The Legendre Symbol and Its Properties

Ryan C. Daileda

Trinity University

Number Theory

Introduction

Today we will begin moving toward the *Law of Quadratic Reciprocity*, which gives an explicit relationship between the congruences $x^2 \equiv q \pmod{p}$ and $x^2 \equiv p \pmod{q}$ for distinct odd primes p, q.

Our main tool will be the *Legendre symbol*, which is essentially the indicator function of the quadratic residues of p.

We will relate the Legendre symbol to indices and Euler's criterion, and prove *Gauss' Lemma*, which reduces the computation of the Legendre symbol to a counting problem.

Along the way we will prove the *Supplementary Quadratic Reciprocity Laws* which concern the congruences $x^2 \equiv -1 \pmod{p}$ and $x^2 \equiv 2 \pmod{p}$.

The Legendre Symbol

Recall. Given an odd prime p and an integer a with $p \nmid a$, we say a is a *quadratic residue of p* iff the congruence $x^2 \equiv a \pmod{p}$ has a solution.

Definition

Let p be an odd prime. For $a \in \mathbb{Z}$ with $p \nmid a$ we define the *Legendre symbol* to be

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue of } p, \\ -1 & \text{otherwise.} \end{cases}$$

Remark. It is customary to define $\left(\frac{a}{p}\right) = 0$ if $p | a$.

Let p be an odd prime.

Notice that if $a \equiv b \pmod{p}$, then the congruence $x^2 \equiv a \pmod{p}$ has a solution if and only if $x^2 \equiv b \pmod{p}$ does.

And $p|a$ if and only if $p|b$.

Thus $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ whenever $a \equiv b \pmod{p}$.

It follows that we can view the Legendre symbol as a function

$$\left(\frac{\cdot}{p}\right) : \mathbb{Z}/p\mathbb{Z} \to \{0, \pm 1\},$$

by letting it act on representatives, i.e. $\left(\frac{a + p\mathbb{Z}}{p}\right) = \left(\frac{a}{p}\right)$.

Example

Let $p = 11$. Direct computation yields the table

$x \pmod{11}$	1	2	3	4	5	6	7	8	9	10
$x^2 \pmod{11}$	1	4	9	5	3	3	5	9	4	1

Thus

$$\left(\frac{1}{11}\right) = \left(\frac{3}{11}\right) = \left(\frac{4}{11}\right) = \left(\frac{5}{11}\right) = \left(\frac{9}{11}\right) = 1$$

and

$$\left(\frac{2}{11}\right) = \left(\frac{6}{11}\right) = \left(\frac{7}{11}\right) = \left(\frac{8}{11}\right) = \left(\frac{10}{11}\right) = -1.$$

Euler's Criterion Revisited

Let p be an odd prime. Recall *Euler's Criterion*, which states that if $p \nmid a$, then a is a quadratic residue if and only if

$$a^{(p-1)/2} \equiv 1 \pmod{p}.$$

It turns out that Euler's criterion also nicely classifies the quadratic nonresidues.

Let r be a primitive root modulo p. Since

$$1 \equiv r^{p-1} \equiv \left(r^{(p-1)/2}\right)^2 \pmod{p},$$

$r^{(p-1)/2}$ solves the congruence $x^2 - 1 \equiv 0 \pmod{p}$.

Clearly $x = \pm 1$ are two incongruent solutions of the same congruence.

Lagrange's theorem implies that these are the *only* solutions modulo p.

Thus $r^{(p-1)/2} \equiv \pm 1 \pmod{p}$.

But r has order $p-1$ modulo p, so $r^{(p-1)/2} \not\equiv 1 \pmod{p}$.

Therefore $r^{(p-1)/2} \equiv -1 \pmod{p}$.

Now suppose $p \nmid a$. Then $r^k \equiv a \pmod{p}$, where $k \in \mathrm{ind}_r(a)$.

Hence

$$a^{(p-1)/2} \equiv (r^k)^{(p-1)/2} \equiv \left(r^{(p-1)/2}\right)^k \equiv (-1)^{\mathrm{ind}_r(a)} \pmod{p}.$$

Remark. Every element of $\mathrm{ind}_r(a)$ has the same parity since $p-1$ is even. So we are free to choose any representative when computing $(-1)^{\mathrm{ind}_r(a)}$.

Now recall that the congruence $x^2 \equiv a \pmod{p}$ has a solution iff $(p-1, 2) = 2 \mid \operatorname{ind}_r(a)$.

