Chapter 3

Quadratic Reciprocity and Primitive Roots

In this chapter, we consider congruence equations of degree 2 or higher. This topic leads to the Theorem of Quadratic Reciprocity (Theorem 3.14) and to studying primitive roots.

1. Quadratic Reciprocity

Consider the simplest quadratic equation $x^2 = a$ for an integer a. This has an integer solution exactly when a is a perfect square (this is the definition of a perfect square). There are exactly two solutions $\pm\sqrt{a}$, unless $a = 0$, then there is one solution. What happens in modular arithmetic?

Question 3.1. Given a positive integer n and an integer a, when can you solve

$$x^2 \equiv a \pmod{n}?$$

How many solutions does it have?

Example 3.2. With a few simple examples, we can encounter a wide range of behaviors.

- $x^2 \equiv 2 \pmod 3$ has no solutions.
- $x^2 \equiv 2 \pmod 7$ has two solutions.
- $x^2 \equiv 1 \pmod 5$ has two solutions.
- $x^2 \equiv 1 \pmod{12}$ has four solutions.

One of the most interesting of these is the first example, which shows that square roots do not always exist in modular arithmetic!

We give a name to the numbers that have a square root.

Definition 3.3. Given a positive integer n and an integer a relatively prime to n, we say that a is a *quadratic residue modulo* n if the equation $x^2 \equiv a \pmod{n}$ has a solution. If the equation $x^2 \equiv a \pmod{n}$ does not have a solution, we say that a is a *quadratic nonresidue modulo* n.

Investigation 3.4. Given a modulus n, determine how many residue classes are quadratic residues modulo n. Do you see a pattern? Start by considering the case when n is a prime number.

We will address the following question.

Question 3.5. Let p be a prime number. How many of the complete set of residues $\{0, 1, \ldots, p-1\}$ modulo p are quadratic residues?

1.1. Euler's Criterion and the Legendre Symbol.

Example 3.6. We take the first few primes and list the nonzero a values for which we can solve $x^2 \equiv a \pmod{p}$ and those for which we cannot.

p	$x^2 \equiv a \pmod{p}$ for some x	$x^2 \not\equiv a \pmod{p}$ for some x
2	1	
3	1	2
5	$1, 4$	$2, 3$
7	$1, 2, 4$	$3, 5, 6$
11	$1, 3, 4, 5, 9$	$2, 6, 7, 8, 10$
13	$1, 3, 4, 9, 10, 12$	$2, 5, 6, 7, 8, 11$
17	$1, 2, 4, 8, 9, 13, 15, 16$	$3, 5, 6, 7, 10, 11, 12, 14$

It seems that about half of all residue classes are quadratic residues. For $p = 2$ all nonzero residue classes are quadratic residues, so our theorem must exclude 2.

Theorem 3.7. *If $p > 2$ is a prime and $a \neq 0$, then $x^2 \equiv a \pmod{p}$ has either zero or two solutions.*

Proof. Assume that b is a solution, then $-b$ is also a solution. For $p > 2$, since b is nonzero and $-b \not\equiv b \pmod{p}$, if there is one solution, then there are at least two solutions. Now assume that c is any solution. Being a solution implies

$$c^2 \equiv b^2 \equiv a \pmod{p},$$

which is the same as

$$c^2 - b^2 \equiv 0 \pmod{p}.$$

Then

$$p \mid b^2 - c^2 = (b-c)(b+c).$$

Since p is prime, $p \mid b + c$ or $p \mid b - c$. In other words, $b \equiv c \pmod{p}$ or $-b \equiv c \pmod{p}$. Therefore, c is not a new solution. □

Corollary 3.8. *If $p > 2$ is a prime, then there are exactly $\frac{p-1}{2}$ nonzero quadratic residues modulo p (and $\frac{p-1}{2}$ quadratic nonresidues).*

Proof. Consider the complete system of nonzero residues $\{1, \ldots, p-1\}$. Let $\{a_1, \ldots, a_{p-1}\}$ be their squares modulo p; in other words,

$$\begin{aligned} 1^2 &\equiv a_1 \pmod{p} \\ 2^2 &\equiv a_2 \pmod{p} \\ &\vdots \\ (p-1)^2 &\equiv a_{p-1} \pmod{p}. \end{aligned}$$

Since $x^2 \equiv a \pmod{p}$ has either zero or two solutions for $a \neq 0$, each a_i occurs exactly twice in the list. Thus, there are $\frac{p-1}{2}$ nonzero quadratic residues modulo p. □

We now know how often we can solve $x^2 \equiv a \pmod{p}$ and how many solutions can exist. However, given a particular a and p, we still have no way to determine whether a solution exists other than simply checking all possible residues. To help with this problem, we define the Legendre[1] symbol.

Definition 3.9. Let $p > 2$ be a prime, and let a be an integer not divisible by p. Then we define the *Legendre symbol* as

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

Notice that the Legendre symbol depends only on the residue class of a; that is, if $a \equiv b \pmod{p}$, then we have

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

In 1748 Euler proved a way to compute Legendre symbols and, thus, determine whether a is a quadratic residue modulo p.

