The Legendre Symbol

R. C. Daileda

Trinity University

Number Theory

Definitions

Given an odd prime p and $a \in \mathbb{Z}$ with $p \nmid a$, we say a is a *quadratic residue* of p if $a \equiv b^2 \pmod{p}$ for some b.

Otherwise a is a *quadratic nonresidue*.

The *Legendre symbol* of a at p is

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

$\left(\frac{a}{p}\right)$ is clearly p-periodic in a. Thus we can view

$$\left(\frac{\cdot}{p}\right) : (\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}.$$

Euler's criterion immediately implies the next result.

Theorem

Let p be an odd prime, $p \nmid a$. Then

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

We can use this theorem to prove the following important fact.

Theorem

The Legendre symbol is completely multiplicative *and induces a surjective homomorphism*

$$\left(\frac{\cdot}{p}\right) : (\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}.$$

Proof.

We have already seen that exactly half of the elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ are squares a.k.a. quadratic residues.

Therefore $\left(\frac{\cdot}{p}\right)$ is surjective.

Let $a, b \in \mathbb{Z}$ be coprime to p. Then so is ab and

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} \equiv a^{(p-1)/2} b^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}.$$

Because the values of $\left(\frac{\cdot}{p}\right)$ belong to $\{\pm 1\}$,

$$\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = 0, \pm 2.$$

But the left-hand side is divisible by the odd prime p, so ± 2 are impossible. This proves the result. □

Quadratic Reciprocity, First Supplement: $a = -1$

When $a = -1$, the first theorem tells us that

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

Both sides of the congruence belong to $\{\pm 1\}$.

Because p is odd, $1 \not\equiv -1 \pmod{p}$.

Hence (1) must actually be an *equality*.

Theorem (Quadratic Reciprocity, First Supplement)

Let p be an odd prime. Then

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

Reduction to Prime Argument

Given a coprime to p, write $a = \epsilon \prod_i q_i^{n_i}$ with $q_i \neq p$ distinct primes, $\epsilon \in \{\pm 1\}$.

According to the preceding theorem

$$\left(\frac{a}{p}\right) = \left(\frac{\epsilon}{p}\right) \prod_i \left(\frac{q_i}{p}\right)^{n_i} = \left(\frac{\epsilon}{p}\right) \prod_{\substack{i \\ n_i \text{ odd}}} \left(\frac{q_i}{p}\right).$$

The First Supplement evaluates $\left(\frac{\epsilon}{p}\right)$. The Second Supplement will evaluate $\left(\frac{2}{p}\right)$.

We are therefore reduced to evaluating $\left(\frac{q}{p}\right)$ where $q \neq p$ is an odd prime. This is the subject of the *Law of Quadratic Reciprocity*.

Back to $(\mathbb{Z}/p^m\mathbb{Z})^\times$

Let $a \in Z$ be coprime to p. It turns out that $\left(\frac{a}{p}\right)$ controls whether or not a is a square $\pmod{p^m}$ *for all* $m \in \mathbb{N}$!

Theorem

Suppose $\left(\frac{a}{p}\right) = 1$. *Then there is a sequence of integers* $b_1, b_2, b_3, \ldots$ *so that:*

- $b_{m+1} \equiv b_m \pmod{p^m}$ *for all* $m \geq 1$;
- $b_m^2 \equiv a \pmod{p^m}$ *for all* $m \geq 1$.

In particular, $a + p^m\mathbb{Z} \in (\mathbb{Z}/p^m\mathbb{Z})^\times$ *is a square for all* $m \geq 1$.

Remark: These conditions imply that the sequence $\{b_m\}_{m=1}^\infty$ converges in the ring $\mathbb{Z}_p$ of *p-adic integers* to $\sqrt{a}$.

Proof: We recursively construct the sequence of b's.

Since a is a quadratic residue of p, there is a b_1 so that $a \equiv b_1^2 \pmod{p}$.

Suppose we have found $b_1, b_2, \ldots, b_m$ as in the theorem.

Consider $b_m + kp^m$, which is $\equiv b_m \pmod{p^m}$ for any choice of k.

Moreover

$$\begin{aligned}(b_m + kp^m)^2 &= b_m^2 + 2b_m kp^m + k^2 p^{2m}\\ &\equiv b_m^2 + 2b_m kp^m \pmod{p^{m+1}}\\ &\equiv a + \ell p^m + 2b_m kp^m \pmod{p^{m+1}}\\ &\equiv a + (\ell + 2b_m k)p^m \pmod{p^{m+1}}.\end{aligned}$$

We need to choose k so that $p | \ell + 2b_m k$, i.e. $2b_m k \equiv -\ell \pmod{p}$.