Thus, a is a quadratic residue of p iff $\operatorname{ind}_r(a)$ is even iff $(-1)^{\operatorname{ind}_r(a)} = 1$.

And a is a quadratic nonresidue of p iff $(-1)^{\operatorname{ind}_r(a)} = -1$. This proves:

Theorem 1 (Strong Euler's Criterion)

Let p be an odd prime and let r be a primitive root modulo p. If $p \nmid a$, then

$$\left(\frac{a}{p}\right) = (-1)^{\operatorname{ind}_r(a)} \equiv a^{(p-1)/2} \pmod{p}.$$

Remark. Note that the congruence $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$ also holds when $p|a$, as both sides of the congruence are simply 0.

The connection between the Legendre symbol and the index immediately yields:

Theorem 2 (Properties of the Legendre Symbol)

Let p be an odd prime and suppose $p \nmid a$ and $p \nmid b$. Then:

1. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.
2. $\left(\frac{1}{p}\right) = 1$ *and* $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.

Remark. The multiplicativity relationship in **1** automatically holds if $p|a$ or $p|b$ (why?).

Proof. Let r be a primitive root modulo p.

Because the index relative to r is a multiplicative to additive isomorphism, we have

$$\left(\frac{ab}{p}\right) = (-1)^{\mathrm{ind}_r(ab)} = (-1)^{\mathrm{ind}_r(a)+\mathrm{ind}_r(b)}$$
$$= (-1)^{\mathrm{ind}_r(a)}(-1)^{\mathrm{ind}_r(b)} = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Since $r^{(p-1)/2} \equiv -1 \pmod{p}$, we have

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

And since $\mathrm{ind}_r(1) = 0$, we also have $\left(\frac{1}{p}\right) = (-1)^0 = 1.$ □

Example

Let's evaluate $\left(\frac{-72}{131}\right)$. We have

$$\left(\frac{-72}{131}\right) = \left(\frac{-2\cdot 6^2}{131}\right) = \left(\frac{-1}{131}\right)\left(\frac{6^2}{131}\right)\left(\frac{2}{131}\right)$$

$$= (-1)^{(131-1)/2}\left(\frac{2}{131}\right) = -\left(\frac{2}{131}\right).$$

We now appeal to Euler's criterion:

$$-\left(\frac{2}{131}\right) \equiv -2^{(131-1)/2} \equiv -2^{65} \equiv -(2^7)^9 2^2 \equiv -(128)^9\cdot 4 \ (\text{mod } 13$$

$$\equiv -(-3)^9\cdot 4 \equiv 3\cdot(162)^2 \equiv 3\cdot 31^2 \equiv 3\cdot 44 \pmod{131}$$

$$\equiv 132 \equiv 1 \pmod{131}.$$

Hence $\left(\frac{-72}{131}\right) = 1$. □

The next result generalizes to arbitrary nontrivial *Dirichlet characters* modulo n.

Theorem 3

If p is an odd prime, then $\displaystyle\sum_{a=1}^{p-1}\left(\frac{a}{p}\right) = 0$. In particular, there are exactly $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic nonresidues modulo p.

Proof. This can be proved in a number of ways. We opt for the most generalizable argument.

Let r be a primitive root mod p. Then $\left(\frac{r}{p}\right) = (-1)^{\mathrm{ind}_r(r)} = -1$.

Let $S = \displaystyle\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)$.

Since left translation by $r + p\mathbb{Z}$ simply permutes the elements of the group $(\mathbb{Z}/p\mathbb{Z})^\times$, and $\left(\frac{a}{p}\right)$ depends only on the congruence class of a modulo p, we find that

$$\begin{aligned}
-S = \left(\frac{r}{p}\right) S &= \sum_{a=1}^{p-1} \left(\frac{ra}{p}\right) = \sum_{a=1}^{p-1} \left(\frac{ra + p\mathbb{Z}}{p}\right) \\
&= \sum_{a=1}^{p-1} \left(\frac{(r + p\mathbb{Z})(a + p\mathbb{Z})}{p}\right) = \sum_{a+p\mathbb{Z} \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{(r + p\mathbb{Z})(a + p\mathbb{Z})}{p}\right) \\
&= \sum_{a+p\mathbb{Z} \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{a + p\mathbb{Z}}{p}\right) = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = S.
\end{aligned}$$

Hence $2S = 0$, which implies $S = 0$. □

Gauss' Lemma

If p is an odd prime, then $(\mathbb{Z}/p\mathbb{Z})^\times$ is the disjoint union of

$$L = \left\{ r + p\mathbb{Z} \,\middle|\, 1 \leq r < \frac{p}{2} \right\}$$

and

$$R = \left\{ r + p\mathbb{Z} \,\middle|\, \frac{p}{2} < r \leq p - 1 \right\}.$$

Notice that $\frac{p}{2} < r \leq p - 1$ iff $-\frac{p}{2} > -r \geq 1 - p$ iff $\frac{p}{2} > p - r \geq 1$.