Theorem 3.10 (Euler's criterion). *Let $p > 2$ be a prime, and let a be an integer not divisible by p. Then*

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

Proof. We start with Fermat's Little Theorem (Theorem 2.21),

$$a^{p-1} - 1 \equiv 0 \pmod{p}.$$

We can factor this as

$$\left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod{p}.$$

Since p is prime, by Lemma 1.38 we must have

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \quad \text{or} \quad a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

[1] Adrien-Marie Legendre (1752–1833) was a French mathematician.

If a is a quadratic residue, then there is some b such that

$$b^2 \equiv a \pmod{p}.$$

Then we have

$$(b^2)^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \pmod{p}.$$

Thus, every quadratic residue satisfies

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Now assume that a is a quadratic nonresidue. Then we may partition the nonzero residues $\{1, \dots, p-1\}$ into pairs of distinct numbers (x, y) such that

$$xy \equiv a \pmod{p}.$$

In particular, given y, there is a unique x that solves the linear equation

$$xy \equiv a \pmod{p}. \tag{11}$$

We can always solve equation (11) because every nonzero residue y is relatively prime to p. There are $\frac{p-1}{2}$ such pairs, so we have that

$$a^{\frac{p-1}{2}} = \prod_{\text{pairs } (x,y)} xy = (p-1)!.$$

Since $x^2 \equiv 1 \pmod{p}$ has exactly two solutions, ± 1, each number $\{1, \dots, p-1\}$ has an inverse modulo p and, except for ± 1, the inverse is different from the number. So we have

$$a^{\frac{p-1}{2}} \equiv (p-1)! \equiv -1 \pmod{p}. \qquad \square$$

We apply Euler's criterion to show that the Legendre symbol is multiplicative.

Corollary 3.11. *Let $p > 2$ be a prime, and let a and b be integers not divisible by p. Then*

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

Proof. We compute

$$\left(\frac{ab}{p}\right) = (ab)^{\frac{p-1}{2}} \mod p = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \mod p = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right). \qquad \square$$

Because we know the Legendre symbol is multiplicative, we have reduced its computation to the two situations of $\left(\frac{2}{p}\right)$ and $\left(\frac{q}{p}\right)$, where p and q are distinct (odd) primes.

Investigation 3.12.

(a) Given two distinct odd primes p and q, can you determine when p is a quadratic residue modulo q?

(b) If p is a quadratic residue modulo q, does that tell you anything about whether q is a quadratic residue modulo p?

It may be helpful to separate the cases of p and q congruent to 1 or 3 modulo 4.

1.2. Law of Quadratic Reciprocity. The prime 2, as the only even prime, often must be considered separately. We consider the primes p for which 2 is a quadratic residue. Let's gather some data and see what patterns arise.

primes for which 2 is a quadratic residue
7, 17, 23, 31, 41, 47, 71, 73, 79, 89, 97

primes for which 2 is a quadratic nonresidue
3, 5, 11, 13, 19, 29, 37, 43, 53, 59, 61, 67, 83

Since the primes p are all odd, it makes sense to examine their residue class modulo powers of 2. After some experimentation we see that the residue class modulo 8 is the determining factor. For the quadratic residues we have

$$\begin{aligned} 17, 41, 73, 89, 97 &\equiv 1 \pmod{8}, \\ 7, 23, 31, 47, 71, 79 &\equiv 7 \pmod{8}. \end{aligned}$$

For the quadratic nonresidues we have

$$\begin{aligned} 3, 11, 19, 43, 59, 67, 83 &\equiv 3 \pmod{8}, \\ 5, 13, 29, 37, 53, 61 &\equiv 5 \pmod{8}. \end{aligned}$$

In summary, for primes congruent to 1 or 7 modulo 8, 2 is a quadratic residue. For primes that are congruent to 3 or 5 modulo 8, 2 is a quadratic nonresidue. We state this as the supplemental Law of Quadratic Reciprocity.

Theorem 3.13 (Supplemental law). *Let $p > 2$ be a prime number. Then*

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

There are elementary proofs using messy congruences, but instead let's use the roots of unity for a more conceptually pleasing proof.

Proof. Let $\zeta = \sqrt{i}$, where $i^2 = -1$. The number ζ is called an 8*th root of unity* since $\zeta^8 = 1$. Let ζ^{-1} be the inverse of ζ, and let $w = \zeta + \zeta^{-1}$. Then we can verify that $w = \sqrt{2}$ as

$$w^2 = (\zeta + \zeta^{-1})^2 = \zeta^2 + 2 + \zeta^{-2} = i + 2 - i = 2.$$

Note that we used the fact that $\frac{1}{i} = -i$. Now we apply Euler's criterion to $\left(\frac{2}{p}\right)$:

$$\begin{aligned} 2^{\frac{p-1}{2}} &= (\sqrt{2})^{p-1} = w^{p-1} = w^p w^{-1} = (\zeta + \zeta^{-1})^p w^{-1} \\ &\equiv (\zeta^p + \zeta^{-p}) w^{-1} \pmod{p}. \end{aligned}$$

