Proof of Quadratic Reciprocity
Number Theory

Andrea Schefer

December 10, 2023

Abstract

In this paper, we walk through a proof of the Quadratic Reciprocity Theorem which utilizes Gauss's Lemma.

To begin, I give a recap on the Quadratic Reciprocity Theorem:

> **Theorem 1** (Quadratic Reciprocity)**.** Let p and q be distinct odd primes. Then
>
> $$\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}\left(\frac{q}{p}\right),$$
>
> where $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ are Legendre symbols.

For the proof, we need Gauss's Lemma [1, 2], stated here:

> **Lemma 1.1** (Gauss's Lemma)**.** Let p be an odd prime and $\gcd(m,p) = 1$ for some $m \in \mathbb{Z}$. Consider the integers $m, 2m, 3m, \ldots, \frac{p-1}{2}m$ and their least positive residues module p. If the number of these residues that are greater than $\frac{p}{2}$ is n, then $\left(\frac{m}{p}\right) = (-1)^n$.

Here, the least positive residue modulo p for an integer a is the integer k such that $a \equiv k \pmod{p}$.

Proof of Gauss's Lemma. [2] We begin by constructing two sets $A = \{m, 2m, 3m, \ldots, \frac{p-1}{2}m\}$ and B containing reduced-by-p elements of A. However, instead of having the elements of B be in the interval $(0, p)$, we reduce them to be in the interval $(-\frac{p}{2}, \frac{p}{2})$.

There are three properties of set B to note, for any elements s and t of B reduced from different elements in A:

1. $s \neq t$
2. $s, t \neq 0$
3. $s \neq -t$.

Proof of properties 1*,* 2*, and* 3.

1. Since A has all distinct elements, B does as well.
2. Recalling that the $\gcd(m,p) = 1$, reducing the multiples of m in mod p will never leave 0.
3. Suppose the contrary is true and there are some $s, t \in B$ such that $s = -t$. Then $s + t = 0$. Both s and t came from elements in the set A, say k and l, respectively. The difference between k and s is a multiple of p and the difference between l and t is a multiple of p. Therefore, we can create another equation: $k + l = hp$ for some h. But $k, l \leq \frac{p-1}{2}m$, so $k + l \leq (p-1)m$ and $p \nmid (k+l)$. This is a contradiction.

□

Now, suppose that all the elements in B were positive. So the elements are in the interval $(0, \frac{p}{2})$ or, because B is a set of integers, in the interval $(0, \frac{p-1}{2})$. Since there are $\frac{p-1}{2}$ integers in B, a possible instance for B would be $B = \{1, 2, 3, \ldots, \frac{p-1}{2}\}$. Considering the conditions, the only variants of B there could be are if some of the elements were negated instead. Therefore, the possible instances for B are all of the form $B = \{\pm 1, \pm 2, \pm 3, \ldots, \pm\frac{p-1}{2}\}$ (not violating property 3).

Since every element of A is congruent to an element of $B \pmod p$, the product of the elements in A is congruent to the product of the elements in $B \pmod p$. This is equivalent to the following:

$$\prod a_i \equiv \prod b_i \pmod p$$
$$(m)(2m)(3m)\cdots\left(\frac{p-1}{2}m\right) \equiv (\pm 1)(\pm 2)(\pm 3)\cdots\left(\pm\frac{p-1}{2}\right) \pmod p$$
$$m^{\frac{p-1}{2}} \equiv (-1)^v \pmod p,$$

where a_i and b_i are the ith elements of A and B, respectively and v is the number of negative elements in B. Using Euler's Criterion, we may see that the last equivalence can be altered to $\left(\frac{m}{p}\right) \equiv (-1)^v \pmod p$. Both sides of this equivalence are going to be either equal to 1 or -1, so they cannot differ by a multiple of p except when that multiple is 0. Therefore, we can change the equivalence operation to an equals sign, and the proof is complete. ☐

Proof of Theorem 1. [3] Suppose we have the Legendre symbol $\left(\frac{m}{p}\right)$ where $p = 4mj + r$ is a prime and $0 < r < 4m$. As in the proof of Gauss's Lemma, we construct two sets: $A = \{m, 2m, 3m, \ldots, \frac{p-1}{2}m\}$ and B, the reduced-(mod p) version of A where the elements of B are in the range $(-\frac{p}{2}, \frac{p}{2})$. In creating the actual elements of set B, we have to see what intervals the elements of A start in. Firstly, for all $x \in A$, if $x \in (kp, (k+\frac{1}{2})p)$ for some $k \in \mathbb{W}$, reducing $x \pmod p$ will give a number between 0 and $\frac{p}{2}$. Similarly, reducing a number in range $((k-\frac{1}{2})p, kp)$ will give a number between $-\frac{p}{2}$ and 0. To figure out the upper bound for kp, we note that the smallest next integer not in A is $\frac{p+1}{2}m$. So $kp < \frac{p+1}{2}$. We also need to ensure that $\frac{p-1}{2} < (k+\frac{1}{2})p$ (in case $\frac{p-1}{2}m$ reduced is positive). When m is odd, we may set $k = \frac{m-1}{2}$ to fulfill the bounds, and when m is even, we may set $k = \frac{m}{2}$ to fulfill the bounds. Returning to our inequality for reduction of A's elements to negative integers ($(k-\frac{1}{2})p < x < kp$), we may rewrite x as my where y is the integer coefficient for m in A: $(k-\frac{1}{2})p < my < kp$. We next divide by m: $(k-\frac{1}{2})\frac{p}{m} < y < k\frac{p}{m}$. Recall that $p = 4mj + r$ so we substitute p in this inequality:

$$\left(k-\frac{1}{2}\right)\frac{4mj+r}{m} < y < k\frac{4mj+r}{m} \quad\Longrightarrow\quad \left(k-\frac{1}{2}\right)4j + \left(k-\frac{1}{2}\right)\frac{r}{m} < y < k(4j) + k\frac{r}{m}.$$

Now, in order for Gauss's Lemma to be useful here, we only need to know whether the number of x's in this negative range is even or odd (whether the exponent on the (-1) is even or odd). Adding an even number like $(k-\frac{1}{2})4j$ would not affect the parity of the cardinality of the set of x's. Therefore, we may dissolve both even terms on the LHS and the RHS of the above inequality: $\left(k-\frac{1}{2}\right)\frac{r}{m} < y < k\frac{r}{m}$.

