File:CubicResidueSymbol.tex compil. le 4 août 2017,6:38

Le symbole cubique $\chi_\pi = \left(\frac{\bullet}{\pi}\right)_3$

D'après le lemme 1, §4 (Proof of The Law of Cubic Reciprocity) du chap. 9 de Ireland & Rosen, p. 115

Contexte : un premier $p \equiv 1 \bmod 3$ et $p = \pi\overline{\pi}$ sa factorisation normalisée dans $\mathbb{Z}[j]$ i.e. $\pi \equiv 1 \bmod 3$ et du coup $\overline{\pi} \equiv 1 \bmod 3$. Pourquoi le modulus 3 dans la normalisation ? Rappelons d'abord que le groupe des unités de $\mathbb{Z}[j]$ est :

$$\mathbb{Z}[j]^\times = \langle -j \rangle = \{\pm 1, \pm j, \pm j^2\}$$

Le modulus 3 a été choisi parce que la réduction modulo 3 induit un isomorphisme entre les groupes d'inversibles :

$$\mathbb{Z}[j]^\times \xrightarrow[\simeq]{z \mapsto z \bmod 3} \big(\mathbb{Z}[j]/\langle 3\rangle\big)^\times$$

Cette dernière assertion est à la charge du lecteur.
Cela étant, on dispose d'isomorphismes canoniques :

$$\mathbb{F}_p \simeq \mathbb{Z}[j]/\langle\pi\rangle, \qquad \mathbb{F}_p \simeq \mathbb{Z}[j]/\langle\overline{\pi}\rangle, \qquad U_3(\mathbb{Z}[j]/\langle\pi\rangle) \overset{\text{can.}}{\simeq} \mathbb{U}_3 = \langle j\rangle = \{1, j, j^2\}$$

Tout à droite, l'isomorphisme canonique de $\mathbb{U}_3$ vers $U_3(\mathbb{Z}[j]/\langle\pi\rangle)$ est la réduction modulo π. Ceci permet de définir $\chi_\pi : \mathbb{Z}[j] \to \mathbb{U}_3 \cup \{0\}$ vérifiant :

$$\chi_\pi(z) = \begin{cases} 0 & \text{si } \pi \mid z \\ \text{l'unique } u \in \mathbb{U}_3 \text{ tq } u \equiv z^{\frac{p-1}{3}} \bmod \pi & \text{sinon} \end{cases}$$

Explication : dans la branche du bas, $z^{\frac{p-1}{3}}$ modulo π est dans $U_3(\mathbb{Z}[j]/\langle\pi\rangle)$ et il lui correspond donc un unique $u \in \mathbb{U}_3$ tel que ...

Lemme 1.
Soit $p \equiv 1 \bmod 3$. On dispose alors d'une expression de π en fonction d'une somme de Jacobi :

$$\boxed{\pi = -J(\chi_\pi, \chi_\pi)}$$

Preuve.
On a vu une preuve directe (dûe à Weil, cf `Jchi3chi3.pdf`) du fait que $-J(\chi_\pi, \chi_\pi) \equiv 1 \bmod 3$. On sait également que $|J(\chi_\pi, \chi_\pi)| = p$ d'après les propriétés classiques sur les sommes de Gauss-Jacobi.
On va montrer que $J(\chi_\pi, \chi_\pi)$ est multiple de π ; il s'en suivra, puisque π et $-J(\chi_\pi, \chi_\pi)$ vérifient tous les deux la congruence $\cdots \equiv 1 \bmod 3$, qu'ils sont égaux.

• (♡) Justification de $J(\chi_\pi, \chi_\pi) \equiv 0 \bmod \pi$
Par définition :

$$J(\chi_\pi, \chi_\pi) = \sum_{x \in \mathbb{F}_p} \chi_\pi(x)\chi_\pi(1-x)$$

Utilisons, pour $x \in \mathbb{Z}$, que :

$$\chi_\pi(x) \equiv x^{\frac{p-1}{3}} \bmod p, \qquad \chi_\pi(1-x) \equiv (1-x)^{\frac{p-1}{3}} \bmod \pi$$

On a donc :

$$J(\chi_\pi, \chi_\pi) \equiv S \bmod \pi \quad \text{où l'on a posé} \quad S = \sum_{x \in \mathbb{F}_p} x^{\frac{p-1}{3}}(1-x)^{\frac{p-1}{3}}$$

Si on montre que S est nul dans $\mathbb{F}_p$, on aura bien, puisque p est multiple de π, justifié (♡).
La somme S est combinaison linéaire de sommes S_i :

$$S_i = \sum_{x \in \mathbb{F}_p} x^i = \sum_{x \in \mathbb{F}_p^*} x^i \qquad \text{avec } \tfrac{p-1}{3} \le i \le \tfrac{p-1}{3} + \tfrac{p-1}{3}$$

On va montrer que l'on a $S_i = 0$. Soit $g \in \mathbb{F}_p^*$ un générateur de ce groupe cyclique. Alors :

$$S_i = \sum_{k=0}^{p-2} (g^k)^i = \sum_{k=0}^{p-2} (g^i)^k = 1 + g^i + (g^i)^2 + \cdots + (g^i)^{p-2}$$

On va utiliser le fait que $g^i \neq 1$, ce qui est dû au fait que i n'est ni trop petit (i n'est pas nul car minoré par $\frac{p-1}{3}$) ni trop grand, en tout cas non multiple de $p-1$, car majoré par $2\frac{p-1}{3}$

$$S_i = \frac{1-(g^i)^{p-1}}{1-g^i} = \frac{1-(g^{p-1})^i}{1-g^i} = 0 \qquad \text{(puisque } g^{p-1} = 1\text{)}$$

□