The last equivalence follows from the binomial expansion of $(\zeta + \zeta^{-1})^p$ as

$$(\zeta + \zeta^{-1})^p \equiv \zeta^p + \zeta^{-p} \pmod{p}.$$

However, we can compute $\zeta^p + \zeta^{-p}$ using the fact that ζ is an 8th root of unity. In particular, ζ^p can be computed just from the remainder of p after division by 8. For example

$$\zeta^{12} = \zeta^8 \zeta^4 = 1 \cdot \zeta^4 = \zeta^4$$

or

$$\zeta^{27} = \zeta^8\zeta^8\zeta^8\zeta^3 = 1 \cdot 1 \cdot 1 \cdot \zeta^3 = \zeta^3.$$

We compute

$$\zeta^p + \zeta^{-p} \equiv \begin{cases} \zeta + \zeta^{-1} \equiv w \pmod{p} & p \equiv \pm 1 \pmod{8}, \\ \zeta^3 + \zeta^{-3} \equiv -w \pmod{p} & p \equiv \pm 3 \pmod{8}. \end{cases}$$

So we have

$$\begin{aligned} 2^{\frac{p-1}{2}} &\equiv (\zeta^p + \zeta^{-p})w^{-1} \pmod{p} \\ &\equiv \begin{cases} 1 \pmod{p} & p \equiv \pm 1 \pmod{8}, \\ -1 \pmod{p} & p \equiv \pm 3 \pmod{8}. \end{cases} \end{aligned} \qquad \square$$

With $\left(\frac{2}{p}\right)$ solved, we now turn to the situation of Legendre symbols for odd primes, $\left(\frac{q}{p}\right)$. First let's gather some data where we abbreviate R for quadratic residue and N for quadratic nonresidue.

		p										
q		3	5	7	11	13	17	19	23	29	31	37
	3		N	N	R	R	N	N	R	N	N	R
	5	N		N	R	N	N	R	N	R	R	N
	7	R	N		N	N	N	R	N	R	R	R
	11	N	R	R		N	N	R	N	N	N	R
	13	R	N	N	N		R	N	R	R	N	N
	17	N	N	N	N	R		R	N	N	N	N
	19	R	R	N	N	N	R		N	N	R	N
	23	N	N	R	R	R	N	R		R	N	N
	29	N	R	R	N	R	N	N	R		N	N
	31	R	R	N	R	N	N	N	R	N		N
	37	R	N	R	R	N	N	N	N	N	N	

Unfortunately, there does not seem to be much of a pattern here. However, if we consider only the cases where $p \equiv 1 \pmod{4}$ or $q \equiv 1 \pmod{4}$, there is a striking symmetry around the diagonal.

		p										
q		3	5	7	11	13	17	19	23	29	31	37
	3		N			R	N			N		R
	5	N		N	R	N	N	R	N	R	R	N
	7		N			N	N			R		R
	11		R			N	N			N		R
	13	R	N	N	N		R	N	R	R	N	N
	17	N	N	N	N	R		R	N	N	N	N
	19		R			N	R			N		N
	23		N			R	N			R		N
	29	N	R	R	N	R	N	N	R		N	N
	31		R			N	N			N		N
	37	R	N	R	R	N	N	N	N	N	N	

Legendre and Euler both conjectured the following theorem, called the Law of Quadratic Reciprocity, but it was first proven by Gauss[2] in 1801. In fact, Gauss gave six different proofs. To date, there are well over 200 distinct proofs of quadratic reciprocity.

Theorem 3.14 (Quadratic Reciprocity). *Let $p, q > 2$ be distinct prime numbers. Then*

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

We need two easy facts about the Legendre symbol for the proof.

Lemma 3.15. *Let $p > 2$ be a prime. For every integer a not divisible by p, the equation $x^2 \equiv a \pmod{p}$ has*

$$1 + \left(\frac{a}{p}\right)$$

solutions.

Proof. If there is a solution, then by Theorem 3.7 there are two solutions. Similarly, if there is a solution, then a is a quadratic residue, and thus $\left(\frac{a}{p}\right) = 1$.

If there are no solutions, then a is a quadratic nonresidue and $\left(\frac{a}{p}\right) = -1$. □

Lemma 3.16. *Let $p > 2$ be a prime. Then*

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

Proof. Since exactly half of the a are quadratic residues and half are quadratic nonresidues, the sum of their Legendre symbols is 0. □

Now we are ready to prove the Law of Quadratic Reciprocity.

Proof of Theorem 3.14. The proof proceeds by counting the number of solutions to

$$x_1^2 - x_2^2 + x_3^2 - \cdots + x_p^2 \equiv 1 \pmod{q} \tag{12}$$

in two different ways.

Define N_p to be the number of solutions to equation (12). First substitute $x_1 = x_1 + x_2$ to get

$$x_1^2 + x_3^2 - x_4^2 + \cdots + x_p^2 \equiv -2x_1x_2 \pmod{p}.$$

For each $x_1 \neq 0$ and any choice of $(x_3, \ldots, x_p)$, there is a unique x_2 value that solves the resulting (linear) equation. So there are $q^{p-2}(q-1)$ solutions of this form: $(q-1)$ choices for x_1, and q choices for each of $\{x_3, \ldots, x_p\}$. When $x_1 = 0$, the solutions satisfy

$$x_3^2 - x_4^2 + \cdots + x_p^2 \equiv 1 \pmod{q}$$

for any value of x_2.

