Agrégation externe

La loi de réciprocité quadratique via le théorème des restes chinois

2015-2016

Nous rappelons que, pour tout entier n et tout nombre premier impair p, le *symbole de Legendre* $(\frac{n}{p})$ est défini par les relations

$$\left(\frac{n}{p}\right) = \begin{cases} 0 & \text{si } p \text{ divise } n, \\ 1 & \text{si } p \text{ ne divise pas } n \text{ et } n \text{ est un carré modulo } p, \\ -1 & \text{sinon.} \end{cases}$$

La célebre *loi de réciprocité quadratique*, initialement conjecturée par Leonhard Euler, relie $(\frac{p}{q})$ et $(\frac{q}{p})$, où p et q sont deux nombres premiers impairs.

Théorème 1 (Loi de réciprocité quadratique)

Soient p et q deux nombres premiers impairs distincts. En posant $n = \frac{p-1}{2}$ et $m = \frac{q-1}{2}$, on a l'identité

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

Il existe plusieurs démonstrations de ce résultat (plus d'une centaine) ; celle que nous proposons ici s'appuie sur le théorème des restes chinois. Nous allons commencer par un simple résultat préliminaire.

Lemme 2

Pour tout nombre premier impair $p = 2n + 1$, on a la congruence

$$(n!)^2 \equiv (-1)^{n+1} \pmod{p}.$$

Démonstration. On commence par démontrer le *théorème de Wilson*, qui affirme que l'entier $(p-1)!$ est congru à -1 modulo p. Pour ce faire, il suffit de remarquer que l'image de $(p-1)!$ dans $\mathbb{F}_p$ est le produit de tous les éléments inversibles de ce dernier. Si $x \in \mathbb{F}_p^\times$ vérifie $x \neq x^{-1}$ alors ces deux éléments ne contribuent pas au produit, leur produit étant égal à 1. Il s'en suit que $(p-1)!$ est congru au produit des éléments de $\mathbb{F}_p^\times$ tels que $x = x^{-1}$, c'est à dire 1 et -1, d'où le résultat. Pour montrer le lemme, il suffit alors de considérer les relations

$$(p-1)! \equiv \prod_{i=1}^{n} i(p-i) \equiv (-1)^n (n!)^2 \pmod{p}.$$

□

Remarque. Si p est congru à 1 modulo 4, la congruence ci-dessus fournit une expression explicite l'une racine carrée de -1 dans $\mathbb{F}_p$. Il faut cependant remarquer qu'elle n'est pas très utile dans la pratique, car, pour des grandes valeurs de n, le calcul de $n!$ est coûteux en temps d'un point de vue numérique.

Une fois le lemme établi, nous pouvons passer à la démonstration de la loi de réciprocité quadratique : notons G le quotient du groupe $\mathbb{F}_p^\times \times \mathbb{F}_q^\times$ par le sous-groupe $\{(1,1),(-1,-1)\}$. Notre but est de calculer de deux manières différentes le produit t de tous les éléments de G. Indiquons par $[x,y]$ l'élément de G correspondant au couple $(x,y) \in \mathbb{F}_p^\times \times \mathbb{F}_q^\times$ (par la projection canonique $\mathbb{F}_p^\times \times \mathbb{F}_q^\times \to G$). Un élément de G s'écrit de manière unique comme $[a,b]$, avec $a,b \in \mathbb{Z}$ vérifiant $0 < a \leq n$ et $0 < b < q$. On obtient alors les relations

$$t = \prod_{g \in G} g = \prod_{a=1}^{n} \prod_{b=1}^{q-1} [a,b] = \prod_{a=1}^{n} \left[a^{q-1}, (q-1)!\right] = \left[(n!)^{2m}, ((q-1)!)^n\right].$$

En utilisant le lemme 2, on obtient donc l'expression

$$t = \left[\left((n!)^2\right)^m, (-1)^n\right] = \left[(-1)^{m(n+1)}, (-1)^n\right] = \left[(-1)^{mn+n+m}, 1\right].$$

D'autre part, le théorème des restes chinois affirme que $(\mathbb{F}_p)^\times \times (\mathbb{F}_q)^\times$ est isomorphe à $(\mathbb{Z}/pq\mathbb{Z})^\times$. Il s'en suit qu'un élément $x \in G$ s'écrit de manière unique comme $x = [a,a]$, où a appartient au sous-ensemble S de $\{1,\ldots,\frac{pq-1}{2}\}$ formé par les entiers premier avec p et q. Remarquons maintenant qu'un entier appartenant à $\{1,\ldots,\frac{pq-1}{2}\}$ ne peut être à la fois divisible par p et q. En posant

$$A = \prod_{a \in S} a \quad \text{et} \quad B = \prod_{a=1}^{n} qa,$$

et, en tenant compte de la relation $\frac{pq-1}{2} = mp + n$, on a alors l'identité

$$AB = \prod_{\substack{a=1 \\ \mathbf{pgcd}(a,p)=1}}^{mp+n} a.$$

On en déduit les congruences

$$\begin{cases} B \equiv q^n n! \equiv (\frac{q}{p}) n! \pmod{p}, \\ \\ AB \equiv ((p-1)!)^m n! \equiv (-1)^m n! \pmod{p}, \end{cases}$$

et finalement

$$A \equiv (-1)^m \left(\frac{q}{p}\right) \pmod{p}.$$

De manière tout à fait analogue, on obtient la congruence

$$A \equiv (-1)^n \left(\frac{p}{q}\right) \pmod{q},$$

et le théorème découle de l'identité $t = [A,A]$.