J. Austral. Math. Soc. (*Series A*) **51** (1991), 423–425

ON THE QUADRATIC RECIPROCITY LAW

G. ROUSSEAU

(Received 21 December 1989)

Communicated by J. H. Loxton

Abstract

A version of Gauss's fifth proof of the quadratic reciprocity law is given which uses only the simplest group-theoretic considerations (dispensing even with Gauss's Lemma) and makes manifest that the reciprocity law is a simple consequence of the Chinese Remainder Theorem.

1991 *Mathematics subject classification* (*Amer. Math. Soc.*) 11 A 15.

As is known, Euler's criterion and the theorems of Fermat and Wilson can be proved in a very simple manner by determining in two ways the product of the elements of a suitable finite abelian group (cf. Dirichlet [2]). We show that the same is true for the quadratic reciprocity law. This law is thus seen to depend on nothing more mysterious than the Chinese Remainder Theorem, without need for special lemmas or auxiliary considerations which go beyond the sphere of simple congruences.

For integer m let Z_m^* be the multiplicative group of reduced residues modulo m. Let p and q be distinct odd primes. We determine the product π of the elements of the group $G = (Z_p^* \times Z_q^*)/U$, where $U = \{(1, 1), (-1, -1)\}$.

Clearly $\{(i, j): i = 1, 2, \dots, p-1;\ j = 1, 2, \dots, (q-1)/2\}$ is a system of representatives for the cosets of U. The product of the (i, j) is $((p-1)!^{(q-1)/2}, ((q-1)/2)!^{p-1})$, and $((q-1)/2)!^2 \equiv (-1)^{(q-1)/2}(q-1)! \pmod q$, so

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

The set $\{(k \bmod p, k \bmod q): k = 1, 2, \ldots, (pq-1)/2;\ (k, pq) = 1\}$ is also a system of representatives for the cosets of U because $Z_{pq}^* \cong Z_p^* \times Z_q^*$ (Chinese Remainder Theorem). The product of the k, modulo p, is

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

with a similar expression for the product modulo q, so by Euler's criterion

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

Comparing the two expressions for π gives

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

and hence the reciprocity law,

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

We note that, since the first expression for π is symmetrical in p and q, taking $\{(i, j): i = 1, 2, \ldots, (p-1)/2;\ j = 1, 2, \ldots, q-1\}$ as system of representatives would lead to the same expression. Also we obtain the actual value of π on applying Wilson's Theorem:

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

The above proof was suggested by an analysis of the second proof of H. Schmidt [4], which is in turn (as noted in [1]) a variant of the fifth proof by Gauss [3]. The noteworthy feature of Schmidt's proof is that it dispenses with Gauss's Lemma whilst in effect retaining the idea implicit in the latter of considering quotients $Z_m^*/\{1, -1\}$.

References

[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.

The University
Leicester, LE1 7RH
England