[2] Carl Friedrich Gauss (1777–1855) was a German mathematician.

By renaming the variables, this is the same as

$$y_1^2 - y_2^2 + \cdots + y_{p-2}^2 \equiv 1 \pmod{q},$$

which has N_{p-2} solutions. These solutions are valid for any choice of x_2 for a total of qN_{p-2} more solutions. Thus,

$$\begin{aligned}
N_p &= q^{p-2}(q-1) + qN_{p-2} \\
&\quad \text{now substitute } N_{p-2} = q^{-4}(q-1)qN_{p-4} \text{ to get} \\
&= q^{p-2}(q-1) + q(q^{p-4}(q-1) + qN_{p-4}) \\
&= q^{p-1} - q^{p-2} + q^{p-2} - q^{p-3} + q^2 N_{p-4} \\
&= q^{p-1} - q^{p-3} + q^2 N_{p-4} \\
&\quad \text{now substitute for } N_{p-4} \text{ to get} \\
&= q^{p-1} - q^{p-3} + q^2(q^{p-6}(q-1) + qN_{p-6}) \\
&= q^{p-1} - q^{p-3} + q^{p-3} - q^{p-4} + q^3 N_{p-6}) \\
&= q^{p-1} - q^{p-4} + q^3 N_{p-6}) \\
&\vdots \\
&= q^{p-1} - q^{\frac{p-1}{2}} + q^{\frac{p-1}{2}} N_1 \\
&= q^{p-1} - q^{\frac{p-1}{2}} + 2q^{\frac{p-1}{2}} \\
&= q^{p-1} + q^{\frac{p-1}{2}} \\
&\equiv 1 + \left(\frac{q}{p}\right) \pmod{p}.
\end{aligned} \tag{13}$$

Now we count solutions to equation (12) another way. Let $N(x^2 \equiv a \pmod{q})$ be the number of solutions to the quadratic equation $x^2 \equiv a \pmod{q}$. Then we can also determine N_p as

$$\begin{aligned}
N_p = \sum_{t_1+\cdots+t_p \equiv 1 \pmod{q}} & N(x_1^2 \equiv t_1 \pmod{q}) \cdot N(x_1^2 \equiv -t_2 \pmod{q}) \\
& \cdot N(x_3^2 \equiv t_3 \pmod{q}) \cdots N(x_p^2 \equiv t_p \pmod{q}).
\end{aligned}$$

First note that in the set of possible tuples $(t_1, \ldots, t_p)$, each t_i takes on each possible residue class modulo q a power of q times. Consequently, by Lemma 3.16 we have

$$\sum_{t_i} \left(\frac{t_i}{q}\right) = 0.$$

We expand this product and apply Lemma 3.16 to get

$$\begin{aligned} N_p = &\sum_{t_1+\cdots+t_p\equiv 1 \pmod q} 1 + \sum_{i=1}^{p}\left(\frac{(-1)^{i+1}t_i}{q}\right) + \sum_{i,j=1}^{p}(-1)^{i+j}\left(\frac{t_i}{q}\right)\left(\frac{t_j}{q}\right) \\ &\quad + \cdots + (-1)^{(p-1)/2}\prod_{i=1}^{p}\left(\frac{t_i}{q}\right) \\ = &\sum_{t_1+\cdots+t_p\equiv 1 \pmod q} 1 + \sum_{i=1}^{p}\left(\frac{-1}{q}\right)^{i+1}\left(\frac{t_i}{q}\right) + \cdots + \left(\frac{-1}{q}\right)^{\frac{p-1}{2}}\left(\frac{t_1\cdots t_p}{q}\right) \\ = &\sum_{t_1+\cdots+t_p=1} 1 + 0 + \cdots + 0 + \left(\frac{-1}{q}\right)^{\frac{p-1}{2}}\left(\frac{t_1t_2\cdots t_p}{q}\right) \\ = &\, q^{p-1} + \left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right)\sum_{t_1+\cdots+t_p\equiv 1 \pmod q}\left(\frac{t_1t_2\cdots t_p}{q}\right). \end{aligned}$$

Now we examine this expression for N_p modulo p, as in the previous part of the proof. The only terms of the sum that are nonzero modulo p are those where $t_1 \equiv t_2 \equiv \cdots \equiv t_p \equiv p^{-1} \pmod q$ since, by symmetry, the other terms can be collected into groups of size p. For example, if $t_1 \equiv 2^{-1} \pmod q$, then we have terms of the form $\sum_{t_2+\cdots+t_p\equiv 2^{-1} \pmod q}\left(\frac{2^{-1}t_2\cdots t_p}{q}\right)$. But there are p such sets of terms where each of the p different t_i satisfies $t_i \equiv 2^{-1} \pmod q$. Thus, we can group these terms together to get $p\sum_{t_2+\cdots+t_p\equiv 2^{-1} \pmod q}\left(\frac{2^{-1}t_2\cdots t_p}{q}\right) \equiv 0 \pmod p$. The only time we do not get such symmetry is when all the t_i are equal: $t_1 \equiv t_2 \equiv \cdots \equiv t_p \equiv p^{-1} \pmod q$.

