Loi de réciprocité quadratique

École du Barboux – janvier 2017

1 La loi de réciprocité quadratique

Euler. Pour tout $a \in \mathbb{Z}$, on a $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \bmod p$.

Multiplicativité. Pour tous $a, b \in \mathbb{Z}$, on a $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

Loi de réciprocité quadratique. Si $p \neq q$ sont des premiers impairs alors

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

Lois complémentaires. Pour p premier impair, on a

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

Multiplicativité pour le symbole de Jacobi. Si N est un entier impair et $a, b \in \mathbb{Z}$ alors

$$\left(\frac{ab}{N}\right) = \left(\frac{a}{N}\right)\left(\frac{b}{N}\right).$$

Lois de réciprocité de Jacobi. Si N, M sont impairs distincts, alors :
$\left(\frac{-1}{N}\right) = (-1)^{\frac{N-1}{2}}$;
$\left(\frac{2}{N}\right) = (-1)^{\frac{N^2-1}{8}}$;
$\left(\frac{M}{N}\right)\left(\frac{N}{M}\right) = (-1)^{\frac{(N-1)(M-1)}{4}}$.

2 Les sommes de Gauss

Soit $\chi : \mathbb{F}_p^* \to \mathbb{C}^*$ un caractère de $\mathbb{F}_p^*$, prolongé à $\mathbb{F}_p$ par $\chi(0) = \begin{cases} 0 & \text{si } \chi \neq \mathbb{1}; \\ 1 & \text{si } \chi = \mathbb{1}. \end{cases}$

Soit ζ une racine primitive p–ème de l'unité.

La *somme de Gauss* associée à χ et $a \in \mathbb{F}_p$ est :

$$g_a(\chi) = \sum_{x \in \mathbb{F}_p} \chi(x)\zeta^{ax} \quad \in \mathbb{C}.$$

Propriétés.
Si $a \neq 0$ et $\chi \neq \mathbb{1}$: $g_a(\chi) = \chi(a^{-1})g_1(\chi)$.
Si $a \neq 0$ et $\chi = \mathbb{1}$: $g_a(\mathbb{1}) = 0$.
Si $a = 0$ et $\chi \neq \mathbb{1}$: $g_0(\chi) = 0$.
Si $a = 0$ et $\chi = \mathbb{1}$: $g_0(\mathbb{1}) = p$.

Notation : $g(\chi) = g_1(\chi)$

Module. Si $\chi \neq \mathbb{1}$ alors $|g(\chi)| = \sqrt{p}$.

3 Nombre de solutions de $x^n + y^n = 1$ sur $\mathbb{F}_p$

Soit $a \in \mathbb{F}_p$. On pose $N(x^n = a) = \#\{x \in \mathbb{F}_p,\ x^n = a\}$.

Cas $n = 2$: $\quad N(x^2 = a) = 1 + \left(\frac{a}{p}\right)$.

Cas $n \mid (p-1)$: $\quad N(x^n = a) = \sum_{i=0}^{n-1} \chi_0^i(a)$, où χ_0 est un caractère de $\mathbb{F}_p^*$ d'ordre n.

On pose $N(x^n + y^n = 1) = \#\{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p, x^n + y^n = 1\}$.

Si $n \mid (p-1)$:

$$N(x^n + y^n = 1) = \sum_{a+b=1} N(x^n = a)N(y^n = b) = \sum_{0 \le i,j \le n-1} \left(\sum_{a+b=1} \chi_0^i(a)\chi_0^j(b) \right).$$

Soient χ, λ des caractères de $\mathbb{F}_p^*$, prolongés à $\mathbb{F}_p$. La *somme de Jacobi* associée est :

$$J(\chi, \lambda) = \sum_{a+b=1} \chi(a)\lambda(b) \quad \in \mathbb{C}.$$

Propriétés. Soient $\chi \neq \mathbb{1}$ et $\lambda \neq \mathbb{1}$.

$J(\mathbb{1}, \mathbb{1}) = p$;

$J(\mathbb{1}, \chi) = 0$;

$J(\chi, \chi^{-1}) = -\chi(-1)$;

Si $\chi\lambda \neq \mathbb{1}$ alors $J(\chi, \lambda) = \dfrac{g(\chi)g(\lambda)}{g(\chi\lambda)}$.

Module. Si χ, λ et $\chi\lambda$ sont tous distincts de $\mathbb{1}$, alors $|J(\chi, \lambda)| = \sqrt{p}$.

Estimations du nombre de solutions.

Cas $n = 2$: $N(x^2 + y^2 = 1) = p - (-1)^{\frac{p-1}{2}}$.

Si $n \geq 2$, $n \mid (p-1)$, posons $\delta_n = \begin{cases} n & \text{si } -1 \text{ est une puissance } n\text{-ème dans } \mathbb{F}_p, \\ 0 & \text{sinon.} \end{cases}$

Alors

$$|N(x^n + y^n = 1) + \delta_n - (p+1)| \leq (n-1)(n-2)\sqrt{p}.$$

Références.

M. Demazure, *Cours d'algèbre. Primalité. Divisibilité. Codes.* Cassini, 1997.

M. Hindry, *Arithmétique.* Tableau Noir, Calvage et Mounet, 2008.

K. Ireland, M. Rosen, *A classical introduction to modern number theory.* Graduate Texts in Mathematics, 84. Springer.

F. Lemmermeyer, *Reciprocity laws. From Euler to Eisenstein.* Springer Monographs in Mathematics. Springer, Berlin, 2000.

J.-P. Serre, *Cours d'arithmétique.* PUF, Paris, 1977.