Appendix C

Quadratic Reciprocity: an alternative proof

Hundreds of different proofs of this theorem have been published. Gauss, who first proved the result in 1801, gave eight different proofs. We gave a group-theoretic proof in chapter 10. Here is a shorter combinatorial proof.

Theorem C.1. *(The Law of Quadratic Reciprocity) Suppose $p, q \in \mathbb{N}$ are odd primes. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \begin{cases} -1 & \text{if } p \equiv q \equiv 3 \bmod 4 \\ 1 & \text{otherwise.} \end{cases}$$

Proof. Let

$$S = \{1, 2, \dots, \frac{p-1}{2}\},\ T = \{1, 2, \dots, \frac{q-1}{2}\}.$$

We shall choose remainders $\bmod p$ from the set

$$\{-\frac{p}{2} < i < \frac{p}{2}\} = -S \cup \{0\} \cup S,$$

and remainders $\bmod q$ from the set

$$\{-\frac{q}{2} < i < \frac{q}{2}\} = -T \cup \{0\} \cup T.$$

By Gauss' Lemma,

$$\left(\frac{q}{p}\right) = (-1)^{\mu},\ \left(\frac{p}{q}\right) = (-1)^{\nu}.$$

Writing $\#X$ for the number of elements in the set X,

$$\mu = \#\{i \in S : qi \bmod p \in -S\},\ \nu = \#\{i \in T : pi \bmod q \in -T\}.$$

By '$qi \bmod p \in -S$' we mean that there exists a j (necessarily unique) such that

$$qi - pj \in -S.$$

But now we observe that, in this last formula,

$$0 < i < \frac{p}{2} \implies 0 < j < \frac{q}{2}.$$

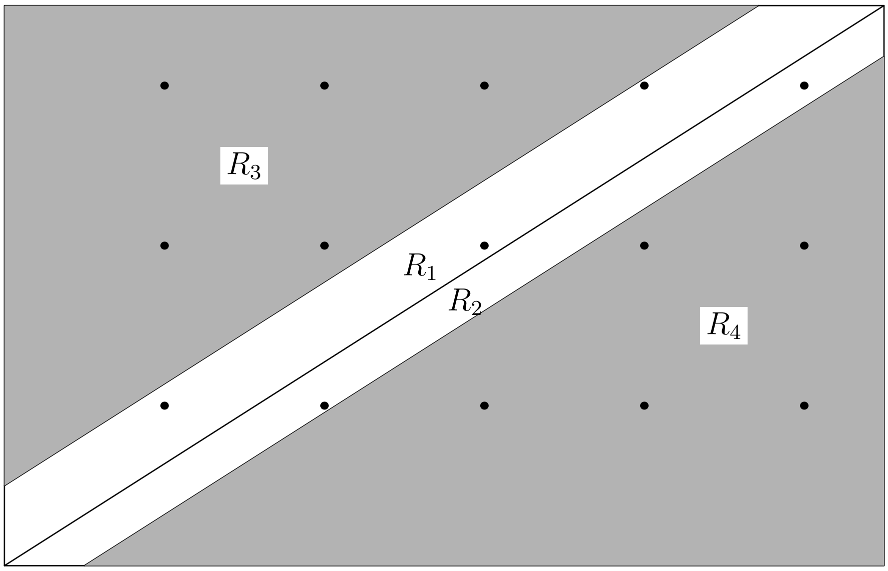

Figure C.1: $p = 11,\ q = 7$

The basic idea of the proof is to associate to each such contribution to μ the 'point' $(i, j) \in S \times T$. Thus

$$\mu = \#\{(i,j) \in S \times T : -\frac{p}{2} < qi - pj < 0\};$$

and similarly

$$\nu = \#\{(i,j) \in S \times T : 0 < qi - pj < \frac{q}{2}\},$$

where we have reversed the order of the inequality on the right so that both formulae are expressed in terms of $(qi - pj)$.

Let us write $[R]$ for the number of integer points in the region $R \subset \mathbb{R}^2$. Then

$$\mu = [R_1],\ \nu = [R_2],$$

where

$$R_1 = \{(x,y) \in R : -\frac{p}{2} < qx - py < 0\},\ R_2 = \{(x,y) \in R : 0 < qx - py < \frac{q}{2}\},$$

and R denotes the rectangle

$$R = \{(x,y) : 0 < x < \frac{p}{2},\ 0 < y < \frac{p}{2}\}.$$

The line

$$qx - py = 0$$

is a diagonal of the rectangle R, and R_1, R_2 are strips above and below the diagonal (Fig C).

