

An elementary proof of quadratic reciprocity

Siddhartha Sahi
Rutgers University

November 2, 2007

Let $p = 2r + 1$ be an odd prime, an integer a is said to be a *quadratic residue* mod p if a is coprime to p and $a \equiv n^2 \pmod{p}$ for some n . We define

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p \\ 0 & \text{if } p \text{ divides } a \\ -1 & \text{otherwise} \end{cases}$$

following Legendre, and then we have $a^r \equiv \left(\frac{a}{p}\right) \pmod{p}$ (Euler's criterion). Gauss's law of quadratic reciprocity states:

Theorem 1 *If $p = 2r + 1, q = 2s + 1$ are different odd primes then*

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

We give an elementary (non-group theoretic) proof, inspired by Rouseau's group-theoretic simplification [2] of Schmid's second proof [3]. Schmid's proof was in turn inspired by Gauss's fifth proof [1].

For an odd integer m , define $H(m) = \{1 \leq a \leq (m-1)/2 : \gcd(a, m) = 1\}$. Then $R(m) = \{\pm n : n \in H(m)\}$ is a reduced residue set mod m .

Lemma 2 *Let h denote the product of the integers in $H(pq)$. Then we have*

$$h \equiv (-1)^s \left(\frac{q}{p}\right) \pmod{p}, \quad h \equiv (-1)^r \left(\frac{p}{q}\right) \pmod{q}. \quad (2)$$

Proof. By symmetry it suffices to prove the first congruence.

The set $H(pq)$ is obtained from $\{1, 2, \dots, (pq-1)/2\}$ by removing multiples of p and q . What are these multiples? Since $(pq-1)/2 = (p(2s+1)-1)/2 = sp+r$, we can arrange the integers in a table with p columns as follows:

1	...	r	...	$p-1$	p
$p+1$...	$p+r$...	$2p-1$	$2p$
\vdots	\ddots	\vdots	\ddots	\vdots	\vdots
$(s-1)p+1$...	$(s-1)p+r$...	$sp-1$	sp
$sp+1$...	$sp+r$			

The p -multiples appear in the last column and they are $\{p, 2p, \dots, sp\}$. By symmetry the q -multiples in the set are $\{q, 2q, \dots, rq\}$.

The integers in the first $p-1$ columns comprise the set $H(pq)$ plus the q -multiples, therefore their product is $hq^r r! \equiv h \left(\frac{q}{p}\right) r! \pmod{p}$ by Euler's criterion. However, we can also compute the same product row by row. The first row gives $(p-1)! \equiv -1 \pmod{p}$ by Wilson's theorem. Since the columns are congruent, the first s rows all give $-1 \pmod{p}$, while the last row gives $r! \pmod{p}$. Thus we get $h \left(\frac{q}{p}\right) r! \equiv (-1)^s r! \pmod{p}$. Since $\left(\frac{q}{p}\right)^2 = (\pm 1)^2 = 1$, multiplying by $\left(\frac{q}{p}\right)$ we get $hr! \equiv (-1)^s \left(\frac{q}{p}\right) r! \pmod{p}$.

We may cancel $r!$ since it is coprime to p , and the result follows. ■

Proof. (of quadratic reciprocity (1)). For each integer x in $R(pq)$, there are unique integers $f(x) \in R(p)$, $g(x) \in R(q)$ which are congruent to $x \pmod{p}$ and \pmod{q} respectively. Then with h as in the previous lemma we have

$$h \equiv \prod_{x \in H(pq)} f(x) \pmod{p}, \quad h \equiv \prod_{x \in H(pq)} g(x) \pmod{q}. \quad (3)$$

By the Chinese remainder theorem, the map $x \mapsto (f(x), g(x))$ is a one-to-one correspondence from $R(pq)$ to the set $R(p) \times R(q)$. We construct a table of 2×2 blocks with rows $\pm i$ from $R(p)$ and columns $\pm j$ from $R(q)$, writing the integer x in $R(pq)$ in row $f(x)$ and column $g(x)$.

The table for $p=3, q=5$ and the general (i, j) block are as follows

$$\begin{array}{c} 1 \\ -1 \end{array} \begin{array}{|cc|cc|} \hline 1 & -1 & 2 & -2 \\ \hline 1 & 4 & 7 & -2 \\ \hline -4 & -1 & 2 & -7 \\ \hline \end{array} \quad \begin{array}{c} i \\ -i \end{array} \begin{array}{|cc|} \hline j & -j \\ \hline * & \# \\ \hline \# & * \\ \hline \end{array}$$

Since $f(-x) = -f(x)$ and $g(-x) = -g(x)$, within each block the two entries marked $*$ are mutual negatives as are the two $\#$ -entries. Hence exactly one of each kind belongs to $H(pq)$ and contributes to the two products in (3).

Thus up to sign, the (i, j) block gives two (row) factors of i for the first product and two (column) factors of j for the second product in (3). As for the signs, the $*$ -entries give the same sign in the two products while the $\#$ -entries give opposite signs. Since there are rs blocks, up to some overall sign ε we have

$$\prod_{x \in H(pq)} f(x) = \varepsilon (r!)^{2s}, \quad \prod_{x \in H(pq)} g(x) = (-1)^{rs} \varepsilon (s!)^{2r}. \quad (4)$$

Applying Wilson's theorem to the complete residue system $R(p)$ we get $(-1)^r (r!)^2 \equiv -1 \pmod{p}$. Hence $(r!)^{2s} \equiv (-1)^s (-1)^{rs} \pmod{p}$. By symmetry $(s!)^{2r} \equiv (-1)^r (-1)^{rs} \pmod{q}$ and so by (3) and (4) we get

$$h \equiv \varepsilon (-1)^s (-1)^{rs} \pmod{p}, \quad h \equiv \varepsilon (-1)^r \pmod{q}.$$

Now from (2) we deduce $\varepsilon (-1)^{rs} = \left(\frac{q}{p}\right)$, $\varepsilon = \left(\frac{p}{q}\right)$, and (1) follows. ■

References

- [1] C.F. Gauss, *Werke II*, (K. Gessell. Wiss., Göttingen) (1870), 47-64
- [2] G. Rousseau, *On the Quadratic Reciprocity Law*, J Austral Math Soc Ser A **51** (1991), 423–425
- [3] H. Schmidt, *Drei neue Beweise des Reciprocitätssatzes in der Theorie der quadratischen Reste*, J. reine. Angew. Math. **111** (1893), 107-120