6
Quadratic Reciprocity

Let a be an integer. The quadratic reciprocity law of Gauss provides a beautiful and precise answer to the following question: "For which primes p is the image of a in $(\mathbb{Z}/p)^{\times}$ a perfect square?" Amazingly, the answer only depends on the residue of p modulo $4a$.

The quadratic reciprocity law has been proved in a huge number of ways (see [Lem] for a list). We give two distinct proofs. The first, which is elementary and involves tediously keeping track of integer points in intervals, is given Section 6.3. The second, given in Section 6.4, is extremely algebraic and uses congruences between sums of powers of the complex number $\zeta = e^{2\pi i/p}$. You should read Sections 6.1 and 6.2, then at least one of Section 6.3 or Section 6.4, depending on taste.

In Section 6.5, we return to the computational question of actually finding square roots in practice.

6.1 Statement of the Quadratic Reciprocity Law

In this section we motivate, then precisely state, the quadratic reciprocity law.

Definition 6.1.1 (Quadratic Residue). An integer a not divisible by a prime p is called a *quadratic residue* modulo p if a is a square modulo p. If a is not a square modulo p then a is called a *quadratic nonresidue*.

The quadratic reciprocity theorem connects the question of whether or not a is a quadratic residue modulo p to the question of whether p is a quadratic residue modulo each of the prime divisors of a. To express it precisely, we introduce some new notation. Let p be an odd prime and let a be an integer coprime to p. Set

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

This notation is well entrenched in the literature, even though it is identical to the notation for "a divided by p"; be careful not to confuse the two.

Just as we defined $\gcd(a, b)$ for $a, b \in \mathbb{Z}/n$, define $\left(\frac{a}{p}\right)$ for $a \in \mathbb{Z}/p$ to be $\left(\frac{\tilde{a}}{p}\right)$ for any lift $\tilde{a}$ of a to $\mathbb{Z}$.

Proposition 6.2.1 below implies that

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

so the map $a \mapsto \left(\frac{a}{p}\right)$ is a multiplicative function in the sense that

$$\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

The symbol $\left(\frac{a}{p}\right)$ only depends on the residue class of a modulo p. Thus tabulating the value of $\left(\frac{a}{5}\right)$ for hundreds of a would be silly, since it is so easy.

Question 6.1.2. Would it be equally silly to make a table of $\left(\frac{5}{p}\right)$ for many of primes p?

We find out by constructing Table 6.1 and looking for a simple pattern. It appears that $\left(\frac{5}{p}\right)$ depends only on the congruence class of p modulo 5. More precisely, $\left(\frac{5}{p}\right) = 1$ if and only if $p \equiv 1, 4 \pmod{5}$, i.e., $\left(\frac{5}{p}\right) = 1$ if and only if p is a square modulo 5. We might try to prove this using Proposition 6.2.1 below; however, I see no simple reason that knowing that $p \equiv 1, 4 \pmod{5}$ helps us to evaluate $5^{(p-1)/2} \pmod{p}$. See Exercise 4 for further a discussion on proving our observation about Table 6.1 directly.

Based on similar observations, various mathematicians found a conjectural explanation for the mystery suggested by Table 6.1 in the 18th century. Finally, on April 8, 1796, at the age of only 19, Gauss proved the following theorem.

Theorem 6.1.3 (Quadratic Reciprocity Law). *Suppose that p and q are distinct odd primes. Then*

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

TABLE 6.1. When is 5 a square modulo p?

p	$\left(\frac{5}{p}\right)$	$p \bmod 5$
7	-1	2
11	1	1
13	-1	3
17	-1	2
19	1	4
23	-1	3
29	1	4
31	1	1
37	-1	2
41	1	1
43	-1	3
47	-1	2

Also

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

We will give two proofs of Gauss's formula for $\left(\frac{p}{q}\right)$. The first very elementary proof is in Section 6.3, and the second more algebraic proof is in Section 6.4. The assertion about $\left(\frac{-1}{p}\right)$ will follow from Proposition 6.2.1 below. We only prove the assertion about $\left(\frac{2}{p}\right)$ in Section 6.3 (see Proposition 6.3.4), but do not give a corresponding proof in Section 6.4.

In our example, Gauss's theorem implies that

$$\left(\frac{5}{p}\right) = (-1)^{2\cdot\frac{p-1}{2}}\left(\frac{p}{5}\right) = \left(\frac{p}{5}\right) = \begin{cases} +1 & \text{if } p \equiv 1,4 \pmod 5 \\ -1 & \text{if } p \equiv 2,3 \pmod 5, \end{cases}$$

which is exactly what we expected.

The following example illustrates how to answer questions like "is a a square modulo b" using Theorem 6.1.3.

