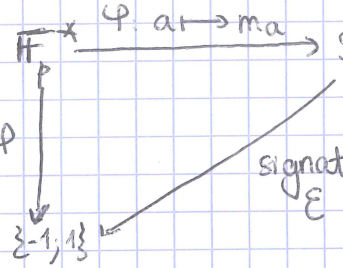
LEMME DE ZOLOTAREV

Leçons: 105, 120, 121

Références: Caunet algèbre, P. Caldero (à paraître) avant les deux normalement :)

Résumé:



Le but du dev c'est de montrer que
- $\varepsilon(m_a) = \left(\frac{a}{p}\right)$
- $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

pour p premier impair.

où m_a est la multiplication par a (modulo p)
et $\left(\frac{a}{p}\right)$ est le symbole de Legendre : $\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } a \text{ est divisible par } p \\ 1 & \text{s'il existe } k \text{ tq } a \equiv k^2 \bmod p \\ -1 & \text{sinon.} \end{cases}$

On va montrer que :

I - si $\varphi : \mathbb{F}_p^* \longrightarrow \{-1;1\}$ est un morphisme non trivial alors c'est le morphisme $a \longmapsto \left(\frac{a}{p}\right)$.

II - $\phi : \mathbb{F}_p^* \longrightarrow S(\mathbb{F}_p^*)$ est un morphisme de groupes.
$a \longmapsto m_a$

III - Pour tout $a \in \mathbb{F}_p^*$, $\varepsilon(m_a) = \left(\frac{a}{p}\right)$
d'où $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

I • Soit $\chi : \mathbb{F}_p^* \longrightarrow \{-1, 1\}$ un morphisme de groupes non trivial.
et z un carré de $\mathbb{F}_p^*$, ie il existe $y \in \mathbb{F}_p^*$, tel que $z = y^2$.

· On a alors $\chi(z) = \chi(y)^2 = 1$, d'où :
$K = \{z \in \mathbb{F}_p^* \text{ carrés}\} \subseteq \ker \chi$.

• Or $|\ker\chi| \times \underbrace{|\mathrm{Im}\,\chi|}_{=|\{-1,1\}|=2} = \underbrace{|\mathbb{F}_p^*|}_{=p-1}$.

d'où $|\ker\chi| = \frac{p-1}{2}$ et $K = \ker\chi$ par égalité des cardinaux.

• Donc $\chi = \left(\frac{\cdot}{p}\right)$.

II • $a \in \mathbb{F}_p^*$ est inversible, donc $m_a^{-1} = m_{a^{-1}}$ donc m_a est bijective. ↗ $m_a \in S(\mathbb{F}_p^*)$.

• Pour $a, b \in \mathbb{F}_p^*$, z, $m_{ab}(z) = (ab)z = a(bz) = m_a \circ m_b(z)$.

• Donc ϕ est bien un morphisme de $\mathbb{F}_p^*$ dans $S(\mathbb{F}_p^*)$.

III • D'après I, si $a \mapsto \left(\frac{a}{p}\right)$ et $a \mapsto \varepsilon(m_a)$ sont deux morphismes non triviaux de $\mathbb{F}_p^*$ dans $\{-1;1\}$, alors on a gagné.

- $a \mapsto \left(\frac{a}{p}\right)$? il vaut -1 sur les non-carrés (et il y en a !)
- $a \mapsto \varepsilon(m_a)$?
  - $\mathbb{F}_p^*$ est cyclique généré par un certain $g \in \mathbb{F}_p^*$ on a alors $m_g = (1 \quad a \quad a^2 \quad \dots \quad a^{p-2})$
  - et $\varepsilon(m_g) = (-1)^{(p-1)-1} = (-1)^{p-2} = -1$.

⟶ les deux sont donc non-triviaux

+ ce sont des morphismes : $a \mapsto \left(\frac{a}{p}\right)$ par le critère d'Euler $a^{\frac{p-1}{2}} = \left(\frac{a}{p}\right)$ mod p.
$a \mapsto \varepsilon(m_a)$ par II.

donc ce sont les mêmes

• On a donc $\left(\frac{2}{p}\right) = \varepsilon(m_2)$

et $m_2 = \begin{pmatrix} 1 & 2 & 3 & \dots & \frac{p-1}{2} & \frac{p+1}{2} & \dots & p-1 \\ 2 & 4 & 6 & & p-1 & 1 & \dots & p-2 \end{pmatrix}$ i,j tq $i<j$ et $m_2(i) > m_2(j)$

Or $\varepsilon(m_2) = (-1)^{\mathrm{Inv}(m_2)}$ où $\mathrm{Inv}(m_2)$ est le nombre d'inversions de m_2.

Et $\mathrm{Inv}(m_2) = 1 + 2 + \dots + \frac{p-1}{2} = \frac{1}{2}\underbrace{\frac{p-1}{2}\frac{p+1}{2}}_{\text{multiple de 2 car 4 divise } p-1 \text{ ou } p+1 !} = \frac{p^2-1}{8}$.

• On peut aussi remarquer que cela peut être difficile de déterminer la parité de $\frac{p^2-1}{8}$, mais si l'on regarde bien :
$\frac{p^2-1}{8}$ est pair ssi $p^2-1 \equiv 0 \bmod 16$ ie $p^2-1 \in \mathbb{Z}/16\mathbb{Z}$.

On a donc $\overline{p^2-1} = \bar{p}^2 - \bar{1} = \bar{0}$
et p étant impair $\bar{p} = \pm\bar{1}, \pm\bar{3}, \pm\bar{5}, \pm\bar{7}$
d'où $\bar{p}^2 = \pm\bar{1}, \pm\bar{9} = \pm\bar{7}, \pm\overline{25} = \pm\bar{7}, \pm\overline{49} = \pm\bar{1}$.

Conclusion : 2 est un carré modulo p si et seulement
$p \equiv \pm 1 \bmod 16$ ou $p \equiv \pm 7 \bmod 16$.

Bonus : Il y a $\frac{p-1}{2}$ carrés dans $\mathbb{F}_p^*$ & p premier impair.
• Posons $\Phi : \mathbb{F}_p^* \longrightarrow \mathbb{F}_p^*$ c'est un morphisme de groupes.
$x \longmapsto x^2$
• Soit $a \in \ker\Phi$, on a $\Phi(a) = a^2 = 1$.
D'où $(a-1)(a+1) = 0$, soit $a = \pm 1$. (et $-1 \neq 1$ car $p > 2$).
Dès lors, $|\ker\Phi| = 2$ (par synthèse évidente)
• Ainsi, $|\mathrm{Im}\,\Phi| = \frac{|\mathbb{F}_p^*|}{|\ker\Phi|} = \frac{p-1}{2}$.

+ en fait on arrive à $p \equiv \pm 1 \bmod 8$
et il y en a une infinité grâce au petit théorème de Dirichlet.

+ le lemme de Zolotarev fournit un pont entre S_n et la théorie des nombres.

Lien avec le théorème de Zolotarev.

$\varphi : (\mathbb{F}_p)^n \longrightarrow (\mathbb{F}_p)^n$ automorphisme : $\varphi \in GL_n(\mathbb{F}_p)$.

Alors $\varepsilon(\varphi) = \left(\frac{\det \varphi}{p}\right)$.