 + w^6)$$

$$= w(2 - 2w^2)$$

car $w^4 = -1$

$$= 2w(1 - w^2)$$

En particulier, $s(\bar{1}) \neq 0$ donc $s(\bar{1})^{p-1} = \chi(\bar{p})$

$$\text{Et: } s(\bar{1})^2 = (2w(1 - w^2))^2$$

$$= 4w^2(1 - 2w^2 + w^4)$$

$$= -8w^4$$

$$= 8$$

$$\text{Donc: } s(\bar{1})^{p-1} = (s(\bar{1})^2)^{\frac{p-1}{2}}$$

$$= 8^{\frac{p-1}{2}}$$

$$= \left(\frac{8}{p}\right)$$

$$= \left(\frac{2}{p}\right)^3$$

$$= \left(\frac{2}{p}\right)$$

$$\text{Ainsi: } \left(\frac{2}{p}\right) = \chi(\bar{p}) = (-1)^{\frac{p^2-1}{8}}$$