The Law of Quadratic Reciprocity

LEMMA: If p is an odd prime and a is an odd integer not divisible by p, then

$$\left(\frac{a}{p}\right) = (-1)^{T(a,p)}$$

where

$$T(a,p) = \sum_{j=1}^{(p-1)/2} \left[\frac{ja}{p}\right]$$

Proof: Consider the least positive residues of the integers

$$a,\ 2a,\ \ldots,\ \frac{p-1}{2}a$$

Let $u_1, u_2, \ldots, u_s$ be those greater than $p/2$ and let $v_1, v_2, \ldots, v_t$ be those less than $p/2$. The division algorithm tells us that

$$ja = p\left[\frac{ja}{p}\right] + \text{ remainder}$$

where the remainder is one of the u_j or v_j. By adding the $(p-1)/2$ equations of this sort, we obtain

$$\sum_{j=1}^{(p-1)/2} ja = \sum_{j=1}^{(p-1)/2} p\left[\frac{ja}{p}\right] + \sum_{j=1}^{s} u_j + \sum_{j=1}^{t} v_j \tag{1}$$

As we showed in the proof of Gauss's lemma, the integers

$$p-u_1, \quad p-u_2, \quad \ldots, \quad p-u_s, \quad v_1, \quad v_2, \quad \ldots, \quad v_t$$

are precisely the integers $1, 2, \ldots, (p-1)/2$, in some order. Hence, summing all these integers, we obtain

$$\sum_{j=1}^{(p-1)/2} j = \sum_{j=1}^{s}(p-u_j) + \sum_{j=1}^{t} v_j = ps - \sum_{j=1}^{s} u_j + \sum_{j=1}^{t} v_j \tag{2}$$

Subtracting (2) from (1), we find that

$$\sum_{j=1}^{(p-1)/2} ja - \sum_{j=1}^{(p-1)/2} j = \sum_{j=1}^{(p-1)/2} p\left[\frac{ja}{p}\right] - ps + 2\sum_{j=1}^{s} u_j$$

or, equivalently, since $T(a,p) = \displaystyle\sum_{j=1}^{(p-1)/2} \left[\frac{ja}{p}\right]$,

$$(a-1)\sum_{j=1}^{(p-1)/2} j = pT(a,p) - ps + 2\sum_{j=1}^{s} u_j$$

which can be rewritten as

$$(a-1)\sum_{j=1}^{(p-1)/2} j - 2\sum_{j=1}^{s} u_j = p(T(a,p) - s)$$

Since the left-hand side is divisible by 2, $p(T(a,p)-s)$ is also divisible by 2. But $(p,2)=1$, therefore $2 \mid T(a,p)-s$ by Theorem 1 from Section 3.5. Hence,

$$T(a,p) \equiv s \pmod 2$$

which implies $(-1)^s = (-1)^{T(a,p)}$. To finish the proof, we note that from Gauss's lemma

$$\left(\frac{a}{p}\right) = (-1)^s$$

therefore $\left(\frac{a}{p}\right) = (-1)^{T(a,p)}$. ■

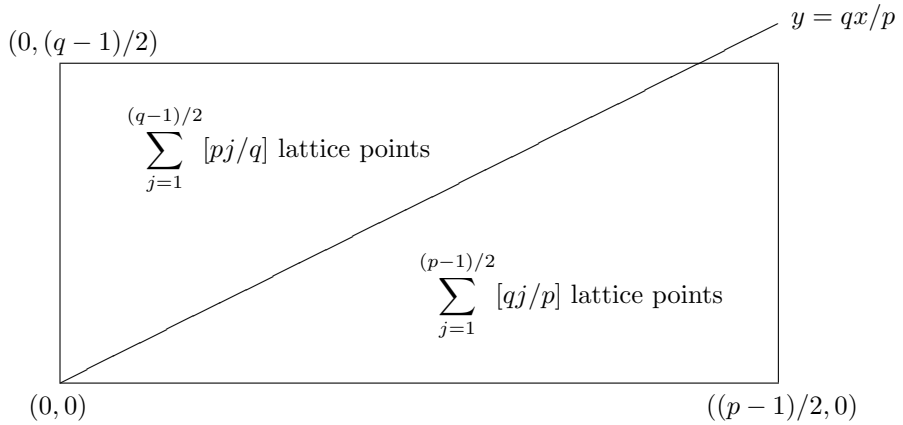
THEOREM (The Law of Quadratic Reciprocity): Let p and q be distinct odd primes. Then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

Proof: We consider pairs of integers (x,y) with $1 \le x \le (p-1)/2$ and $1 \le y \le (q-1)/2$. There are

$$\frac{p-1}{2}\cdot\frac{q-1}{2}$$

such pairs. We divide these pairs into two groups, depending on the relative sizes of qx and py.