Example 6.1.4. Is 69 a square modulo 389? We have

$$\left(\frac{69}{389}\right) = \left(\frac{3\cdot 23}{389}\right) = \left(\frac{3}{389}\right)\cdot\left(\frac{23}{389}\right) = (-1)\cdot(-1) = 1.$$

Here

$$\left(\frac{3}{389}\right) = \left(\frac{389}{3}\right) = \left(\frac{2}{3}\right) = -1,$$

and

$$\begin{aligned}\left(\frac{23}{389}\right) &= \left(\frac{389}{23}\right) = \left(\frac{21}{23}\right) = \left(\frac{-2}{23}\right)\\ &= \left(\frac{-1}{23}\right)\left(\frac{2}{23}\right) = (-1)^{\frac{23-1}{2}} \cdot 1 = -1.\end{aligned}$$

Thus 69 is a square modulo 389.

Though we know that 69 is a square modulo 389, we don't know an explicit x such that $x^2 \equiv 6 \pmod{389}$! This is similar to how we could prove using Theorem 3.3.14 that certain numbers are composite without knowing a factorization. However, it is usually easy in practice to find square roots, as we'll discuss in Section 6.5 and Example 6.5.1.

6.2 Euler's Criterion

Let p be an odd prime and a an integer not divisible by p. Euler used the existence of primitive roots to show that $\left(\frac{a}{p}\right)$ is congruent to $a^{(p-1)/2}$ modulo p. We will use this fact repeatedly below in both proofs of Theorem 6.1.3.

Proposition 6.2.1 (Euler's Criterion). *Then* $\left(\frac{a}{p}\right) = 1$ *if and only if*

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

Proof. By Theorem 5.2.2, there is an integer g that has order $p-1$ modulo p, so every integer coprime to p is congruent to a power of g. First suppose that a is congruent to a perfect square modulo p, so

$$a \equiv (g^r)^2 \equiv g^{2r} \pmod{p}$$

for some r. Then by Theorem 3.3.14

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

Conversely, suppose that $a^{(p-1)/2} \equiv 1 \pmod{p}$. We have $a \equiv g^r \pmod{p}$ for some integer r. Thus $g^{r(p-1)/2} \equiv 1 \pmod{p}$, so

$$p-1 \mid r(p-1)/2$$

which implies that r is even. Thus $a \equiv (g^{r/2})^2 \pmod{p}$, so a is congruent to a square modulo p. ∎

Corollary 6.2.2. *The equation* $x^2 \equiv a \pmod{p}$ *has no solution if and only if* $a^{(p-1)/2} \equiv -1 \pmod{p}$. *Thus* $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.

Proof. This follows from Proposition 6.2.1 and the fact that the polynomial $x^2 - 1$ has no roots besides $+1$ and -1 (which follows from Proposition 5.1.2). $\square$

Example 6.2.3. Suppose $p = 11$. By squaring each element of $(\mathbb{Z}/11)^\times$, we see that the squares modulo 11 are $\{1, 3, 4, 5, 9\}$. We compute $a^{(p-1)/2} = a^5$ for each $a \in (\mathbb{Z}/11)^\times$ and get

$$1^5 = 1,\ 2^5 = -1,\ 3^5 = 1,\ 4^5 = 1,\ 5^5 = 1,$$
$$6^5 = -1,\ 7^5 = -1,\ 8^5 = -1,\ 9^5 = 1,\ 10^5 = -1.$$

Thus the a with $a^5 = 1$ are $\{1, 3, 4, 5, 9\}$, just as Proposition 6.2.1 predicts.

Example 6.2.4. We determine whether or not 3 is a square modulo the prime $p = 726377359$. Using a computer we find that

$$3^{(p-1)/2} \equiv -1 \pmod{726377359}.$$

Thus 3 is not a square modulo p. This computation wasn't difficult, but it would have been tedious by hand. The law of quadratic reciprocity provides a way to answer this questions that could easily be carried out by hand:

$$\begin{aligned}\left(\frac{3}{726377359}\right) &= (-1)^{(3-1)/2\cdot(726377359-1)/2}\left(\frac{726377359}{3}\right)\\ &= (-1)\cdot\left(\frac{1}{3}\right) = -1.\end{aligned}$$

It is a general fact that if G is any abelian group and n is any integer, then the map $x \mapsto x^n$ is a homomorphism. Thus, in group-theoretic language, Proposition 6.2.1 asserts that the map

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

that sends a to $\left(\frac{a}{p}\right)$ is a homomorphism of groups.

