Réciprocité quadratique par les sommes de Gauss

Leçons

110 (dev) Caractères d'un groupe abélien fini et transformée de Fourier discrète

123 (dev) Corps finis. Applications.

125 (dev) Extensions de corps. Exemples et applications

Source Jean-Pierre Serre [Ser70, chapitre I] ou Pierre Samuel [Sam67]. Attention aux notations : on prend p et ℓ comme Serre (et non q et p comme Samuel).

Théorème 1. *Soient p et ℓ deux nombres premiers impairs distincts. Alors*

$$\left(\frac{p}{\ell}\right)\left(\frac{\ell}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{\ell-1}{2}} \tag{1}$$

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

On va approcher à l'aide d'une *somme de Gauss* une racine carrée de $\pm\ell$ dans une extension adéquate de $\mathbb{F}_p$. Pour tester si la racine obtenue est dans $\mathbb{F}_p$, on lui appliquera l'automorphisme de Frobenius. C'est un peu plus facile pour la loi complémentaire, on commence donc par celle-ci.

(a) La loi complémentaire Soit K une extension de décomposition du polynôme $P = X^4 + 1$ sur $\mathbb{F}_p$. Soit α une de ses racines dans K. Comme $\alpha^4 = -1$, le nombre $y = \alpha + \alpha^{-1}$ est une racine carrée de 2 dans K. De plus car$K = p$ donc

$$y^p = \alpha^p + \alpha^{-p}.$$

Si $p \equiv \pm 1$ modulo 8, cela entraîne $y^p = y$, donc y est fixe par le Frobenius Frob_p, ce qui revient à affirmer $y \in \mathbb{F}_p$

Si $p \equiv \pm 3$ modulo 8, $y^p = -y$ et donc $y \notin \mathbb{F}_p$.

On remarque par ailleurs que

$$(-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{si } p \equiv \pm 1\,(8) \\ -1 & \text{si } p \equiv \pm 3\,(8) \end{cases}$$

Conclusion,

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

(b) Loi de réciprocité quadratique Soit K une extension de décomposition de $P = X^\ell - 1$ sur $\mathbb{F}_p$, ζ une racine de P dans K. On introduit la somme de Gauss

$$y = \sum_{a \in \mathbb{Z}/\ell\mathbb{Z}} \left(\frac{a}{\ell}\right) \zeta^a.$$

(l'écriture ζ^a avec $a \in \mathbb{Z}/\ell\mathbb{Z}$ a bien un sens, puisque $\zeta^\ell = 1$).

Proposition 2. *On a*

$$y^2 = \left(\frac{-1}{\ell}\right) \ell. \tag{3}$$

Démonstration. Calculons

$$y^2 = \sum_{(a,b) \in \mathbb{F}_\ell^{\times 2}} \left(\frac{ab}{q}\right) \zeta^{a+b} \underset{c \leftarrow a^{-1}b}{=} \sum_{c \in \mathbb{F}_\ell^\times} \left[\left(\frac{c}{\ell}\right) \sum_{a \in \mathbb{F}_p^\times} \zeta^{a(1+c)} \right].$$

On vérifie que

$$\sum_{a \in \mathbb{F}_\ell^\times} \zeta^{a(1+c)} = \begin{cases} -1 & \text{si } c \neq -1 \\ \ell - 1 & \text{si } c = -1. \end{cases}$$

Finalement (attention aux signes à cet endroit !)

$$\begin{aligned} y^2 &= \sum_{b \in \mathbb{F}_\ell^\times \setminus \{-1\}} \left(\frac{b}{\ell}\right)(-1) + \left(\frac{-1}{\ell}\right)(\ell - 1) \\ &= \sum_{b \in \mathbb{F}_\ell^\times} \left(\frac{b}{\ell}\right)(-1) - (-1)\left(\frac{-1}{\ell}\right) + \left(\frac{-1}{\ell}\right)(\ell - 1), \end{aligned}$$

le premier terme étant nul car il y a autant de carrés que de non-carrés dans $\mathbb{F}_\ell^\times$, on trouve le résultat escompté. $\square$