Lemma 1.2. Suppose we have p, q primes such that $p \equiv q \pmod{4m}$. Then $\left(\frac{m}{p}\right) = \left(\frac{m}{q}\right)$.

We have, of course, just proved the above lemma using Gauss's Lemma. Now, let's take the last inequality we used but instead of the remainder of our prime p being r, we may use a remainder of $4m - r$. We substitute and simplify:

$$\left(k-\frac{1}{2}\right)\frac{4m-r}{m} < y < k\frac{4m-r}{m}$$
$$\left(k-\frac{1}{2}\right)\frac{-r}{m} < y < 2 - k\frac{r}{m} \qquad \text{(remove multiples of 4)}$$
$$-2 + k\frac{r}{m} < y < \left(k-\frac{1}{2}\right)\frac{r}{m}, \qquad \text{(multiply by -1)}$$

where the third line leaves y unchanged because it is simply an integer with no positive/negative sign specified. Let's look at the original inequality from before our substitution and see how it relates to the most recent one. We see that $-2+k\frac{r}{m} < \left(k-\frac{1}{2}\right)\frac{r}{m} < k\frac{r}{m}$. The length of the interval $(-2+k\frac{r}{m}, k\frac{r}{m})$ is 2. We may see that the number of solutions in this interval is then 2. Both the intervals $(-2+k\frac{r}{m}, \left(k-\frac{1}{2}\right)\frac{r}{m})$ and $(\left(k-\frac{1}{2}\right)\frac{r}{m}, k\frac{r}{m})$ therefore have same parity number of solutions. So,

$$\left(\frac{m}{p_{4m-r}}\right) = \left(\frac{m}{p}\right).$$

Let's set $p_{4m-r} = q = (4m)j + 4m - r$. We see that $p \equiv -q \pmod{4m}$. So this brings us to our second lemma:

Lemma 1.3. Suppose we have p, q primes such that $p \equiv -q \pmod{4m}$. Then $\left(\frac{m}{p}\right) = \left(\frac{m}{q}\right)$.

Since we just proved this lemma, we can move on to looking at the Legendre symbol product $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)$ for some distinct prime numbers p, q where $p \equiv q \pmod 4$. This means that $p = 4d + q$ for some $d \in \mathbb{Z}$ and so

$$\left(\frac{p}{q}\right) = \left(\frac{4d+q}{q}\right) = \left(\frac{4d}{q}\right) = \left(\frac{4}{q}\right)\left(\frac{d}{q}\right) = \left(\frac{d}{q}\right),$$

where the last expression equality is true because 4 is always a quadratic residue. The same thing can be done for $\left(\frac{q}{p}\right)$ so that

$$\left(\frac{q}{p}\right) = \left(\frac{p-4d}{p}\right) = \left(\frac{-4d}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{4}{p}\right)\left(\frac{d}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{d}{p}\right).$$

Since $p = 4d + q$, we also see that $p \equiv q \pmod{4d}$ and by Lemma 1.2, we have $\left(\frac{d}{p}\right) = \left(\frac{d}{q}\right)$. Thus, multiplying our two original Legendre symbols together gives us

$$\begin{aligned}\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) &= \left(\frac{d}{p}\right)^2\left(\frac{-1}{p}\right) = \left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod p \\ &= (-1)^{\frac{p-1}{2}}. && \text{(congruence mod p is guaranteed equality)}\end{aligned}$$

Now, the only case that is left after accounting for $p \equiv q \pmod{4d}$ is $p \equiv -q \pmod{4d}$, so $p = 4d - q$ for some $d \in \mathbb{Z}$. So $\left(\frac{p}{q}\right) = \left(\frac{4d-q}{q}\right) = \left(\frac{4}{q}\right)\left(\frac{d}{q}\right) = \left(\frac{d}{q}\right)$ and $\left(\frac{q}{p}\right) = \left(\frac{d}{p}\right)$. As before, $p \equiv q \pmod{4d}$ so we may apply Lemma 1.3:

$$\left(\frac{d}{p}\right) = \left(\frac{d}{q}\right) \quad \to \quad \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1.$$

Thus we have

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases}(-1)^{\frac{p-1}{2}} & p \equiv q \pmod 4 \\ 1 & p \not\equiv q \pmod 4.\end{cases}$$

It is verifiable that this is equivalent to the Theorem 1, and thus Quadratic Reciprocity is shown.

□

References

[1] Awatef Noweafa Almuteri. *Quadratic Reciprocity: Proofs and Applications*. PhD thesis, 2019.

[2] Mu Prime Math. Proof and Explanation: Gauss's Lemma in Number Theory. `https://www.youtube.com/watch?v=JhbSYWAOCOU`, 2020.

[3] Mu Prime Math. Quadratic Reciprocity using Gauss's Lemma. `https://www.youtube.com/watch?v=kQV3AXdlfv4`, 2020.