Proposition 6.2.5. *The homomorphism* $\left(\frac{\bullet}{p}\right) : (\mathbb{Z}/p)^\times \to \{\pm 1\}$ *is surjective.*

Proof. If $\left(\frac{\bullet}{p}\right)$ is not surjective, then $\left(\frac{a}{p}\right) = 1$ for every $a \in (\mathbb{Z}/p)^\times$. This means that the squaring map $a \mapsto a^2$ on $(\mathbb{Z}/p)^\times$ is surjective. But -1 is in the kernel of squaring and $(\mathbb{Z}/p)^\times$ is finite, so squaring is not surjective. $\square$

6.3 First Proof of Quadratic Reciprocity

Our first proof of quadratic reciprocity is elementary but tedious. The proof involves keeping track of integer points in intervals. Proving Gauss's lemma is the first step; this lemma computes $\left(\frac{a}{p}\right)$ in terms of the number of integers of a certain type that lie in a certain interval. Next we prove Lemma 6.3.2, which controls how the parity of the number of integer points in an interval changes when an endpoint of the interval is changed. Then we prove that $\left(\frac{a}{p}\right)$ only depends on p modulo $4a$ by applying Gauss's lemma and keeping careful track of intervals as they are rescaled and their endpoints changed. Finally, in Section 6.3.2 we use some basic algebra to deduce the quadratic reciprocity law using the tools we've just developed.

Lemma 6.3.1 (Gauss's Lemma). *Let p be an odd prime and let a be an integer $\not\equiv 0 \pmod{p}$. Form the numbers*

$$a,\ 2a,\ 3a,\ \ldots,\ \frac{p-1}{2}a$$

and reduce them modulo p to lie in the interval $(-\frac{p}{2},\ \frac{p}{2})$. Let ν be the number of negative numbers in the resulting set. Then

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

Proof. In defining ν, we expressed each number in

$$S = \left\{a, 2a, \ldots, \frac{p-1}{2}a\right\}$$

as congruent to a number in the set

$$\left\{1, -1, 2, -2, \ldots, \frac{p-1}{2}, -\frac{p-1}{2}\right\}.$$

No number $1, 2, \ldots, \frac{p-1}{2}$ appears more than once, with either choice of sign, because if it did then either two elements of S are congruent modulo p or 0 is the sum of two elements of S, and both events are impossible. Thus the resulting set must be of the form

$$T = \left\{\varepsilon_1 \cdot 1, \varepsilon_2 \cdot 2, \ldots, \varepsilon_{(p-1)/2} \cdot \frac{p-1}{2}\right\},$$

where each ε_i is either $+1$ or -1. Multiplying together the elements of S and of T, we see that

$$(1a) \cdot (2a) \cdot (3a) \cdots \left(\frac{p-1}{2}a\right) \equiv (\varepsilon_1 \cdot 1) \cdot (\varepsilon_2 \cdot 2) \cdots \left(\varepsilon_{(p-1)/2} \cdot \frac{p-1}{2}\right) \pmod{p},$$

so

$$a^{(p-1)/2} \equiv \varepsilon_1 \cdot \varepsilon_2 \cdots \varepsilon_{(p-1)/2} \pmod{p}.$$

The lemma then follows from Proposition 6.2.1, since $\left(\frac{a}{p}\right) = a^{(p-1)/2}$. $\square$

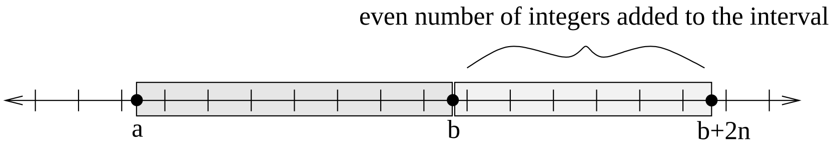

FIGURE 6.1. Illustration of Lemma 6.3.2

6.3.1 Euler's Conjecture

For rational numbers $a, b \in \mathbb{Q}$, let

$$(a, b) \cap \mathbb{Z} = \{x \in \mathbb{Z} : a \le x \le b\}$$

be the set of integers between a and b. The following Lemma will help us to keep track of how many integers lie in certain intervals.

Lemma 6.3.2. *Let $a, b \in \mathbb{Q}$. Then for any integer n,*

$$\#\left((a, b) \cap \mathbb{Z}\right) \equiv \#\left((a, b + 2n) \cap \mathbb{Z}\right) \pmod{2}$$

and

$$\#\left((a, b) \cap \mathbb{Z}\right) \equiv \#\left((a - 2n, b) \cap \mathbb{Z}\right) \pmod{2},$$

provided that each interval involved in the congruence is nonempty.

The statement is illustrated in Figure 6.1. Note that if one of the intervals is empty, then the statement is false; e.g., if $(a, b) = (-1/2, 1/2)$ and $n = -1$ then $\#((a, b) \cap \mathbb{Z}) = 1$ but $\#(a, b-2) \cap \mathbb{Z} = 0$.