Thus, we have

$$\begin{aligned} N_p &\equiv 1 + \left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right)\left(\frac{p^{-p}}{q}\right) \pmod p \\ &\equiv 1 + (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right) \pmod p. \end{aligned} \tag{14}$$

The last equality relies on the observation that p is a square modulo q if and only if p^{-p} is a square modulo q (Theoretical Exercise 3.17). The reciprocity law follows by comparing the two equations (13) and (14). □

The multiplicativity of the Legendre symbol and the Law of Quadratic Reciprocity combine to give a very efficient method of determining whether a is a quadratic residue or nonresidue modulo a prime. In particular, given a quadratic congruence

$$x^2 \equiv a \pmod p,$$

the Legendre symbol and the Law of Quadratic Reciprocity give an efficient way of determining whether there is a solution. The algorithm is similar to the Euclidean algorithm, as demonstrated in Example 3.17.

Example 3.17. We first use multiplicativity to reduce to the case of primes:

$$\left(\frac{124}{17}\right) = \left(\frac{2^2 31}{17}\right) = \left(\frac{2}{17}\right)^2 \left(\frac{31}{17}\right).$$

We can then simplify powers since $(-1)^n$ depends only on the parity of n. In other words, all Legendre symbols to even powers are just 1 and Legendre symbols to odd powers are the same as the Legendre symbol to the first power. So we have

$$\left(\frac{2}{17}\right)^2 \left(\frac{31}{17}\right) = \left(\frac{31}{17}\right).$$

Next we can use the fact that if $a \equiv b \pmod{p}$, we have

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

to get

$$\left(\frac{31}{17}\right) = \left(\frac{14}{17}\right).$$

Now we again factor

$$\left(\frac{14}{17}\right) = \left(\frac{2 \cdot 7}{17}\right) = \left(\frac{2}{17}\right)\left(\frac{7}{17}\right).$$

We compute $\left(\frac{2}{17}\right)$ by looking the residue class of 17 modulo 8 (Theorem 3.13), which is 1, so that 2 is a quadratic residue modulo 17 and

$$\left(\frac{2}{17}\right)\left(\frac{7}{17}\right) = \left(\frac{7}{17}\right).$$

Since we are down to the case of two odd primes, we apply quadratic reciprocity (Theorem 3.14) to flip the Legendre symbol:

$$\left(\frac{7}{17}\right) = (-1)^{\frac{7-1}{2}\frac{17-1}{2}} \left(\frac{17}{7}\right) = -\left(\frac{17}{7}\right).$$

We again take a different representative in the residue class:

$$-\left(\frac{17}{7}\right) = -\left(\frac{3}{7}\right).$$

Now we again apply quadratic reciprocity to flip the Legendre symbol:

$$-\left(\frac{3}{7}\right) = -(-1)^{\frac{3-1}{2}\frac{7-1}{2}} \left(\frac{7}{3}\right) = -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

Each time we flip the Legendre symbol, we are taking the remainder after division and reducing the size of the numbers we are working with, similar to the Euclidean algorithm.

This example may have seemed long, but in practice this is quite fast. For large numbers, the hardest step is the factoring step, which is a very difficult problem for large numbers.

1.3. Jacobi Symbol.

Now we turn our attention to composite moduli.

Question 3.18. When does $x^2 \equiv a \pmod{n}$ have solutions when n is composite?

Investigation 3.19. As a first step toward Question 3.18, see if you can generalize the Legendre symbol to a composite modulus.

(a) Choose a composite modulus $n = pq$ which is a product of two primes.

(b) Determine which residue classes are quadratic residues and nonresidues modulo n.

(c) Determine whether each residue class is a quadratic residue modulo each prime p and q.

(d) Does this give you any ideas as to how you might generalize the Legendre symbol?

We follow Jacobi[3] and define a generalization of the Legendre symbol.

Definition 3.20. Let n be a positive integer, and factor n into a product of distinct prime numbers as $n = p_1^{e_1} \cdots p_r^{e_r}$, where the e_i are positive integers. We can define the *Jacobi symbol* for an integer a relatively prime to n as

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \cdots \left(\frac{a}{p_r}\right)^{e_r}.$$

But be careful; $\left(\frac{a}{n}\right) = -1$ only if a is a quadratic nonresidue, but it is also possible that $\left(\frac{a}{n}\right) = 1$ when a is a quadratic nonresidue.

Example 3.21. Recall that 2 is a quadratic nonresidue for both 3 and 5. Then we have

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1,$$

but 2 is a quadratic nonresidue modulo 15.

Theorem 3.22. *Let a, b, and n be integers with $n > 0$. If $\gcd(ab, n) = 1$, we have the following properties for the Jacobi symbol:*

(a) *If $a \equiv b \pmod{n}$, then $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.*

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

(c) $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$.

(d) $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$.

(e) *If $\gcd(n, m) = 1$, then*

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}.$$

We leave the proof as Theoretical Exercise 3.20.

[3] Carl Gustav Jacob Jacobi (1804–1851) was a German mathematician.

2. Computing mth Roots Modulo n

We next turn to the question of higher degree equations.

