Loi de réciprocité quadratique par les sommes de Gauss (104, 120, 121, 123)

Zavidovique p. 28

Lem : Soit $x \in \mathbb{F}_p^*$, on a $\mathbb{F}_p^{*2} = \{x \in \mathbb{F}_p^*,\ x^{\frac{p-1}{2}} = 1\}$.

<u>démo</u> : On note $A = \{x \in \mathbb{F}_p^*,\ x^{\frac{p-1}{2}} = 1\}$.

* Mq $\mathbb{F}_p^{*2} \subseteq A$. Soit $x \in \mathbb{F}_p^{*2}$ alors il existe $a \in \mathbb{F}_p^*$ tel que $x = a^2$.
Ainsi $x^{\frac{p-1}{2}} = a^{p-1} = 1$ par le petit théorème de Fermat.

* Mq $\mathbb{F}_p^{*2} = A$. On considère le morphisme d'anneaux $\varphi : \begin{array}{ccc} \mathbb{F}_p^* & \longrightarrow & \mathbb{F}_p^{*2} \\ x & \longmapsto & x^2 \end{array}$. Il est surjectif par définition de $\mathbb{F}_p^{*2}$. De plus par intégrité de $\mathbb{F}_p^*$, on a $\operatorname{Ker}\varphi = \{\pm 1\}$.

Ainsi par le 1er thm d'isomorphisme, on a $|\mathbb{F}_p^{*2}| = \frac{|\mathbb{F}_p^*|}{2} = \frac{p-1}{2}$.
Or A est l'ensemble des racines du polynôme $X^{\frac{p-1}{2}} - 1$. Mais par intégrité de $\mathbb{F}_p$, celui-ci possède au plus $\frac{p-1}{2}$ racines. Donc $|A| \leq \frac{p-1}{2}$. Mais on a $\mathbb{F}_p^{*2} \subseteq A$, donc par égalité des cardinaux on a $\mathbb{F}_p^{*2} = A$.

Thm : Soit p et l deux nombres premiers impairs distincts. Alors $\left(\frac{p}{l}\right)\left(\frac{l}{p}\right) = (-1)^{\frac{(p-1)(l-1)}{4}}$.

<u>démo</u> : Soit p et l deux nombres premiers impairs distincts, Ω une clôture algébrique de $\mathbb{F}_p$ et ω une racine l-ième de l'unité dans Ω et $\omega \neq 1$.

On pose $y = \sum_{x \in \mathbb{F}_l} \left(\frac{x}{l}\right) \omega^x$.

* Montrons que y est bien défini.

Comme $\omega^l = 1$, on a $\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \Omega \\ k & \longmapsto & \omega^k \end{array}$ passe au quotient par $l\mathbb{Z}$. Ainsi y est bien défini.

* Calculons y^2

On a $y^2 = \left(\sum_{x \in \mathbb{F}_l} \left(\frac{x}{l}\right)\omega^x\right)\left(\sum_{z \in \mathbb{F}_l} \left(\frac{z}{l}\right)\omega^z\right) = \sum_{x,z \in \mathbb{F}_l} \left(\frac{xz}{l}\right)\omega^{x+z} \underset{u = x+z}{=} \sum_{u \in \mathbb{F}_l} \omega^u \left(\sum_{t \in \mathbb{F}_l} \left(\frac{t(u-t)}{l}\right)\right)$

Regardons $\sum_{t \in \mathbb{F}_l} \left(\frac{t(u-t)}{l}\right)$.

Comme on a $\left(\frac{0}{l}\right) = 0$, on a alors $\sum_{t \in \mathbb{F}_l} \left(\frac{t(u-t)}{l}\right) = \sum_{t \in \mathbb{F}_l^*} \left(\frac{t(u-t)}{l}\right)$

Or $\sum_{t\in\mathbb{F}_\ell^*}\left(\frac{t(u-t)}{\ell}\right) = \sum_{t\in\mathbb{F}_\ell^*}\left(\frac{-1}{\ell}\right)\left(\frac{t^2}{\ell}\right)\left(\frac{1-ut^{-1}}{\ell}\right) = (-1)^{\frac{\ell-1}{2}}\sum_{t\in\mathbb{F}_\ell^*}\left(\frac{1-ut^{-1}}{\ell}\right)$

Ainsi $y^2 = (-1)^{\frac{\ell-1}{2}}\sum_{u\in\mathbb{F}_\ell} C_u\,\omega^u$ avec $C_u = \sum_{t\in\mathbb{F}_\ell^*}\left(\frac{1-ut^{-1}}{\ell}\right)$

Regardons C_u :

- Si $u=0$, alors $C_0 = \sum_{t\in\mathbb{F}_\ell^*}\left(\frac{1}{\ell}\right) = \ell-1$.

- Sinon, on pose $s = 1-ut^{-1}$. On a s qui décrit $\mathbb{F}_\ell\setminus\{1\}$ lorsque t décrit $\mathbb{F}_\ell^*$.

Donc $C_u = \sum_{s\in\mathbb{F}_\ell\setminus\{1\}}\left(\frac{s}{\ell}\right) = \sum_{s\in\mathbb{F}_\ell}\left(\frac{s}{\ell}\right) - \left(\frac{1}{\ell}\right) = -\left(\frac{1}{\ell}\right) = -1$.

d'après le lemme, il y a autant de carré dans $\mathbb{F}_\ell^*$ que de non carrés

donc $\sum_{s\in\mathbb{F}_\ell^*}\left(\frac{s}{\ell}\right) = (-1)\frac{\ell-1}{2} + 1\cdot\frac{\ell-1}{2} = 0$.

Ainsi $y^2 = (-1)^{\frac{\ell-1}{2}}\left(\ell-1 - \sum_{u\in\mathbb{F}_\ell^*}\omega^u\right) = (-1)^{\frac{\ell-1}{2}}\underbrace{\left(\ell-1-\frac{\omega-\omega^\ell}{1-\omega}\right)} = (-1)^{\frac{\ell-1}{2}}\,\ell$.

$= \ell-1-\frac{\omega^\ell-\omega}{\omega-1} = \ell - \frac{\omega^\ell-1}{\omega-1}$ or $\omega^\ell=1$.

* Montrons que $y^{p-1} = \left(\frac{p}{\ell}\right)$.

On a $y^p = \left(\sum_{x\in\mathbb{F}_\ell}\left(\frac{x}{\ell}\right)\omega^x\right)^p = \sum_{x\in\mathbb{F}_\ell}\left(\frac{x}{\ell}\right)^p\omega^{px} = \sum_{x\in\mathbb{F}_\ell}\left(\frac{x}{\ell}\right)\omega^{px} = \sum_{z\in\mathbb{F}_\ell}\left(\frac{zp^{-1}}{\ell}\right)\omega^z$

morphisme de Frobenius

p est impair donc $\left(\frac{x}{\ell}\right)^p = \left(\frac{x}{\ell}\right)$

$= \left(\frac{p^{-1}}{\ell}\right)y = \left(\frac{p}{\ell}\right)y$.

D'où $y^{p-1} = \left(\frac{p}{\ell}\right)$.

* Conclusion :

$\left(\frac{p}{\ell}\right) = y^{p-1} = \left(y^2\right)^{\frac{p-1}{2}} = \left((-1)^{\frac{\ell-1}{2}}\ell\right)^{\frac{p-1}{2}} = (-1)^{\frac{(\ell-1)(p-1)}{4}}\,\ell^{\frac{p-1}{2}} = (-1)^{\frac{(\ell-1)(p-1)}{4}}\left(\frac{\ell}{p}\right)$

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