Proof. Since $n > 0$,

$$(a, b + 2n) = (a, b) \cup [b, b + 2n),$$

where the union is disjoint. Recall that $\lceil x \rceil$ denotes the least integer $\ge x$. There are $2n$ integers,

$$\lceil b \rceil, \lceil b \rceil + 1, \ldots, \lceil b \rceil + 2n - 1,$$

in the interval $[b, b + 2n)$, so the first congruence of the lemma is true in this case. We also have

$$(a, b - 2n) = (a, b) \backslash [b - 2n, b)$$

and $[b - 2n, b)$ also contains exactly $2n$ integers, so the lemma is also true when n is negative. The statement about $\#\left((a - 2n, b) \cap \mathbb{Z}\right)$ is proved in a similar manner. $\square$

The following proposition was conjectured by Euler, based on extensive numerical evidence. Once we've proved this proposition, it will be easy to deduce the quadratic reciprocity law.

Proposition 6.3.3 (Euler's Conjecture). *Let p be an odd prime and a a positive integer with $p \nmid a$.*

1. *The symbol $\left(\frac{a}{p}\right)$ depends only on p modulo $4a$.*

2. *If q is a prime with $q \equiv -p \pmod{4a}$, then $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.*

Proof. We will apply Lemma 6.3.1 to compute $\left(\frac{a}{p}\right)$. Let

$$S = \left\{a, 2a, 3a, \ldots, \frac{p-1}{2}a\right\}$$

and

$$I = \left(\frac{1}{2}p, p\right) \cup \left(\frac{3}{2}p, 2p\right) \cup \cdots \cup \left(\left(b - \frac{1}{2}\right) p, bp\right),$$

where $b = \frac{1}{2}a$ or $\frac{1}{2}(a-1)$, whichever is an integer. We check that every element of S that reduces to something in the interval $(-\frac{p}{2}, 0)$ lies in I. This is clear if $b = \frac{1}{2}a < \frac{p-1}{2}a$. If $b = \frac{1}{2}(a-1)$, then $bp + \frac{p}{2} > \frac{p-1}{2}a$, so $((b - \frac{1}{2})p, bp)$ is the last interval that could contain an element of S that reduces to $(-\frac{p}{2}, 0)$. Note that the integer endpoints of I are not in S, since those endpoints are divisible by p, but no element of S is divisible by p. Thus, by Lemma 6.3.1,

$$\left(\frac{a}{p}\right) = (-1)^{\#(S \cap I)}.$$

To compute $\#(S \cap I)$, first rescale by a to see that

$$\#(S \cap I) = \#\left(\mathbb{Z} \cap \frac{1}{a} I\right),$$

where

$$\frac{1}{a} I = \left(\left(\frac{p}{2a}, \frac{p}{a}\right) \cup \left(\frac{3p}{2a}, \frac{2p}{a}\right) \cup \cdots \cup \left(\frac{(2b-1)p}{2a}, \frac{bp}{a}\right)\right).$$

Write $p = 4ac + r$, and let

$$J = \left(\left(\frac{r}{2a}, \frac{r}{a}\right) \cup \left(\frac{3r}{2a}, \frac{2r}{a}\right) \cup \cdots \cup \left(\frac{(2b-1)r}{2a}, \frac{br}{a}\right)\right).$$

The only difference between I and J is that the endpoints of intervals are changed by addition of an even integer. By Lemma 6.3.2,

$$\nu = \#\left(\mathbb{Z} \cap \frac{1}{a} I\right) \equiv \#(\mathbb{Z} \cap J) \pmod{2}.$$

Thus $\left(\frac{a}{p}\right) = (-1)^\nu$ depends only on r, i.e., only on p modulo $4a$.

If $q \equiv -p \pmod{4a}$, then the only change in the above computation is that r is replaced by $4a - r$. This changes $\frac{1}{a}I$ into

$$K = \left(2 - \frac{r}{2a}, 4 - \frac{r}{a}\right) \cup \left(6 - \frac{3r}{2a}, 8 - \frac{2r}{a}\right) \cup \cdots \\ \cup \left(4b - 2 - \frac{(2b-1)r}{2a}, 4b - \frac{br}{a}\right).$$

Thus K is the same as $-\frac{1}{a}I$, except even integers have been added to the endpoints. By Lemma 6.3.2,

$$\#(K \cap \mathbb{Z}) \equiv \#\left(\left(\frac{1}{a}I\right) \cap \mathbb{Z}\right) \pmod{2},$$

so $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$, which completes the proof. $\square$

The following more careful analysis in the special case when $a = 2$ helps illustrate the proof of the above lemma, and is frequently useful in computations.