Question 3.23. When can we solve the congruence

$$x^m \equiv a \pmod{n}?$$

How many solutions does it have?

Definition 3.24. Let n and m be positive integers. We say that an integer a relatively prime to n is an *mth power residue modulo n* if the equation

$$x^m \equiv a \pmod{n}$$

has a solution.

Example 3.25. We generate a few examples to see the different behavior.

- $x^3 \equiv 3 \pmod{7}$ has no solutions.
- $x^3 \equiv 1 \pmod{7}$ has three solutions.
- $x^4 \equiv 9 \pmod{12}$ has two solutions.
- $x^4 \equiv 1 \pmod{12}$ has four solutions.
- $x^5 \equiv 0 \pmod{16}$ has eight solutions.

The key points to notice from these few examples are that it is possible to have no solutions and it is possible to have less than, equal to, or more than m solutions for $x^m \equiv a \pmod{n}$. That is quite a wide range of behaviors.

To answer Question 3.23, we need the notions of multiplicative order and primitive roots.

Definition 3.26. Let n be a positive integer. We say that an integer a has (*multiplicative*) *order d* modulo n if

$$a^d \equiv 1 \pmod{n}$$

and

$$a^t \not\equiv 1 \pmod{n} \quad \text{for all } 0 < t < d.$$

Recall from Euler's formula (Theorem 2.31) that for any (positive) modulus n, every integer a with $\gcd(a, n) = 1$ has multiplicative order dividing $\varphi(n)$. Just knowing that the order divides $\varphi(n)$ is not very specific; it could be as large as $\varphi(n)$ and as small as 1. We know that $a = 1$ always has multiplicative order 1, so the smallest order is possible. What about large orders?

Question 3.27. For each positive integer n, is there an a whose multiplicative order modulo n is $\varphi(n)$?

Investigation 3.28. Choose a positive integer n.

(a) Compute the multiplicative order for all residue classes relatively prime to n. Try several different values of n.

(b) Can you say anything about the resulting set of multiplicative orders and/or answer Question 3.27?

Example 3.29. We compute a few orders modulo 36 for $\gcd(a, 36) = 1$. Note that $\varphi(36) = 12$.

a	order
5	6
7	6
11	6
13	3
17	2
19	2
23	6
25	3
29	6
31	6
35	2

All have order dividing 12, but their orders are all less than 12.

So the answer to Question 3.27 is no. However, the next example shows that it is possible to have order $\varphi(n)$.

Example 3.30. We compute orders modulo 18 for $\gcd(a, n) = 1$. Note that $\varphi(18) = 6$.

a	order
5	6
7	3
11	6
13	3
17	2

They all have order dividing 6, and both 5 and 11 have order 6.

We modify question Question 3.27 to reflect our new information.

Question 3.31. For which positive integers n is there an a whose multiplicative order modulo n is $\varphi(n)$?

Definition 3.32. We say that a is a *primitive root modulo* n if $\varphi(n)$ is the order of a modulo n.

Investigation 3.33.

(a) Find some positive integers n that have a primitive root.

(b) Can you find a restriction on n that guarantees it has a primitive root?

It is interesting to note that $\varphi(n)$ is the number of positive integers less than n and relatively prime to n. An integer a having multiplicative order $\varphi(n)$ means that the $\varphi(n)$ powers $\{a, a^2, a^3, \ldots, a^{\varphi(n)}\}$ are all distinct. Since $\gcd(a, n) = 1$, each of the powers a^m, $1 \leq m \leq \varphi(n)$ is relatively prime to n. So the set of residue classes relatively prime to n is the same as the set of powers of a, i.e., the set $\{a, a^2, a^3, \ldots, a^{\varphi(n)}\}$ is exactly the set of residue classes modulo n that are relatively prime to n. In particular, every integer relatively prime to the modulus can be written as a power of a primitive root.

Example 3.34. From Example 3.30 we see that 5 and 11 are both primitive roots modulo 18. In particular, we generate all the residue classes relatively prime to 18 as

$$\{5, 5^2, 5^3, 5^4, 5^5, 5^6\} \equiv \{5, 7, 17, 13, 11, 1\} \pmod{18}.$$

Proposition 3.35. *Let n be a positive integer. If n has a primitive root g, then for any integer a with $\gcd(a, n) = 1$ there exists an integer k such that*

$$g^k \equiv a \pmod{n}.$$

Proof. Assume that g is a primitive root of n and that $\gcd(a, n) = 1$. The elements of the set $\{g, g^2, \ldots, g^{\varphi(n)}\}$ are all distinct since a primitive root g has multiplicative order $\varphi(n)$. Also, for any k

$$g^k g^{\varphi(n)-k} \equiv 1 \pmod{n},$$

so each number in the set $\{g, g^2, \ldots, g^{\varphi(n)}\}$ has an inverse modulo n. By Theorem 2.19, there are $\varphi(n)$ residue classes that have inverses modulo n. Thus, $\{g, g^2, \ldots, g^{\varphi(n)}\}$ are all the residue classes that have inverses. Since a is relatively prime to n, it has an inverse (Theorem 2.19) and, thus, $a \in \{g, g^2, \ldots, g^{\varphi(n)}\}$. □

For moduli with primitive roots, we now know we can write a (relatively prime to n) as a power of the primitive root and reduce Question 3.23 to a linear congruence of the exponents. We can then use Theorem 2.38 to solve the linear congruence.

