Quadratic reciprocity: a lattice point proof

Robin Chapman

24 September 2013

This is the proof of quadratic reciprocity given by Hardy and Wright in *An Introduction to the Theory of Numbers*. It is shorter than that in Davenport's *The Higher Arithmetic* but its motivation is much more opaque.

Let p and q be distinct odd primes. Let

$$R = \{(x, y) \in \mathbf{Z}^2 : 0 < x < p/2, 0 < y < q/2\}.$$

We can regard R as the set of "lattice points" in the interior of the rectangle with vertices $(0, 0)$, $(p/2, 0)$, $(0, q/2)$ and $(p/2, q/2)$. The x-coordinates of points in R lie in the set $\{1, 2, \ldots, \frac{1}{2}(p-1)\}$ and the y-coordinates lie in the set $\{1, 2, \ldots, \frac{1}{2}(q-1)\}$. Thus

$$|R| = \frac{p-1}{2} \times \frac{q-1}{2}.$$

So $|R|$ is even unless $p \equiv q \equiv 3 \pmod 4$ when $|R|$ is odd. So the Law of Quadratic Reciprocity is equivalent to

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

We study what Gauss's lemma tells us about $\left(\frac{q}{p}\right)$. It equals $(-1)^\mu$ where μ is the number of elements $x \in \{1, \ldots, \frac{1}{2}(p-1)\}$ for which qx is p-negative. Now qx is p-negative if and only if there is an integer y such that $py - p/2 < qx < py$. We claim that for this integer y, the point (x, y) lies in R. To see this we have

$$\frac{q}{p}x < y < \frac{q}{p}x + \frac{1}{2}$$

and as $x > 0$ and $x < p/2$ then $0 < y < \frac{1}{2}(q+1)/2$. As $\frac{1}{2}(q+1)$ is the next integer after $\frac{1}{2}(q-1)$ then $0 < y \le frac12(q-1) < q/2$. Hence $(x, y) \in R$ and $0 > qx - py > -p/2$. Let

$$R_1 = \{(x, y) \in R : 0 > qx - py > -p/2\}.$$

Then $0 < x < p/2$ and the $py > qx > py - p/2$ proving that qx is p-negative. So $|R_1|$ is the number of $x \in \{1, \dots, \frac{1}{2}(p-1)\}$ for which qx is p-negative, that is $|R_1| = \mu$. Hence $\left(\frac{q}{p}\right) = (-1)^{|R_1|}$.

Swapping over p and q (and x and y) we get that similarly $\left(\frac{p}{q}\right) = (-1)^{|R_2|}$ where

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

The sets R_1 and R_2 are disjoint, so that

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{|R_1 \cup R_2|}.$$

I claim there are no points on the line $qx - py = 0$ inside R. For such a point $qx = py$ is a multiple of pq and also positive, so at least pq. Thus $x \geq pq/q = p$ which is impossible. Therefore

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

The complement of $R_1 \cup R_2$ in R is $R_3 \cup R_4$ where

$$R_3 = \{(x, y) \in R : qx - py \leq -p/2\}$$

and

$$R_4 = \{(x, y) \in R : qx - py \geq q/2\}$$

(which are obviously disjoint). I claim that R_3 and R_4 have the same number of elements. If $(x, y) \in R$ then $\phi(x, y) = (x', y') \in R$ where $x' = \frac{1}{2}(p+1) - x$ and $y' = \frac{1}{2}(q+1) - y$. Clearly $\phi(\phi(x, y)) = (x, y)$ so that ϕ is bijective. Also for $(x, y) \in R$ then $(x, y) \in R_3$ if and only if $qx - py \leq -p/2$ if and only if

$$q\left(\frac{p+1}{2} - x'\right) - p\left(\frac{q+1}{2} - y'\right) \leq -p/2$$

if and only if

$$\frac{q-p}{2} - (qx' - py') \leq -p/2$$

if and only if $q/2 \leq qx' - py'$ if and only if $(x', y') \in R_4$. Then $\phi(R_3) = R_4$ and as ϕ is bijective, $|R_4| = |R_3|$. Thus

$$|R_1 \cup R_2| = |R| - |R_3| - |R_4| = |R| - 2|R_3| \equiv |R| \pmod 2$$

so that

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{|R_1 \cup R_2|} = (-1)^{|R|}$$

which is the Law of Quadratic Reciprocity.