Proposition 6.3.4. *Let p be an odd prime. Then*

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

Proof. When $a = 2$, the set $S = \{a, 2a, \ldots, 2 \cdot \frac{p-1}{2}\}$ is

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

We must count the parity of the number of elements of S that lie in the interval $I = (\frac{p}{2}, p)$. Writing $p = 8c + r$, we have

$$\begin{aligned} \#\,(I \cap S) &= \#\left(\frac{1}{2}I \cap \mathbb{Z}\right) = \#\left(\left(\frac{p}{4}, \frac{p}{2}\right) \cap \mathbb{Z}\right) \\ &= \#\left(\left(2c + \frac{r}{4}, 4c + \frac{r}{2}\right) \cap \mathbb{Z}\right) \equiv \#\left(\left(\frac{r}{4}, \frac{r}{2}\right) \cap \mathbb{Z}\right) \pmod{2}, \end{aligned}$$

where the last equality comes from Lemma 6.3.2. The possibilities for r are $1, 3, 5, 7$. When $r = 1$, the cardinality is 0, when $r = 3, 5$ it is 1, and when $r = 7$ it is 2. $\square$

6.3.2 Proof of Quadratic Reciprocity

It is now straightforward to deduce the quadratic reciprocity law.

First Proof of Theorem 6.1.3. First suppose that $p \equiv q \pmod 4$. By swapping p and q if necessary, we may assume that $p > q$, and write $p - q = 4a$. Since $p = 4a + q$,

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

and

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

Proposition 6.3.3 implies that $\left(\frac{a}{q}\right) = \left(\frac{a}{p}\right)$, since $p \equiv q \pmod{4a}$. Thus

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

where the last equality is because $\frac{p-1}{2}$ is even if and only if $\frac{q-1}{2}$ is even.

Next suppose that $p \not\equiv q \pmod 4$, so $p \equiv -q \pmod 4$. Write $p + q = 4a$. We have

$$\left(\frac{p}{q}\right) = \left(\frac{4a-q}{q}\right) = \left(\frac{a}{q}\right), \quad \text{and} \quad \left(\frac{q}{p}\right) = \left(\frac{4a-p}{p}\right) = \left(\frac{a}{p}\right).$$

Since $p \equiv -q \pmod{4a}$, Proposition 6.3.3 implies that $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$. Since $(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = 1$, the proof is complete. □

Example 6.3.5. Is 3 a square modulo $p = 726377359$? We proved that the answer is "no" in the previous lecture by computing $3^{p-1} \pmod p$. It's easier to prove that the answer is no using Theorem 6.1.3:

$$\left(\frac{3}{726377359}\right) = (-1)^{1\cdot\frac{726377358}{2}}\cdot\left(\frac{726377359}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

6.4 A Proof of Quadratic Reciprocity Using Gauss Sums

In this section we present a beautiful proof of Theorem 6.1.3 using algebraic identities satisfied by sums of "roots of unity". The objects we introduce in the proof are of independent interest, and provide a powerful tool to prove higher-degree analogues of quadratic reciprocity. (For more on higher reciprocity see [IR90]. See also Section 6 of [IR90] on which the proof below is modeled.)

Recall that a *complex number* is a number of the form $a + b\sqrt{-1}$, where a and b are real numbers, and that the set of complex numbers forms a field.

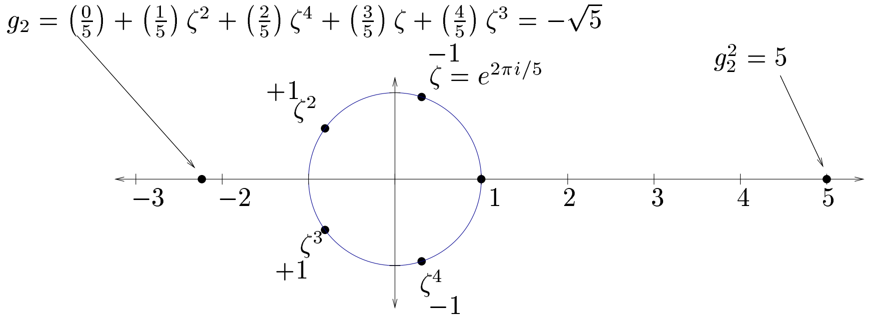

FIGURE 6.2. Gauss sum g_2 for $p = 5$

Definition 6.4.1 (Root of Unity). An nth *root of unity* is a complex number ζ such that $\zeta^n = 1$. A root of unity is *primitive* if n is the smallest positive integer such that $\zeta^n = 1$.

Since for θ a real number, $e^{i\theta} = \cos(\theta) + i\sin(\theta)$, the complex number $e^{2\pi i/n}$ is an nth root of unity.

For the rest of this section, fix a prime p and a primitive pth root ζ of unity, e.g., $\zeta = e^{2\pi i/p}$.

Definition 6.4.2 (Gauss Sum). The *Gauss sum* associated to an integer a is

$$g_a = \sum_{n=0}^{p-1} \left(\frac{n}{p}\right) \zeta^{an}.$$

(Note that p is implicit in the definition of g_a. If we were to change p, then the Gauss sum g_a associated to a would be different.)

Figure 6.2 illustrates the Gauss sum g_2 for $p = 5$. The picture suggests the following proposition, whose proof will require some work.

