Sur la loi de réciprocité quadratique

G. Rousseau

Résumé : une version de la cinquième preuve de Gauss de la loi de réciprocité quadratique est donnée qui utilise seulement des considérations simples de théorie des groupes (en se passant même du lemme de Gauss) et qui rend manifeste que la loi de réciprocité quadratique est une conséquence simple du théorème des restes chinois.

Comme on le sait, le critère d'Euler et les théorèmes de Fermat et Wilson peuvent être démontrés de manière très simple en déterminant de deux manières le produit des éléments d'un groupe abélien fini adéquat (cf. Dirichlet [2]). On montre qu'il en est de même pour la loi de réciprocité quadratique. Cette loi est ainsi vue comme ne dépendant de rien de plus mystérieux que du théorème des restes chinois, sans nécessiter de lemmes particuliers ou de considérations auxiliaires qui vont au-delà du domaine des simples congruences.

Pour un entier m, soit $\mathbb{Z}_m^*$ le groupe multiplicatif des restes réduits modulo m. Soient p et q deux nombres premiers impairs distincts. On détermine le produit π des éléments du groupe $G = (\mathbb{Z}_p^* \times \mathbb{Z}_q^*)/U$, où $U = \{(1,1),(-1,-1)\}$.

Clairement, $\{(i,j) : i = 1,2,...,p-1; j = 1,2,...,(q-1)/2\}$ est un système de représentants pour les cosets de U. Le produit des (i,j) est $((p-1)!^{(q-1)/2}, ((q-1)/2)!^{p-1})$, et $((q-1)/2)!^2 \equiv (-1)^{(q-1)/2}(q-1)! \pmod q$, donc

$$\pi = ((p-1)!^{(q-1)/2},\ \ (q-1)!^{(p-1)/2}(-1)^{((p-1)/2)((q-1)/2)})U.$$

L'ensemble $\{(k \bmod p, k \bmod q) : k = 1,2,...,(pq-1)/2 \ \ ; \ \ (k,pq) = 1\}$ est aussi un système de représentants pour les cosets de U parce que $\mathbb{Z}_{pq}^* \cong \mathbb{Z}_p^* \times \mathbb{Z}_q^*$ (théorème des restes chinois). Le produit des k, modulo p, est

$$\frac{\left(\prod_{i=1}^{p-1} i\right)\left(\prod_{i=1}^{p-1} p+i\right)\cdots\left(\prod_{i=1}^{p-1}\left(\frac{q-1}{2}-1\right)p+i\right)\left(\prod_{i=1}^{p-1}\frac{q-1}{2}p+i\right)}{1.q.2q\ldots\frac{p-1}{n}q} \equiv \frac{(p-1)!^{(q-1)/2}}{q^{(p-1)/2}},$$

avec une expression similaire pour le produit modulo q, donc par le critère d'Euler

$$\pi = ((p-1)!^{(q-1)/2}(q|p),\ \ (q-1)!^{(p-1)/2}(p|q))U.$$

Comparer les deux expressions pour π donne

$$(1,(-1)^{((p-1)/2)((q-1)/2)})U = ((q|p),(p|q))U$$

(Reçu le 21 décembre 1989),
Communiqué par J. H. Loxton.

J. Austral. Math. Soc. (Série A) 51 (1991), 423-425.

et par conséquent la loi de réciprocité quadratique,

$$(q|p) = (-1)^{((p-1)/2)((q-1)/2)}(p|q)$$

On note que, puisque la première expression pour π est symétrique en p et q, prendre $\{(i,j) : i = 1, 2, ..., (p-1)/2 \ ; \ j = 1, 2, ..., q-1\}$ comme système de représentants amènerait à la même expression. On obtient également la valeur réelle sans appliquer le théorème de Wilson :

$$\pi = (1, (-p|q)(-q|p))U = \begin{cases} (1,1)U & \text{si } p \equiv q \equiv 1 \pmod 4 \\ (1,-1)U & \text{sinon.} \end{cases}$$

La preuve ci-dessus nous a été suggérée par l'étude de la seconde preuve de H. Schmidt [4], qui est en retour (comme noté dans [1]) une variante de la cinquième preuve de Gauss [3]. La caractéristique remarquable de la preuve de Schmidt est qu'elle se dispense du lemme de Gauss alors qu'elle retient en effet l'idée implicite de ce dernier de considérer les quotients $\mathbb{Z}_m^*/\{1,-1\}$.

Références

[1] P. Bachmann, *Niedere Zahlentheorie* I, (Teubner, Leipzig, 1910, reprinted Chelsea, New York, 1968).

[2] P. G. L. Dirichlet, Démonstrations nouvelles de quelques théorèmes relatifs aux nombres, *J. Reine Angew. Math.* **3** (1828), 390-393.

[3] C. F. Gauss, *Werke* II, (K. Gesell. Wiss., Göttingen, 1870), 47-64.

[4] H. Schmidt, Drei neue Beweise des Reciprocitätssatzes in der Theorie der quadratischen Reste, *J. Reine Angew. Math.* **111** (1893), 107-120.

Université de Leicester,
LE1 7RH
Royaume uni