Thus

$$\begin{aligned} -R &= \left\{ -r + p\mathbb{Z} \,\middle|\, \frac{p}{2} < r \leq p - 1 \right\} \\ &= \left\{ (p - r) + p\mathbb{Z} \,\middle|\, \frac{p}{2} < r \leq p - 1 \right\} \\ &= \left\{ r + p\mathbb{Z} \,\middle|\, 1 \leq r < \frac{p}{2} \right\} = L. \end{aligned}$$

Suppose $p \nmid a$. Define $T_a : L \to L$ by

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

We claim that T_a is a bijection.

Because L is finite it suffices to prove T_a is one-to-one.

So suppose $T_a(r + p\mathbb{Z}) = T_a(s + p\mathbb{Z})$. Then $ar + p\mathbb{Z} = \pm as + p\mathbb{Z}$.

Since $p \nmid a$, $a + p\mathbb{Z} \in (\mathbb{Z}/p\mathbb{Z})^\times$. Multiplication by $(a + p\mathbb{Z})^{-1}$ then yields

$$r + p\mathbb{Z} = \pm s + p\mathbb{Z}.$$

Since $-s + p\mathbb{Z} \in R$ and $L \cap R = \varnothing$, we must have $r + p\mathbb{Z} = s + p\mathbb{Z}$.

Thus T_a is one-to-one, as claimed, and hence a bijection.

It follows that

$$\prod_{r+p\mathbb{Z}\in L}(r+p\mathbb{Z}) = \prod_{r+p\mathbb{Z}\in L} T_a(r+p\mathbb{Z})$$
$$= (-1)^n \prod_{r+p\mathbb{Z}\in L}(ar+p\mathbb{Z})$$
$$= (-1)^n (a+p\mathbb{Z})^{(p-1)/2} \prod_{r+p\mathbb{Z}\in L}(r+p\mathbb{Z}),$$

where n is the number of $r+p\mathbb{Z}\in L$ for which $ar+p\mathbb{Z}\in R$. Because $(\mathbb{Z}/p\mathbb{Z})^\times$ is a group, we can cancel the product from both sides to obtain

$$1+p\mathbb{Z} = (-1)^n\left(a^{(p-1)/2}+p\mathbb{Z}\right) \;\Leftrightarrow\; 1 \equiv (-1)^n a^{(p-1)/2} \pmod{p}$$
$$\equiv (-1)^n \left(\frac{a}{p}\right) \pmod{p}.$$

Because $\left(\frac{a}{p}\right) \in \{\pm 1\}$, we arrive at the following conclusion.

Theorem 4 (Gauss' Lemma)

Let p be an odd prime and suppose $p \nmid a$. Let n be the number of $r + p\mathbb{Z} \in L$ for which $ar + p\mathbb{Z} \in R$. Then

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

Remark. Note that we can write $n = \left|(a + n\mathbb{Z})L \cap R\right|$.

Although Gauss' Lemma is of more theoretical than practical importance, let's give an example to illustrate it.

Example 1

Use Gauss' Lemma to compute $\left(\frac{7}{13}\right)$.

Solution. We have

$$L = \{1 + 13\mathbb{Z}, 2 + 13\mathbb{Z}, 3 + 13\mathbb{Z}, 4 + 13\mathbb{Z}, 5 + 13\mathbb{Z}, 6 + 13\mathbb{Z}\}$$

and

$$(7+13\mathbb{Z})L = \{7+13\mathbb{Z}, 1+13\mathbb{Z}, 8+13\mathbb{Z}, 2+13\mathbb{Z}, 9+13\mathbb{Z}, 3+13\mathbb{Z}\}.$$

Thus $n = 3$ so that $\left(\frac{7}{13}\right) = (-1)^3 = -1$, by Gauss' Lemma. □

We will now apply Gauss' Lemma to prove:

Theorem 5

Let p be an odd prime. Then $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

Remark. Since $n^2 \equiv 1 \pmod 8$ for all odd n, the exponent is definitely an integer.