Proposition 6.4.3. *For any a not divisible by p,*

$$g_a^2 = (-1)^{(p-1)/2} p.$$

In order to prove the proposition, we introduce a few lemmas.

Lemma 6.4.4. *Let p be a prime. Then for any integer a,*

$$\sum_{n=0}^{p-1} \zeta^{an} = \begin{cases} p, & \text{if } a \equiv 0 \pmod{p} \\ 0, & \text{otherwise.} \end{cases}$$

Proof. If $a \equiv 0 \pmod{p}$, then $\zeta^a = 1$, so the sum equals the number of summands, which is p. If $a \not\equiv 0 \pmod{p}$, then we use the identity $x^p - 1 = (x-1)(x^{p-1} + \cdots + x + 1)$ with $x = \zeta^a$. We have $\zeta^a \neq 1$, so $\zeta^a - 1 \neq 0$ and

$$\sum_{n=0}^{p-1} \zeta^{an} = \frac{\zeta^{ap} - 1}{\zeta^a - 1} = 0.$$

□

Lemma 6.4.5. *Let x and y be integers and let $\delta(x,y)$ be 1 if $x=y$ or 0 if $x \neq y$. Then*

$$\sum_{n=0}^{p-1} \zeta^{n(x-y)} = p \cdot \delta(x,y).$$

Proof. This follows immediately from Lemma 6.4.4. □

Lemma 6.4.6. *Let p be a prime. Then*

$$\sum_{n=0}^{p-1} \left(\frac{n}{p}\right) = 0.$$

Proof. By Proposition 6.2.5 the map

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

is a surjective homomorphism of groups. Thus exactly half the elements of $(\mathbb{Z}/p)^{\times}$ map to $+1$ and half map to -1. Since $\left(\frac{0}{p}\right) = 0$, the sum in the statement of the lemma is 0. □

Lemma 6.4.7. *Let p be a prime and a any integer. Then*

$$g_a = \left(\frac{a}{p}\right) g_1.$$

Proof. When $a \equiv 0 \pmod{p}$ the lemma is implied by Lemma 6.4.6, so suppose that $a \not\equiv 0 \pmod{p}$. Then

$$\left(\frac{a}{p}\right) g_a = \left(\frac{a}{p}\right) \sum_{n=0}^{p-1} \left(\frac{n}{p}\right) \zeta^{an} = \sum_{n=0}^{p-1} \left(\frac{an}{p}\right) \zeta^{an} = \sum_{m=0}^{p-1} \left(\frac{m}{p}\right) \zeta^{m} = g_1.$$

Now multiply both sides by $\left(\frac{a}{p}\right)$ and use that $\left(\frac{a}{p}\right)^2 = 1$. □

We now have enough lemmas to prove Proposition 6.4.3.

Proof of Proposition 6.4.3. We evaluate the sum $\sum_{a=0}^{p-1} g_a g_{-a}$ in two different ways. For $a \neq 0$,

$$g_a g_{-a} = \left(\frac{a}{p}\right) g_1 \left(\frac{-a}{p}\right) g_1 = \left(\frac{-1}{p}\right) \left(\frac{a}{p}\right)^2 g_1^2 = (-1)^{(p-1)/2} g_1^2,$$

where the last step follows from Proposition 6.2.1 and the fact that $\left(\frac{a}{p}\right) \in \{\pm 1\}$. Thus

$$\sum_{a=0}^{p-1} g_a g_{-a} = (p-1)(-1)^{(p-1)/2} g_1^2. \tag{6.1}$$

On the other hand,

$$\begin{aligned} g_a g_{-a} &= \sum_{n=0}^{p-1} \left(\frac{n}{p}\right) \zeta^{an} \sum_{m=0}^{p-1} \left(\frac{m}{p}\right) \zeta^{-am} \\ &= \sum_{n=0}^{p-1} \sum_{m=0}^{p-1} \left(\frac{n}{p}\right) \left(\frac{m}{p}\right) \zeta^{an} \zeta^{-am} \\ &= \sum_{n=0}^{p-1} \sum_{m=0}^{p-1} \left(\frac{n}{p}\right) \left(\frac{m}{p}\right) \zeta^{an-am}. \end{aligned}$$

Thus by Lemma 6.4.5,

$$\begin{aligned} \sum_{a=0}^{p-1} g_a g_{-a} &= \sum_{a=0}^{p-1} \sum_{n=0}^{p-1} \sum_{m=0}^{p-1} \left(\frac{n}{p}\right) \left(\frac{m}{p}\right) \zeta^{an-am} \\ &= \sum_{n=0}^{p-1} \sum_{m=0}^{p-1} \left(\frac{n}{p}\right) \left(\frac{m}{p}\right) \sum_{a=0}^{p-1} \zeta^{an-am} \\ &= \sum_{n=0}^{p-1} \sum_{m=0}^{p-1} \left(\frac{n}{p}\right) \left(\frac{m}{p}\right) p\delta(n,m) \\ &= \sum_{n=0}^{p-1} \left(\frac{n}{p}\right)^2 p = p(p-1). \end{aligned}$$

