The Law of Quadratic Reciprocity

Ryan C. Daileda

Trinity University

Number Theory

Introduction

Given odd primes $p \neq q$, the Law of Quadratic Reciprocity gives an explicit relationship between the congruences $x^2 \equiv q \pmod{p}$ and $x^2 \equiv p \pmod{q}$.

Euler first conjectured the Law around 1783, but Gauss was the first to give a complete proof in 1798 (when he was about 20 years old).

Gauss referred to the Law of Quadratic Reciprocity as "the fundamental theorem," and found (at least) 6 different proofs during his lifetime.

Quadratic reciprocity is a favorite of number theorists. There are more than 240 published proofs, and it has far reaching generalizations.

We shall need the following explicit reformulation of Gauss' Lemma.

Lemma 1

If p is an odd prime and $a \in \mathbb{Z}$ is odd with $p \nmid a$, then

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{(p-1)/2} [ka/p]}.$$

Proof. As in Gauss' Lemma, let

$$L = \{r + p\mathbb{Z} \,|\, 1 \leq r < p/2\}$$

and let n be the number of $ar + p\mathbb{Z} \notin L$.
Recall the bijection $T_a : L \to L$ given by

$$T_a(r + p\mathbb{Z}) = \begin{cases} ar + p\mathbb{Z} & \text{if } ar + p\mathbb{Z} \in L, \\ -ar + p\mathbb{Z} & \text{otherwise.} \end{cases}$$

For $1 \leq r < p/2$, write

$$ar = q_r p + t_r,$$

where $1 \leq t_r < p$. Then

$$T_a(r + p\mathbb{Z}) = \begin{cases} t_r + p\mathbb{Z} & \text{if } t_r < p/2, \\ (p - t_r) + p\mathbb{Z} & \text{if } t_r > p/2. \end{cases}$$

Since $T_a : L \to L$ is a bijection,

$$\sum_{r=1}^{(p-1)/2} r = \sum_{t_r < p/2} t_r + \sum_{t_r > p/2} (p - t_r) = pn + \sum_{t_r < p/2} t_r - \sum_{t_r > p/2} t_r$$

$$\equiv n + \sum_{r=1}^{(p-1)/2} t_r \equiv n + \sum_{r=1}^{(p-1)/2} (ar - pq_r) \pmod 2.$$

But $a \equiv p \equiv 1 \pmod 2$, so this becomes

$$\sum_{r=1}^{(p-1)/2} r \equiv n + \sum_{r=1}^{(p-1)/2} (r - q_r) \equiv n + \sum_{r=1}^{(p-1)/2} r - \sum_{r=1}^{(p-1)/2} q_r \pmod 2.$$

However, $q_r = \frac{ar-t_r}{p} \leq \frac{ar}{p} < \frac{ar+(p-t_r)}{p} = q_r + 1$, so that

$$\left[\frac{ar}{p}\right] = q_r.$$

Thus

$$n \equiv \sum_{r=1}^{(p-1)/2} q_r \equiv \sum_{r=1}^{(p-1)/2} \left[\frac{ar}{p}\right] \pmod 2.$$

The result now follows from Gauss' Lemma. $\square$

Example 1

Use Lemma 1 to compute $\left(\frac{6}{17}\right)$.

Solution. Taking $p = 17$ and $a = 11$ (since 6 is even) in Lemma 1, we find that

$$
\begin{aligned}
n &\equiv \sum_{k=1}^{8} \left[\frac{11k}{17}\right] \pmod 2 \\
&= \left[\frac{11}{17}\right] + \left[\frac{22}{17}\right] + \left[\frac{33}{17}\right] + \left[\frac{44}{17}\right] + \left[\frac{55}{17}\right] + \left[\frac{66}{17}\right] + \left[\frac{77}{17}\right] + \left[\frac{88}{17}\right] \\
&= 0 + 1 + 1 + 2 + 3 + 3 + 4 + 5 \equiv 1 \pmod 2.
\end{aligned}
$$

Thus $\left(\frac{6}{17}\right) = \left(\frac{-11}{17}\right) = \left(\frac{-1}{17}\right)\left(\frac{11}{17}\right) = (-1)^n = -1$, by Lemma 1. $\square$

Theorem 1 (Law of Quadratic Reciprocity)

Let p and q be odd primes. Then

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

Proof. Let

$$L_p = \{r \in \mathbb{Z} \,|\, 0 < r < p/2\} \quad \text{and} \quad L_q = \{s \in \mathbb{Z} \,|\, 0 < s < q/2\},$$

and consider the rectangle of lattice points $R_{pq} = L_p \times L_q$ in $\mathbb{R}^2$.

The line $s = (q/p)r$ passes through the diagonal of R_{pq}, but never hits any point in R_{pq}, because $(r, s) \in \mathbb{Z} \times \mathbb{Z}$ lies on $s = (q/p)r$ iff

$$ps = qr \;\Rightarrow\; p|r \text{ and } q|s \;\Rightarrow\; p \le r \text{ and } q \le s.$$

Thus we may divide R_{pq} into the disjoint subsets

$$A = \{(r,s) \in R_{pq} \,|\, s > (q/p)r\} \quad \text{and} \quad B = \{(r,s) \in R_{pq} \,|\, s < (q/p)r\},$$

consisting of those points Above and those points Below the diagonal.

Suppose we count B by columns. If $0 < r < p/2$, then $(r,s) \in B$ iff $0 < s < (q/p)r$.

Thus there are $\left[\frac{qr}{p}\right]$ elements of B in the rth column.

