Université de Rennes 1
Préparation à l'agrégation de mathématiques
Auteur du document :

J-C. Raoult

Révisé : mars 2003

RESIDUS QUADRATIQUES

Voici une démonstration combinatoire, amusante et courte, du théorème de réciprocité quadratique, qui est une alternative à la démonstration habituelle utilisant les sommes de Gauss.

§ 1. Rappels sur les substitutions

On note $\varepsilon(\sigma)$ la signature de la substitution $\sigma : \{1,\dots,n\} \to \{1,\dots,n\}$ ou $\mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$, $A \times B$ le produit cartésien des ensembles A et B, et $A+B$ leur réunion disjointe (formellement, la réunion $\{1\} \times A \cup \{2\} \times B$).

PROPOSITION 1. —
a) $\varepsilon(\mathrm{id}) = 1,\ \varepsilon(\sigma^{-1}) = \varepsilon(\sigma),\ \varepsilon(\sigma \circ \tau) = \varepsilon(\sigma)\varepsilon(\tau)$.
b) $\varepsilon(\sigma+\tau) = \varepsilon(\sigma)\varepsilon(\tau)$ *où* $\sigma+\tau$ *est la substitution définie sur la somme par* σ *sur* $\mathbf{Z}/n\mathbf{Z}$ *et par* τ *sur* $\mathbf{Z}/m\mathbf{Z}$.
c) $\varepsilon(\sigma) = (-1)^{n-1}$ *lorsque* σ *est une permutation circulaire de n objets.*

a) et *b)* viennent de ce que le nombre de transpositions de $\sigma \circ \tau$, comme $\sigma+\tau$, est la somme des nombres de transpositions de σ et de τ. Enfin *c)* vient de la décomposition $(12\dots n) = (12)\cdots(1n)$, cqfd.

Par exemple l'application $x \mapsto x+1$ de $\mathbf{Z}/n\mathbf{Z} \to \mathrm{Z}/n\mathbf{Z}$ est une permutation circulaire et a donc pour signature $(-1)^{n-1}$. Et $x \mapsto x+k$ qui en est la puissance k-ième a pour signature $(-1)^{k(n-1)}$, d'après *a)*.

PROPOSITION 2. — *La substitution de* $\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$ *qui consiste à passer de l'ordre lexicographique de gauche à droite à l'ordre lexicographique de droite à gauche a pour signature* $(-1)^{\frac{n(n-1)}{2}\cdot\frac{m(m-1)}{2}}$.

On compte les inversions : $(i,j) < (i',j') \Leftrightarrow i < i'$ ou $(i = i'$ et $j < j')$ pour l'ordre lexicographique. Et $(i,j) > (i',j') \Leftrightarrow j > j'$ ou $(j = j'$ et $i > i')$ pour l'ordre lexicographique de droite à gauche. Seule possibilité : $i < i'$ et $j > j'$ soit $C_n^2 C_m^2$ inversions, cqfd.

DÉFINITION 3. — *On note* $\left(\frac{m}{n}\right) = \varepsilon(m)$ *la signature de la multiplication par m dans* $\mathbf{Z}/n\mathbf{Z}$ *et on l'appelle le symbole de Zolotarev.*

§ 2. La loi de réciprocité quadratique

On dit que m est un *résidu quadratique modulo n* si la classe de m est un carré dans $\mathbf{Z}/n\mathbf{Z}$. Dans le cas où n est un nombre premier >2, on définit le symbole de Legendre $\left(\frac{m}{n}\right)$ par

$$\left(\frac{m}{n}\right) = 1 \quad \text{si } m \text{ est un résidu quadratique modulo } n$$
$$= -1 \quad \text{sinon.}$$

C'est le morphisme $(\mathbf{Z}/n\mathbf{Z})^\times \to (\mathbf{Z}/n\mathbf{Z})^\times/(\mathbf{Z}/n\mathbf{Z})^{\times 2} \cong \{-1,+1\}$. On en déduit qu'il vérifie les deux propriétés énoncées dans la proposition suivante, ce qui implique qu'il est égal au symbole de Zolotarev

PROPOSITION 4. — *Le symbole de Zolotarev vérifie les propriétés suivantes :*

$$a)\ \left(\frac{mm'}{n}\right) = \left(\frac{m}{n}\right)\left(\frac{m'}{n}\right) \quad et$$
$$b)\ \left(\frac{m}{n}\right) \equiv m^{\frac{n-1}{2}} \pmod{n} \quad si\ n\ est\ premier$$

La première propriété vient de ce que la composition des multiplications par m et m' est la multiplication par mm'. Pour la seconde, notons r l'ordre de m dans le groupe cyclique $(\mathbf{Z}/n\mathbf{Z})^\times$. Ce groupe est divisé en $(n-1)/r$ orbites de r éléments. Sur chacune d'elles, la multiplication par m est une permutation circulaire. On a donc $\varepsilon(m) = (-1)^{(r-1)\frac{n-1}{r}}$. D'autre part, si r est pair, on a bien $m^{\frac{n-1}{2}} = \left(m^{\frac{r}{2}}\right)^{\frac{n-1}{r}} \equiv (-1)^{\frac{n-1}{r}} = \varepsilon(m)$. Si r est impair, $(n-1)$ est divisible par $2r$ et on a $m^{\frac{n-1}{2}} = \left(m^r\right)^{\frac{n-1}{2r}} \equiv 1 = \varepsilon(m)$, cqfd.

THÉORÈME 5. — *Si m et n sont impairs et premiers entre eux, ils vérifient la loi de réciprocité quadratique :*

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}$$

L'application $\sigma : \mathbf{Z}/n\mathbf{Z}\times\mathbf{Z}/m\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}\times\mathbf{Z}/m\mathbf{Z}$ définie par $(i,j) \mapsto (mi+j, j)$ a $\left(\frac{m}{n}\right)$ pour signature sur $\mathbf{Z}/n\mathbf{Z}\times\{j\}$ parce que c'est la composée de la multiplication par m et de la translation par j, qui est de signature 1 pour n impair. Comme j prend m valeurs (m impair), $\varepsilon(\sigma) = \left(\frac{m}{n}\right)$ (proposition 1*b)*). De même l'application $\tau : \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$ définie par $(i,j) \mapsto (i, nj+i)$ a pour signature $\varepsilon(\tau) = \left(\frac{n}{m}\right)$.

Mais la bijection $\mathbf{Z}/mn\mathbf{Z} \xrightarrow{\pi} \mathbf{Z}/n\mathbf{Z}\times\mathbf{Z}/m\mathbf{Z}$ vérifie $\pi(mi+j) = (mi+j, j)$ et $\pi(nj+i) = (i, nj+i)$. Donc, en notant $\lambda : \{0,\ldots,mn-1\} \to \{0,\ldots,mn-1\}$ la bijection $mi+j \mapsto nj+i$, on a

$$\lambda \circ \pi^{-1} \circ \sigma = \pi^{-1} \circ \tau.$$

Or λ est le passage de l'ordre lexicographique à l'ordre lexicographique de droite à gauche, d'où le résultat en appliquant les propositions 1 et 2.