Or, $y \in \mathbb{F}_p \iff y^p = y$ (puisque $\mathbb{F}_p$ est, dans K, le sous-corps fixé par le Frobenius). Comme nous sommes en caractéristique p,

$$y^p = \sum_{a \in \mathbb{F}_\ell} \left(\frac{a}{\ell}\right) \zeta^{ap} = \sum_{b \in \mathbb{F}_\ell} \left(\frac{bp^{-1}}{\ell}\right) \zeta^b = \left(\frac{p^{-1}}{\ell}\right) y = \left(\frac{p}{\ell}\right) y.$$

Donc, $\left(\frac{-1}{\ell}\right)\ell$ est un carré modulo p si et seulement si p est un carré modulo ℓ. Finalement

$$\left(\frac{\ell}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{\ell-1}{2}}\left(\frac{p}{\ell}\right).$$

Remarque 3. Plutôt que de prendre un corps de racine K variant avec ℓ, on peut comme [Ser70] se placer une bonne fois pour toutes dans $\overline{\mathbb{F}_p}$, clôture algébrique de $\mathbb{F}_p$, limite inductive des $\mathbb{F}_{p^{n!}}$. Attention toutefois à bien prendre une racine α **primitive** 8-ième de l'unité dans la preuve de la loi complémentaire. Celle-ci existe bien puisque le polynôme X^8-1 est séparable sur $\mathbb{F}_p$ (ce ne serait pas le cas de X^p-1, pour prendre un exemple).

Remarque 4. Avec la loi de réciprocité quadratique, décider si a est un carré modulo p est un problème algorithmiquement rapide. L'usage du symbole de Jacobi permet même d'éviter d'avoir à décomposer a en facteurs premiers, ce qui ramène le calcul de (a/p) à une complexité comparable à celle de l'algorithme d'Euclide[1]. La recherche effective d'une racine carrée dans $\mathbb{F}_p$ n'est pas non plus très difficile une fois que l'on sait calculer des symboles de Legendre (avec l'algorithme de Cippola), contrairement au cas général dans $\mathbb{Z}/n\mathbb{Z}$.

Remarque 5. Une autre approche (peut-être plus fidèle à Gauss ?) est de calculer les sommes de Gauss dans $\mathbb{C}$, ce qui oblige à écrire les congruences modulo l'anneau des entiers algébriques $\overline{\mathbb{Z}}$. Toutefois, la relation maîtresse (3) apparaît alors un peu plus naturelle. En effet, si $\zeta = e^{2i\pi/\ell}$, alors

$$y = \sum_{a\in\mathbb{Z}/\ell\mathbb{Z}}\left(\frac{a}{\ell}\right)\zeta^a = \sum_{a\in\mathbb{F}_\ell^\times}\left(\frac{a}{\ell}\right)\zeta^a.$$

Si l'on pose $\eta_\ell(a) = \left(\frac{a}{\ell}\right)$ et $\chi(a) = \zeta^a$, alors η_ℓ est un caractère **multiplicatif** (i.e, un élément de $\widehat{\mathbb{F}_p^\times}$) et χ un caractère **additif** (i.e., un élément de $\widehat{\mathbb{F}_p}$). La somme de Gauss est (au choix) la transformée de Fourier de $\chi \in L^2\left(\mathbb{F}_p^\times\right)$ évaluée en η_ℓ, ou bien encore la transformée de Fourier de $\overline{\eta}$ évaluée en χ. L'apparition de ℓ dans le carré de y (qui est aussi une transformée de Fourier) s'interprète comme un coefficient de renormalisation. Pour plus de précisions voir le livre de Mérindol, [Mer06].

Références

[Mer06] Jean-Yves Merindol. *Nombres et algèbres.* Collection Grenoble Sciences. EDP Sciences, 2006.

[Sam67] Pierre Samuel. *Théorie algébrique des nombres.* Hermann, Paris, 1967.

[Ser70] Jean-Pierre Serre. *Cours d'arithmétique : par Jean-Pierre Serre.* SUP. Le mathématicien. Presses universitaires de France, 1970.

1. Pour rappel, logarithmique, d'après un théorème de Lamé.