Equating (6.1) and the above equality then canceling $(p-1)$ shows that

$$g_1^2 = (-1)^{(p-1)/2} p.$$

Since $a \not\equiv 0 \pmod{p}$, we have $\left(\frac{a}{p}\right)^2 = 1$, so by Lemma 6.4.7,

$$g_a^2 = \left(\frac{a}{p}\right)^2 g_1^2 = g_1^2,$$

and the proposition is proved. □

6.4.1 Proof of Quadratic Reciprocity

We are now in a position to prove Theorem 6.1.3 using Gauss sums.

Proof. Let $q \neq p$ be an odd prime. Set $p^* = (-1)^{(p-1)/2}p$ and recall that Proposition 6.4.3 asserts that $p^* = g^2$, where $g = g_1 = \sum_{n=0}^{p-1} \left(\frac{n}{p}\right) \zeta^n$ is a Gauss sum with $\zeta = e^{2\pi i/p}$ a primitive pth root of unity.

Proposition 6.2.1 trivially implies that

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

We have $g^{q-1} = (g^2)^{(q-1)/2} = (p^*)^{(q-1)/2}$, so multiplying both sides of the above equation by g yields a congruence

$$g^q \equiv g \left(\frac{p^*}{q}\right) \pmod{q}. \tag{6.2}$$

But what does this congruence *mean*, given that g^q is not an integer? In Exercise 8, you will prove that every $\mathbb{Z}$-linear combination of powers of ζ can be written uniquely as a $\mathbb{Z}$-linear combination of elements of $B = \{1, \zeta, \ldots, \zeta^{p-2}\}$. The above congruence simply means that if we write g^q and $g\left(\frac{p^*}{q}\right)$ as $\mathbb{Z}$-linear combinations of the elements of B then the coefficients of the linear combination are congruent modulo q.

Another useful property of congruences, which you will prove in Exercise 9, is that if x and y are two $\mathbb{Z}$-linear combinations of powers of ζ, then $(x+y)^p \equiv x^p + y^p \pmod{p}$. Applying this in our current situation, we see (also using that q is odd) that

$$g^q = \left(\sum_{n=0}^{p-1} \left(\frac{n}{p}\right) \zeta^n\right)^q \equiv \sum_{n=0}^{p-1} \left(\frac{n}{p}\right)^q \zeta^{nq} \equiv \sum_{n=0}^{p-1} \left(\frac{n}{p}\right) \zeta^{nq} \equiv g_q \pmod{q}.$$

By Lemma 6.4.7,

$$g^q \equiv g_q = \left(\frac{q}{p}\right) g \pmod{q}.$$

Combining this with (6.2) yields

$$\left(\frac{q}{p}\right) g \equiv \left(\frac{p^*}{q}\right) g \pmod{q}.$$

Since $g^2 = p^*$ and $p \neq q$, we can cancel g from both sides and find that $\left(\frac{q}{p}\right) \equiv \left(\frac{p^*}{q}\right) \pmod{q}$. Since both residue symbols are ± 1 and q is odd, it follows that $\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right)$. Finally, we note (using Proposition 6.2.1) that

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

□

6.5 How To Find Square Roots

After all this theory, we return in this section to the computational question of computing square roots.

One of the first things a school child learns in their algebra course is that the solutions to the quadratic equation

$$ax^2 + bx + c = 0 \qquad \text{(with } a \neq 0\text{)}$$

are

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a},$$

as one can see, e.g., by substituting the formula on the right back into the quadratic equation.

In school, $a \neq 0$, b, and c are typically chosen to be real or complex numbers. We're grown up now, so let p be an odd prime, and suppose instead that $a, b, c \in \mathbb{Z}/p$. Then the quadratic formula still gives solutions to $ax^2 + bx + c = 0$, and using Proposition 5.1.1 we can see that it gives all of them.

Using Theorem 6.1.3, we can decide whether or not $b^2 - 4ac$ is a perfect square, and hence whether or not $ax^2 + bx + c = 0$ has a solution in $\mathbb{Z}/p$. If $b^2 - 4ac$ *is* a perfect square, Theorem 6.1.3 says nothing about finding an actual square root. Also, note that for this problem we do *not* need quadratic reciprocity; in practice to decide whether an element of $\mathbb{Z}/p$ is a perfect square Proposition 6.2.1 is fast, in light of Section 3.5.