Let's take a simple example involving square roots.

Example 3.36. Solve $x^2 \equiv 7 \pmod{18}$. We know from Example 3.30 that 5 is a primitive root modulo 18, so every residue class relatively prime to 18 can be written as a power of 5:

$$\begin{aligned}
5^1 &\equiv 5 \pmod{18}\,,\\
5^2 &\equiv 7 \pmod{18}\,,\\
5^3 &\equiv 17 \pmod{18}\,,\\
5^4 &\equiv 13 \pmod{18}\,,\\
5^5 &\equiv 11 \pmod{18}\,,\\
5^6 &\equiv 1 \pmod{18}\,.
\end{aligned}$$

Then we can replace the variable x by 5^y for some new variable y to have the equation

$$5^{2y} \equiv 7 \pmod{18}\,.$$

We can also replace 7 by the power 5^2 to have the equation

$$5^{2y} \equiv 5^2 \pmod{18}\,. \tag{15}$$

Since 5 is a primitive root, it has order $\varphi(18) = 6$, which means that for any integer m,

$$5^m \equiv 5^{m+6} \equiv 5^{m+12} \equiv \cdots \pmod{18}\,.$$

So we compare exponents in equation (15) modulo $\varphi(18) = 6$ to get the linear equation

$$2y \equiv 2 \pmod{6}\,.$$

It is now easy to see that $y = 1$ is a solution, which is

$$x \equiv 5^y \equiv 5^1 \equiv 5 \pmod{18}\,.$$

We now give the general solution for mth power residues.

Theorem 3.37. *Let n and m be positive integers, and let a be an integer. If n has a primitive root and $\gcd(a, n) = 1$, then a is an mth power residue if and only if $a^{\varphi(n)/d} \equiv 1 \pmod{n}$ for $d = \gcd(m, \varphi(n))$. If there is an mth power residue, then there are d of them.*

Proof. Let g be a primitive root modulo n and $a = g^b$ and $x = g^y$ for some integers b and y. Then the congruence

$$x^m \equiv a \pmod{n}$$

is equivalent to

$$g^{my} \equiv g^k \pmod{n}\,,$$

which is in turn equivalent to

$$my \equiv k \pmod{\varphi(n)}\,.$$

The last equation is solvable if and only if $\gcd(m, \varphi(n)) = d \mid k$, and if there is one solution, then there are exactly d solutions (Theorem 2.38).

We now need to show that $d \mid k$ is equivalent to $a^{\varphi(n)/d} \equiv 1 \pmod{n}$.

If $d \mid k$, then

$$a^{\varphi(n)/d} \equiv g^{k\varphi(n)/d} \equiv (g^{\varphi(n)})^{k/d} \equiv 1 \pmod{n}\,.$$

Conversely, if $a^{\varphi(n)/d} \equiv 1 \pmod{n}$, then

$$g^{k\varphi(n)/d} \equiv 1 \pmod{n},$$

which implies $\varphi(n)$ divides $\frac{k\varphi(n)}{d}$, which implies $d \mid k$. □

Remark. Notice that the condition for the existence of a solution does not require knowing the primitive root. So we can determine existence of a solution even if we cannot find the solution.

Example 3.38. Working modulo 14, we can try to solve

$$x^3 \equiv 11 \pmod{14}.$$

We compute $\varphi(n) = 14$ and

$$d = \gcd(m, \varphi(n)) = \gcd(3, 6) = 3.$$

We compute

$$11^{\varphi(n)/d} \equiv 11^2 \equiv 9 \pmod{14},$$

and we see that there is no solution. We can explicitly compute all the third powers modulo 14 to check.

a	$a^3 \pmod{14}$
1	$1^3 \equiv 1$
3	$3^3 \equiv 13$
5	$5^3 \equiv 13$
9	$9^3 \equiv 1$
11	$11^3 \equiv 1$
13	$13^3 \equiv 13$

Now consider $a = 13$,

$$x^3 \equiv 13 \pmod{14}.$$

We compute

$$a^{\varphi(n)/d} \equiv 13^2 \equiv 1 \pmod{14},$$

so we expect a solution, in fact, three solutions. Using the primitive root 3 and writing

$$x \equiv 3^y \pmod{14} \quad \text{and} \quad 13 \equiv 3^3 \pmod{14}$$

for some integer y, we have

$$3^{3y} \equiv 3^3 \pmod{14}.$$

The resulting linear equation is

$$3y \equiv 3 \pmod{6},$$

and we may choose $y = 1$ to get $x = 3$ as a solution. From Theorem 2.38, the other two solutions are $y = 3$ and $y = 5$, which correspond to $x = 13$ and $x = 5$, respectively. The table of third powers confirms these solutions.

We use Theorem 3.37 to construct Algorithm 3.1 for computing mth roots.