$2b_m k \equiv -\ell \pmod{p}$ is a linear congruence in the variable k.

Since $p \nmid 2b_m$, we have $(2b_m, p) = 1$, which means the congruence has a unique solution $\pmod{p}$.

Choose any element k of the solution set and define $b_{m+1} = b_m + kp^m$. Then b_{m+1} has the desired properties.

Continuing this process indefinitely yields the sought after sequence. $\square$.

Example

Example

Show that -1 *is a square* $\pmod{625}$ *and find its two square roots.*

We have

$$\left(\frac{-1}{5}\right) = (-1)^{(5-1)/2} = (-1)^2 = 1.$$

Hence -1 is a square $\pmod{5^m}$ for all $m \geq 1$.

To find its square roots we implement the algorithm in the proof.

Since $-1 \equiv 4 \pmod 5$, clearly $b_1 = 2$. And since $2^2 = -1 + 1 \cdot 5$, $\ell = 1$. So $b_2 = b_1 + 5k$ where

$$2b_1 k \equiv -\ell \pmod 5 \;\Rightarrow\; 4k \equiv -1 \pmod 5 \;\Rightarrow\; k \equiv 1 \pmod 5,$$

i.e. $b_2 = 7$.

Now $b_2^2 = -1 + 2 \cdot 5^2$ so that $\ell = 2$. So we need to solve

$$2b_2k \equiv -\ell \pmod 5 \;\Rightarrow\; 4k \equiv -2 \pmod 5 \;\Rightarrow\; k \equiv 2 \pmod 5,$$

and $b_3 = b_2 + 5^2k = 57$.

Finally, $b_3^2 = -1 + 26 \cdot 5^3$ yields $\ell = 26$ and we solve for k:

$$2b_3k \equiv -\ell \pmod 5 \;\Rightarrow\; 4k \equiv -1 \pmod 5 \;\Rightarrow\; k \equiv 1 \pmod 5.$$

Thus $b_4 = b_3 + 5^3k = 182$.

Therefore the two square roots of $-1 \pmod{625}$ are

$$\boxed{\pm 182 \pmod{625}}.$$

Gauss' Lemma

Let's finally start heading toward the Law of Quadratic Reciprocity. Our first auxiliary result is the following.

Lemma (Gauss' Lemma)

Let p be an odd prime and suppose that $p \nmid a$. For each

$$r \in \left\{a, 2a, 3a, \ldots, \frac{p-1}{2}a\right\}$$

choose the unique $s_r \in \left\{-\frac{p-1}{2}, -\frac{p-3}{2}, \ldots, -1, 1, 2, \ldots, \frac{p-1}{2}\right\}$ so that $r \equiv s_r \pmod{p}$. Then

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

where ν is the number of negative values of s_r.

Proof of Gauss' Lemma

Let $I_p = \left\{-\frac{p-1}{2}, -\frac{p-3}{2}, \ldots, -1, 1, 2, \ldots, \frac{p-1}{2}\right\}$.

Note that if $s \neq t \in I_p$ then:

- $(s, p) = (t, p) = 1$;
- $0 < |s - t| \leq p - 1 < p \;\Rightarrow\; p \nmid s - t \;\Rightarrow\; s \not\equiv t \pmod{p}$;
- $|I_p| = p - 1 = \varphi(p)$.

Therefore the map

$$\begin{aligned} I_p &\to (\mathbb{Z}/p\mathbb{Z})^\times \\ s &\mapsto s + p\mathbb{Z} \end{aligned}$$

is a bijection and s_r is well-defined.

Suppose $s_r = -s_{r'}$. Then $r \equiv -r' \pmod p$.

Thus $ai \equiv -aj \pmod p$ for some $1 \leq i, j \leq \frac{p-1}{2}$.

Since $(a, p) = 1$, we can cancel it to obtain $i \equiv -j \pmod p$ or

$$i + j \equiv 0 \pmod p \;\Rightarrow\; p | i + j.$$

But $0 < i + j < p - 1$, so this is impossible.

Therefore $\{s_r\}$ cannot contain both s and $-s$ for any $s \in I_p$.