Hence

$$|B| = \sum_{r=1}^{(p-1)/2} \left[\frac{qr}{p}\right] \;\Rightarrow\; \left(\frac{q}{p}\right) = (-1)^{|B|},$$

by Lemma 1. Counting A instead by rows we arrive at the symmetric relation

$$|A| = \sum_{s=1}^{(q-1)/2} \left[\frac{ps}{q}\right] \;\Rightarrow\; \left(\frac{p}{q}\right) = (-1)^{|A|}.$$

Since $|A| + |B| = |R_{pq}| = \frac{p-1}{2} \cdot \frac{q-1}{2}$, we find that

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{|A|+|B|} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}},$$

which is equivalent to the result. $\square$

Example 2

Use quadratic reciprocity to compute $\left(\frac{430}{541}\right)$.

Solution. We have

$$\begin{aligned}
\left(\frac{430}{541}\right) &= \left(\frac{-111}{541}\right) = \left(\frac{-1}{541}\right)\left(\frac{3}{541}\right)\left(\frac{37}{541}\right) \\
&= (-1)^{(541-1)/2}(-1)^{\frac{3-1}{2}\cdot\frac{541-1}{2}}\left(\frac{541}{3}\right)(-1)^{\frac{37-1}{2}\cdot\frac{541-1}{2}}\left(\frac{541}{37}\right) \\
&= \left(\frac{1}{3}\right)\left(\frac{23}{37}\right) = (-1)^{\frac{23-1}{2}\cdot\frac{37-1}{2}}\left(\frac{37}{23}\right) = \left(\frac{14}{23}\right) \\
&= \left(\frac{2}{23}\right)\left(\frac{7}{23}\right) = (-1)^{\frac{7-1}{2}\cdot\frac{23-1}{2}}\left(\frac{23}{7}\right) = -\left(\frac{2}{7}\right) = -1,
\end{aligned}$$

by the Law of Quadratic Reciprocity and its Supplements. □

Example 3

Let $p \neq 3$ be an odd prime. Show that

$$\left(\frac{6}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1, \pm 5 \pmod{24}, \\ -1 & \text{if } p \equiv \pm 7, \pm 11 \pmod{24}. \end{cases}$$

Remark. Since $\varphi(24) = \varphi(3)\varphi(8) = 2 \cdot 4 = 8$, this covers every possible case modulo 24.

Solution. Using quadratic reciprocity we have

$$\left(\frac{6}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{2}{p}\right)(-1)^{\frac{3-1}{2}\cdot\frac{p-1}{2}}\left(\frac{p}{3}\right)$$

$$= (-1)^{(p-1)/2}\left(\frac{2}{p}\right)\left(\frac{p}{3}\right).$$

If $p \equiv 1 \pmod 8$, then $p \equiv 1 \pmod 4$, and

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

If $p \equiv 3 \pmod 8$, then $p \equiv 3 \pmod 4$, and

$$(-1)^{(p-1)/2}\left(\frac{2}{p}\right) = (-1)(-1) = 1.$$

If $p \equiv 5 \pmod 8$, then $p \equiv 1 \pmod 4$, and

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

And if $p \equiv 7 \pmod 8$, then $p \equiv 3 \pmod 4$, and

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

If $p \equiv 1 \pmod 3$, then $\left(\frac{p}{3}\right) = 1$ and hence

$$\left(\frac{6}{p}\right) = (-1)^{(p-1)/2}\left(\frac{2}{p}\right)\left(\frac{p}{3}\right)$$

$$= (-1)^{(p-1)/2}\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1,3 \pmod 8) \\ -1, & \text{if } p \equiv 5,7 \pmod 8). \end{cases}$$

On the other hand, if $p \equiv 2 \pmod 3$, then

$$\left(\frac{6}{p}\right) = (-1)^{(p-1)/2}\left(\frac{2}{p}\right)\left(\frac{p}{3}\right)$$

$$= -(-1)^{(p-1)/2}\left(\frac{2}{p}\right) = \begin{cases} -1 & \text{if } p \equiv 1,3 \pmod 8 \\ 1, & \text{if } p \equiv 5,7 \pmod 8. \end{cases}$$

Thus $\left(\frac{6}{p}\right) = 1$ if and only if $p \equiv 1 \pmod 3$ and $p \equiv 1, 3 \pmod 8$ or $p \equiv 2 \pmod 3$ and $p \equiv 5, 7 \pmod 8$.

This gives us four pairs of congruences modulo 3 and 8, which we can solve via the CRT.

We find these are equivalent to

$$p \equiv 1, 5, 19, 23 \equiv \pm 1, \pm 5 \pmod{24}.$$

The only remaining options are

$$p \equiv 7, 11, 13, 17 \equiv \pm 7, \pm 11 \pmod{24},$$

and we must therefore have $\left(\frac{6}{p}\right) = -1$ in these cases. $\square$

Remark

Given an odd prime p, let $p^* = (-1)^{(p-1)/2} p = \pm p$.

Then the Law of Quadratic Reciprocity and Euler's criterion give

$$\begin{aligned} \left(\frac{p}{q}\right) &= (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{q}{p}\right) \\ &= \left((-1)^{(q-1)/2}\right)^{(p-1)/2} \left(\frac{q}{p}\right) \\ &= \left(\frac{(-1)^{(q-1)/2}}{p}\right) \left(\frac{q}{p}\right) = \left(\frac{q^*}{p}\right). \end{aligned}$$

This is a common restatement of the Law of Quadratic Reciprocity.