Proof. We have

$$\begin{aligned}(2+p\mathbb{Z})L \cap R &= \{2+p\mathbb{Z}, 4+p\mathbb{Z}, 6+p\mathbb{Z}, \ldots, (p-1)+p\mathbb{Z}\} \cap R \\ &= \{2r+p\mathbb{Z} \,|\, 2r > p/2 \text{ and } 1 \le r < p/2\} \\ &= \{2r+p\mathbb{Z} \,|\, p/4 < r < p/2\}.\end{aligned}$$

So the exponent n in Gauss' Lemma is the number of integers in the open interval $(p/4, p/2)$.

The largest such integer is $\frac{p-1}{2}$.

Since $p/4$ is not an integer, the smallest such integer is $[p/4]+1$, where $[x]$ is the greatest integer $\leq x$.

So the number of integers in $(p/4, p/2)$ is

$$n = \frac{p-1}{2} - \left(\left[\frac{p}{4}\right]+1\right) + 1 = \frac{p-1}{2} - \left[\frac{p}{4}\right].$$

We now consider p modulo 8.

If $p \equiv 1 \pmod 8$, then $p = 1 + 8k$ for some k. Hence

$$n = \frac{p-1}{2} - \left[\frac{p}{4}\right] = 4k - \left[2k + \frac{1}{4}\right] = 4k - 2k = 2k$$

By Gauss' Lemma we therefore have $\left(\frac{2}{p}\right) = (-1)^n = (-1)^{2k} = 1$.

If $p \equiv 3 \pmod 8$, then $p = 3 + 8k$ and

$$n = \frac{p-1}{2} - \left[\frac{p}{4}\right] = 1 + 4k - \left[2k + \frac{3}{4}\right] = 1 + 4k - 2k = 2k + 1,$$

which is odd. Hence $\left(\frac{2}{p}\right) = (-1)^n = -1$.

If $p \equiv 5 \pmod 8$, then $p = 5 + 8k$ and

$$n = \frac{p-1}{2} - \left[\frac{p}{4}\right] = 2 + 4k - \left[2k + \frac{5}{4}\right] = 2 + 4k - (2k + 1) = 2k + 1,$$

which is odd. Hence $\left(\frac{2}{p}\right) = (-1)^n = -1$.

Finally, if $p \equiv 7 \pmod 8$, then $p = 7 + 8k$ and

$$n = \frac{p-1}{2} - \left[\frac{p}{4}\right] = 3+4k - \left[2k + \frac{7}{4}\right] = 3+4k-(2k+1) = 2k+2,$$

which is even. Hence $\left(\dfrac{2}{p}\right) = (-1)^n = 1$.

This proves that

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

The final equality is left as an exercise. □

Example

Recall that earlier we showed

$$\left(\frac{-72}{131}\right) = -\left(\frac{2}{131}\right),$$

and then proceeded to compute 2^{65} modulo 131 so that we could apply Euler's criterion.

Now we can simply use Theorem 5. Since

$$131 = 128 + 3 = 2^7 + 3 \equiv 3 \pmod{8},$$

we have

$$-\left(\frac{2}{131}\right) = -(-1) = 1,$$

as computed earlier.

Remarks

The results

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} \quad \text{and} \quad \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$$

are sometimes referred to as the *Supplementary Quadratic Reciprocity Laws*.

Note that the first tells us (again) that -1 is a square modulo p iff $p \equiv 1 \pmod 4$.

The map $\left(\frac{\cdot}{p}\right) : (\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}$ is an example of a *Dirichlet character modulo n*: a multiplicative map $(\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$.

One More Thing...

The Legendre symbol has an interesting combinatorial interpretation.

If p is an odd prime and $p \nmid a$, then left translation by $a + p\mathbb{Z}$ yields a permutation λ_a of $(\mathbb{Z}/p\mathbb{Z})^\times$.

Every permutation is a composition of transpositions, which simply interchange two elements.

Although the number n of transpositions needed is *not* unique, its parity *is*, so that $(-1)^n$ is a well-defined invariant of a permutation called its *sign*.

If $\sigma(\lambda_a)$ is the sign of λ_a, then one can show that in fact

$$\sigma(\lambda_a) = \left(\frac{a}{p}\right).$$