It follows that

$$\{s_r\} = \left\{\epsilon_1 \cdot 1, \epsilon_2 \cdot 2, \epsilon_3 \cdot 3, \ldots, \epsilon_{\frac{p-1}{2}} \cdot \frac{p-1}{2}\right\}$$

where each $\epsilon_i \in \{\pm 1\}$.

Now multiply together all of the r's and s_r's:

$$\underbrace{a^{(p-1)/2}\left(\frac{p-1}{2}\right)!}_{\text{the } r\text{'s}} \equiv \underbrace{\epsilon_1\epsilon_2\cdots\epsilon_{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!}_{\text{the } s_r\text{'s}} \pmod{p}$$

By an earlier theorem we therefore have

$$\left(\frac{a}{p}\right) \equiv (-1)^\nu \pmod{p} \;\Rightarrow\; \left(\frac{a}{p}\right) = (-1)^\nu$$

since both sides belong to $\{\pm 1\}$ and p is odd. □

Example

Consider $p = 11$ and $a = 7$. We have $\frac{p-1}{2} = 5$ and

$$\begin{aligned} 7 &\equiv -4 \pmod{11}, \\ 2 \cdot 7 &\equiv 3 \pmod{11}, \\ 3 \cdot 7 &\equiv -1 \pmod{11}, \\ 4 \cdot 7 &\equiv -5 \pmod{11}, \\ 5 \cdot 7 &\equiv 2 \pmod{11}. \end{aligned}$$

Therefore, by Gauss' Lemma,

$$\left(\frac{7}{11}\right) = (-1)^3 = -1,$$

and 7 is a quadratic nonresidue $\pmod{11}$.

Remark

Let $r \in \left\{a, 2a, 3a, \ldots, \frac{p-1}{2}a\right\}$. Use the Division Algorithm to write

$$r = qp + r', \;\; 0 \leq r' < p.$$

Since $r \equiv r' \pmod{p}$, the uniqueness of s_r implies:

- If $r' < \frac{p}{2}$, then $s_r = r'$.
- If $r' > \frac{p}{2}$, then $-\frac{p}{2} < r' - p < 0$ and $r \equiv r' - p \pmod{p}$.

  Hence $s_r = r' - p$.

It follows that ν in Gauss' Lemma is the number of r' that exceed $p/2$.

This alternate characterization of ν can sometimes be useful.

Quadratic Reciprocity, Second Supplement: $a = 2$

We can now prove the second piece of the Law of Quadratic Reciprocity.

Theorem (Quadratic Reciprocity, Second Supplement)

Let p be an odd prime. Then

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

Proof. According to the preceding remark, we need to count how often the remainder $\pmod p$ in the set

$$\{2, 4, 6, 8, \ldots, p-1\}$$

exceeds $p/2$.

Since these numbers are already remainders, we are really asking:

How many even numbers are between $\frac{p}{2}$ and $p-1$?

Since the least integer greater than $\frac{p}{2}$ is $\frac{p+1}{2}$, there are two cases.

Case 1. $\frac{p+1}{2}$ is odd, i.e. $p+1 \not\equiv 0 \pmod 4 \iff p \equiv 1 \pmod 4$.

In this case exactly half the numbers from $\frac{p+1}{2}$ to $p-1$ are even.

The evens therefore number

$$\frac{p-1-\frac{p+1}{2}+1}{2} = \frac{p-1}{4}.$$

Note that $p \equiv 1 \pmod 4 \Rightarrow \frac{p+1}{2}$ is odd. Thus, according to Gauss' Lemma

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{4}} = ((-1)^{\frac{p+1}{2}})^{\frac{p-1}{4}} = (-1)^{\frac{p^2-1}{8}}.$$

Case 2. $\frac{p+1}{2}$ is even, i.e. $p+1 \equiv 0 \pmod 4 \iff p \equiv 3 \pmod 4$.

In this case exactly half the numbers from $\frac{p+3}{2}$ (odd) to $p-1$ are even, together with $\frac{p+1}{2}$.

So the number of evens is

$$1 + \frac{p - 1 - \frac{p+3}{2} + 1}{2} = 1 + \frac{p-3}{4} = \frac{p+1}{4}.$$

In this case $\frac{p-1}{2}$ is odd, so that Gauss' Lemma gives

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p+1}{4}} = ((-1)^{\frac{p-1}{2}})^{\frac{p+1}{4}} = (-1)^{\frac{p^2-1}{8}}.$$

The congruence based cases follow directly from this (common) formula for $\left(\frac{2}{p}\right)$. □