First, we note that $qx \ne py$ for all of these pairs. For if $qx = py$, then $q \mid py$, which implies that $q \mid p$ or $q \mid y$. However, since q and p are distinct primes, we know that $q \nmid p$, and since $1 \le y \le (q-1)/2$, we know that $q \nmid y$.

To enumerate the pairs of integers (x,y) with

$$1 \le x \le (p-1)/2, \quad 1 \le y \le (q-1)/2, \quad \text{and} \quad qx > py \tag{3}$$

we note that these pairs are precisely those where

$$1 \le x \le (p-1)/2 \quad \text{and} \quad 1 \le y < qx/p \tag{4}$$

because $y < qx/p$ and $x \le (p-1)/2$ imply $y \le (q-1)/2$. Indeed,

$$y < \frac{qx}{p} = \frac{q}{p}\cdot x \le \frac{q}{p}\cdot\frac{p-1}{2} = \frac{q}{2}\cdot\frac{p-1}{p} < \frac{q}{2}$$

So, $y < q/2$, therefore $y \le (q-1)/2$, since y is an integer number.

From (4) it follows that for each fixed value of the integer x, where $1 \leq x \leq (p-1)/2$, there are $[qx/p]$ integers satisfying (3). Consequently, the total number of pairs of integers (x, y) satisfying (3) is

$$\sum_{j=1}^{(p-1)/2} \left[\frac{qj}{p}\right]$$

We now consider the pairs of integers (x, y) with

$$1 \leq x \leq (p-1)/2, \quad 1 \leq y \leq (q-1)/2, \quad \text{and} \quad qx < py \tag{5}$$

These pairs are precisely the pairs of integers (x, y) with

$$1 \leq y \leq (q-1)/2 \quad \text{and} \quad 1 \leq x < py/q \tag{6}$$

because $x < py/q$ and $y \leq (q-1)/2$ imply $x \leq (p-1)/2$. Indeed,

$$x < \frac{py}{q} = \frac{p}{q} \cdot y \leq \frac{p}{q} \cdot \frac{q-1}{2} = \frac{p}{2} \cdot \frac{q-1}{q} < \frac{p}{2}$$

So, $x < p/2$, therefore $x \leq (p-1)/2$, since x is an integer number.

From (6) it follows that for each fixed value of the integer y, where $1 \leq y \leq (q-1)/2$, there are exactly $[py/q]$ integers x satisfying (5). This shows that the total number of pairs of integers (x, y) satisfying (5) is

$$\sum_{j=1}^{(q-1)/2} \left[\frac{pj}{q}\right]$$

Adding the numbers of pairs in these classes, and recalling that the total number of such pairs

$$\frac{p-1}{2} \cdot \frac{q-1}{2}$$

we see that

$$\sum_{j=1}^{(p-1)/2} \left[\frac{qj}{p}\right] + \sum_{j=1}^{(q-1)/2} \left[\frac{pj}{q}\right] = \frac{p-1}{2} \cdot \frac{q-1}{2}$$

or, using the notation of the Lemma above,

$$T(q, p) + T(p, q) = \frac{p-1}{2} \cdot \frac{q-1}{2}$$

Hence,

$$(-1)^{T(q,p)+T(p,q)} = (-1)^{T(q,p)}(-1)^{T(p,q)} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

The Lemma above tells us that

$$(-1)^{T(q,p)} = \left(\frac{q}{p}\right) \quad \text{and} \quad (-1)^{T(p,q)} = \left(\frac{p}{q}\right)$$

Hence

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

This concludes the proof of the law of quadratic reciprocity. ■