This leaves two triangular regions in R,

$$R_3 = \{(x,y) \in R : qx - py < -\frac{p}{2}\},\ R_4 = \{(x,y) \in R : qx - py > \frac{q}{2}\}.$$

We shall show that, surprisingly perhaps, reflection in a central point sends the integer points in these two regions into each other, so that

$$[R_3] = [R_4].$$

Since

$$R = R_1 \cup R_2 \cup R_3 \cup R_4,$$

it will follow that

$$[R_1] + [R_2] + [R_3] + [R_4] = [R] = \frac{p-1}{2}\frac{q-1}{2},$$

ie

$$\mu + \nu + [R_3] + [R_4] = \frac{p-1}{2}\frac{q-1}{2}.$$

But if now $[R_3] = [R_4]$ then it will follow that

$$\mu + \nu \equiv \frac{p-1}{2}\frac{q-1}{2} \bmod 2,$$

which is exactly what we have to prove.

It remains to define our central reflection. Note that reflection in the centre $(\frac{p}{4}, \frac{q}{4})$ of the rectangle R will not serve, since this does not send integer points into integer points. For that, we must reflect in a point whose coordinates are integers or half-integers.

We choose this point by "shrinking" the rectangle R to a rectangle bounded by integer points, ie the rectangle

$$R' = \{1 \le x \le \frac{p-1}{2},\ 1 \le y \le \frac{q-1}{2}\}.$$

Now we take P to be the centre of this rectangle, ie

$$P = (\frac{p+1}{2},\ \frac{q+1}{2}).$$

The reflection is then given by

$$(x, y) \mapsto (X, Y) = (p + 1 - x, q + 1 - y).$$

It is clear that reflection in P will send the integer points of R into themselves. But it is not clear that it will send the integer points in R_3 into those in R_4, and vice versa. To see that, let us shrink these triangles as we shrank the rectangle. If $x, y \in \mathbb{Z}$ then

$$qx - py < -\frac{p}{2} \implies qx - py \le -\frac{p+1}{2};$$

and similarly

$$qx - py > \frac{q}{2} \implies qx - py \ge \frac{q+1}{2}.$$

Now reflection in P *does* send the two lines

$$qx - py = -\frac{p+1}{2}, \; qx - py = \frac{q+1}{2}$$

into each other; for

$$qX - pY = q(p + 1 - x) - p(q + 1 - y) = (q - p) - (qx - py),$$

and so

$$qx - py = -\frac{p+1}{2} \iff qX - pY = (q - p) + \frac{p+1}{2} = \frac{q+1}{2}.$$

We conclude that

$$[R_3] = [R_4].$$

Hence

$$[R] = [R_1] + [R_2] + [R_3] + [R_4] \equiv \mu + \nu \bmod 2,$$

and so

$$\mu + \nu \equiv [R] = \frac{p-1}{2}\frac{q-1}{2}.$$

$\square$

Example: Take $p = 37,\ q = 47$. Then

$$\begin{aligned}
\left(\frac{37}{47}\right) &= \left(\frac{47}{37}\right) \text{ since } 37 \equiv 1 \bmod 4 \\
&= \left(\frac{10}{37}\right) \\
&= \left(\frac{2}{37}\right)\left(\frac{5}{37}\right) \\
&= -\left(\frac{5}{37}\right) \text{ since } 37 \equiv -3 \bmod 8 \\
&= -\left(\frac{37}{5}\right) \text{ since } 5 \equiv 1 \bmod 4 \\
&= -\left(\frac{2}{5}\right) \\
&= -(-1) = 1.
\end{aligned}$$

Thus 37 *is* a quadratic residue $\bmod 47$.

We could have avoided using the result for $\left(\frac{2}{p}\right)$:

$$\begin{aligned}
\left(\frac{10}{37}\right) &= \left(\frac{-27}{37}\right) \\
&= \left(\frac{-1}{37}\right)\left(\frac{3}{37}\right)^3 \\
&= (-1)^{18}\left(\frac{37}{3}\right) \\
&= \left(\frac{1}{3}\right) = 1.
\end{aligned}$$