Suppose $a \in \mathbb{Z}/p$ is a nonzero quadratic residue. If $p \equiv 3 \pmod 4$ then $b = a^{\frac{p+1}{4}}$ is a square root of a because

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

I've read that there is no publically known deterministic polynomial time algorithm to compute a square root of a when $p \equiv 1 \pmod 4$. The following is a probabilistic algorithm to compute a square root of a. Let R be the ring $(\mathbb{Z}/p)[x]/(x^2 - a)$. Thus

$$R = \{u + vx : u, v \in \mathbb{Z}/p\}$$

with

$$(u + vx)(z + wx) = (uz + awv) + (uw + vz)x.$$

Let b and c be the square roots of a (we can't compute b and c at this stage, but we can consider them in order to deduce an algorithm to find them). Then by a generalization of the Chinese Remainder Theorem, there is a ring isomorphism

$$\varphi : R \longrightarrow \mathbb{Z}/p \times \mathbb{Z}/p$$

given by $\varphi(u+vx) = (u+vb, u+vc)$. Let z be a random element of $(\mathbb{Z}/p)^\times$ and let $u+vx = (1+zx)^{\frac{p-1}{2}}$. If $v \neq 0$ we can quickly find b and c as follows. The quantity $u+vb$ is a $(p-1)/2$th power in $\mathbb{Z}/p$, so it equals either 0, 1, or -1. Thus $b = -u/v$, $(1-u)/v$, or $(-1-u)/v$. Since we know u and v we can try each of $-u/v$, $(1-u)/v$, and $(-1-u)/v$ and see which is a square root of a.

Example 6.5.1. Continuing example 6.1.4, we find a square root of 69 modulo 389. We apply the algorithm described above in the case $p \equiv 1 \pmod 4$. We first choose the random element $1+24x$, and find that $(1+24x)^{194} = -1$. The coefficient of x in the power is 0, so we try again. This time we have $(1+51x)^{194} = 239x = u+vx$. The inverse of 239 in $\mathbb{Z}/389$ is 153, so we consider the following three possibilities for a square root of 69:

$$-\frac{u}{v} = 0 \qquad \frac{1-u}{v} = 153 \qquad -\frac{1-u}{v} = -153.$$

Thus 153 and -153 are the square roots of 69 in $\mathbb{Z}/389$.

Exercises

6.1 Calculate the following symbols by hand: $\left(\frac{3}{97}\right)$, $\left(\frac{5}{389}\right)$, $\left(\frac{2003}{11}\right)$, and $\left(\frac{5!}{7}\right)$.

6.2 Prove that for $p \geq 5$ prime, $\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 11 \pmod{12}, \\ -1 & \text{if } p \equiv 5, 7 \pmod{12}. \end{cases}$

6.3 Use the fact that $(\mathbb{Z}/p)^\times$ is cyclic to give a direct proof that $\left(\frac{-3}{p}\right) = 1$ when $p \equiv 1 \pmod 3$. [Hint: There is an $c \in (\mathbb{Z}/p)^\times$ of order 3. Show that $(2c+1)^2 = -3$.]

6.4 If $p \equiv 1 \pmod 5$, show directly that $\left(\frac{5}{p}\right) = 1$ by the method of Exercise 3. [Hint: Let $c \in (\mathbb{Z}/p)^\times$ be an element of order 5. Show that $(c+c^4)^2 + (c+c^4) - 1 = 0$, etc.]

6.5 For which primes p is $\displaystyle\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0$?

6.6 How many natural numbers $x < 2^{13}$ satisfy the equation

$$x^2 \equiv 5 \pmod{2^{13}-1}?$$

(You may assume that $2^{13}-1$ is prime.)

6.7 Find the natural number $x < 97$ such that $x \equiv 4^{48} \pmod{97}$. (Note that 97 is prime.)

6.8 Let p be a prime and let ζ be a primitive pth root of unity. Prove that every $\mathbb{Z}$-linear combination of powers of ζ can be written uniquely as a $\mathbb{Z}$-linear combination of elements of $B = \{1, \zeta, \ldots, \zeta^{p-2}\}$. [Hint: $\zeta^p - 1 = 0$, so $\zeta^{p-1} + \cdots + \zeta + 1 = 0$, so $\zeta^{p-1} = -(\zeta^{p-2} + \cdots + \zeta + 1)$. Next prove that the polynomial $x^{p-1} + \cdots + x + 1$ does not factor over $\mathbb{Q}$.]

6.9 Let p be a prime and let ζ be a primitive pth root of unity. Suppose that x and y are $\mathbb{Z}$-linear combinations of powers of ζ. Prove that $(x + y)^p \equiv x^p + y^p \pmod{p}$.

6.10 Formulate an analogue of quadratic reciprocity for $\left(\frac{a}{q}\right)$ but without the restriction that q be a prime. By "analogue of quadratic reciprocity", I mean an easy way to tell whether or not a is a square modulo q. [Hint: Use Theorem 3.4.2 to reduce to the case where q is a prime power. Prove that if p is an odd prime that doesn't divide a then a is a square modulo p if and only if a is a square modulo p^n for any positive n.]