A simple proof of the quadratic reciprocity law

Larry Hammick

31 May 2002

Abstract

For any distinct odd primes p and q, a certain simple bijection of $\mathbb{Z}/(pq)$ onto $\mathbb{Z}/(p) \times \mathbb{Z}/(q)$ embodies the hypotheses of Gauss's lemma for both $(\frac{q}{p})$ and $(\frac{p}{q})$. With the help of an elementary counting argument, the quadratic reciprocity law follows.

Throughout, $p = 2a + 1$ and $q = 2b + 1$ are distinct odd primes. For $x, y \in \mathbb{Z}$, $[x,y]$ will denote the interval $\{z \in \mathbb{Z} | x \le z \le y\}$ of $\mathbb{Z}$. For a prime r and an integer m, $(\frac{m}{r})$ is the Legendre symbol, equal to 0 if $r|m$, to 1 if m is a nonzero square mod r, and to -1 otherwise.

The quadratic reciprocity law is:

Proposition (Gauss). With the above notation,

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

We will use the following well-known lemma, for which see e.g. [1, p.9].

Gauss's lemma. Let m be an integer not divisible by p, and let u be the number of elements of $\{m, 2m, \ldots, am\}$ which are congruent mod p to some element of $\{-a, -a+1, \ldots, -1\}$. Then $\left(\frac{m}{p}\right) = (-1)^u$.

There exist unique functions

$$f : \mathbb{Z} \to [-a, a]$$

$$g : \mathbb{Z} \to [-b, b]$$

such that for all $m \in \mathbb{Z}$

$$f(m) \equiv m \pmod{p}$$

$$g(m) \equiv m \pmod{q}.$$

Denote by R the interval $[-(pq-1)/2, (pq-1)/2]$ of $\mathbb{Z}$, and by S the subset $[-a, a] \times [-b, b]$ of $\mathbb{Z} \times \mathbb{Z}$. Denote by h the mapping $m \mapsto (f(m), g(m))$ of R into S. The Chinese remainder theorem shows that h is a bijection. Let P be the image of the restriction of h to $[1, (pq-1)/2]$. We will examine how the elements of P are distributed among the quadrants and semiaxes of S.

Write

$$\begin{aligned} P_0 &= \{(x, y) \in P | x > 0, y > 0\} \\ P_1 &= \{(x, y) \in P | x < 0, y \geq 0\} \\ P_2 &= \{(x, y) \in P | x \geq 0, y < 0\} \end{aligned}$$

and let N_i be the cardinal of P_i for each i.

There are a elements of P on the axis $g = 0$, namely $h(mq)$ for each $m \in [1, a]$. Denote by u the number of such points having $f < 0$. Likewise P has b elements on the axis $f = 0$, and we denote by v the number of them which have $g < 0$.

P has $ab + a$ elements in the region $g > 0$, namely $h(m)$ for all m of the form $k + lp$ with $1 \leq k \leq a$ and $0 \leq l \leq b$. Thus

$$N_0 + N_1 = ab + b - (b - v) + u$$

i.e.

$$N_0 + N_1 = ab + u + v. \tag{1}$$

In the same way,

$$N_0 + N_2 = ab + u + v. \tag{2}$$

For any $m \in \mathbb{Z}$,

$$f(-m) = -f(m)$$

$$g(-m) = -g(m).$$

It follows that for any $(x, y) \in S$ other than $(0, 0)$, either (x, y) or $(-x, -y)$ is in P, but not both. Therefore

$$N_1 + N_2 = ab + u + v. \tag{3}$$

Adding (1), (2), and (3) gives us

$$0 \equiv ab + u + v \pmod 2$$

so

$$(-1)^{ab} = (-1)^u(-1)^v$$

which, in view of Gauss's lemma, is the desired conclusion.

Reference

[1] J.-P. Serre, A Course in Arithmetic (Springer-Verlag, New York, 1970).

Postscript

G. Rousseau (On the quadratic reciprocity law, J. Austral. Math. Soc. 51 (1991), 423-425) has given a proof of the QRL which uses, instead of additive groups, the multiplicative groups of invertible residue classes mod p, mod q, and mod pq. It is shorter than the above, and does not lean on Gauss's lemma.

If we define a fourth region

$$P_3 = \{(x, y) \in P | x \le 0, y \le 0\}$$

with, let us say, N_3 elements, then a linear calculation gives

$$N_i = k/2$$

for all four values of i, where $k = ab + u + v$. This again shows $k \equiv 0 \pmod 2$. But moreover $k \equiv 0 \pmod 4$. Let me just sketch a proof. The lower left region P_3 is symmetric under a half-turn around its center. One verifies

– the half-turn maps elements of P to elements of P

– the half-turn has no fixed points except its centre

– the centre, if it is a lattice point, is not in P.

Thus the $k/2$ elements in the region fall into orbits each of which contains two elements.

More is true. Let's say that a point $(x, y) \in P$ is "verticle" (resp. "horizontal") if $(x, -y) \in P$ (resp. $(-x, y) \in P$). It is easy to see that every element of P is verticle or horizontal and not both. But in fact each of the sets P_i contains $k/4$ verticle and $k/4$ horizontal elements. The proof is not easy.

We cannot define h simply as "the" mapping

$$\begin{aligned} m &\mapsto (m, m) && (4) \\ \mathbb{Z}/(pq) &\to \mathbb{Z}/(p) \times \mathbb{Z}/(q), && (5) \end{aligned}$$

like a curve on a torus, because the bijection (5) is not canonical.