Algorithm 3.1. mth Roots

Input: positive integers m, n and an integer a such that $\gcd(a, n) = 1$
Output: an mth root of a modulo n
Algorithm:

```
1: Compute $\varphi(n)$.
2: Define $d = \gcd(m, \varphi(n))$.
3: Find positive integers $x, y$ such that $xm - y\varphi(n) = d$.
4: Compute $a^{x/d}$.
```

Investigation 3.39. The fraction x/d in the exponent of Algorithm 3.1 step (4) is worrisome since unless $d \mid x$, this is a fractional power!

(a) Apply Algorithm 3.1 to

$$x^3 \equiv 13 \pmod{14}.$$

Was there an issue with step (4)? Did you need to know a primitive root?

(b) Apply Algorithm 3.1 to

$$x^6 \equiv 6 \pmod{25}.$$

Was there an issue with step (4)? How is this issue resolved by knowing a primitive root?

In the special case $d = 1$, we do not have to worry about the possible divisibility for the exponent in step (3) and, hence, do not need to know primitive roots, and we can use Algorithm 3.1 without concern.

3. Existence of Primitive Roots

We now return to Question 3.31 about the existence of primitive roots. In particular, we are looking for positive integers n for which there is a residue class a whose multiplicative order is $\varphi(n)$. We know that it is possible for primitive roots to exist, and we know there are moduli that do not have primitive roots.

Example 3.40.

- 2 and 3 both have multiplicative order 4 modulo 5, so they are primitive roots.
- There is no primitive root modulo 15.

Investigation 3.41. See if you can conjecture the correct statement for which moduli n have primitive roots.

(a) First consider $n = p$ a prime.

(b) Consider $n = p^k$ with $k > 1$, a power of a single prime.

(c) Consider $n = pq$ the product of two distinct primes.

We start with two lemmas that we will need later in this section.

Lemma 3.42. *Let n be a positive integer, and let a and b be integers relatively prime to n. If the multiplicative order of a modulo n is x and the multiplicative order of b modulo n is y with $\gcd(x, y) = 1$, then the multiplicative order of ab modulo n is xy.*

Proof. Let r be the multiplicative order of ab modulo n, that is, $(ab)^r \equiv 1 \pmod{n}$. We will show that $r = xy$ by seeing that $r \mid xy$ and $xy \mid r$.

First we compute

$$(ab)^{xy} \equiv a^{xy}b^{xy} \equiv (a^x)^y(b^y)^x \equiv 1 \cdot 1 \equiv 1 \pmod{n}.$$

So we must have $xy \mid r$.

For the other direction, consider the following two computations:

$$\begin{aligned} a^{ry} &\equiv a^{ry} \cdot 1 \equiv a^{ry}(b^y)^r \equiv (ab)^{ry} \equiv 1 \pmod{n}, \\ b^{rx} &\equiv b^{rx} \cdot 1 \equiv b^{rx}(a^x)^r \equiv (ab)^{rx} \equiv 1 \pmod{n}. \end{aligned}$$

So $x \mid ry$ and $y \mid rx$. Since $\gcd(x, y) = 1$, these become $x \mid r$ and $y \mid r$. Written as congruences, we have

$$\begin{aligned} r &\equiv 0 \pmod{x}, \\ r &\equiv 0 \pmod{y} \end{aligned}$$

with $\gcd(x, y) = 1$. We can apply the Chinese Remainder Theorem (Theorem 2.44) to see that

$$r \equiv 0 \pmod{xy}.$$

This congruence is the same as $xy \mid r$. □

Example 3.43. We illustrate Lemma 3.42 with an example. Consider $n = 7$. Then for $a = 2$,

$$\begin{aligned} a &\equiv 2 \pmod{7}, \\ a^2 &\equiv 4 \pmod{7}, \\ a^3 &\equiv 8 \equiv 1 \pmod{7} \end{aligned}$$

so that the multiplicative order of a is 3. For $b = 6$ we have

$$\begin{aligned} b &\equiv 6 \pmod{7}, \\ b^2 &\equiv 36 \equiv 1 \pmod{7} \end{aligned}$$

so that the multiplicative order of b is 2. Then $2 \cdot 6 \equiv 12 \equiv 5 \pmod{7}$, which has multiplicative order $6 = 2 \cdot 3$. We check this as

$$\begin{aligned} 5 &\equiv 5 \pmod{7}, \\ 5^2 &\equiv 25 \equiv 4 \pmod{7}, \\ 5^3 &\equiv 20 \equiv 6 \pmod{7}, \\ 5^4 &\equiv 30 \equiv 2 \pmod{7}, \\ 5^5 &\equiv 10 \equiv 3 \pmod{7}, \\ 5^6 &\equiv 15 \equiv 1 \pmod{7}. \end{aligned}$$

Our next lemma relates the primitive roots modulo n to the primitive roots modulo $2n$.

Lemma 3.44. *Let n be an odd positive integer. There is a primitive root modulo n if and only if there is a primitive root modulo $2n$.*

Proof. First observe that for an odd number n, $\varphi(2n) = \varphi(n)$. Next note that a primitive root g (if it exists) modulo $2n$ must be odd, and so for any positive integer k

$$g^k \equiv 1 \pmod{2}.$$

Since $\gcd(2, n) = 1$, the Chinese Remainder Theorem (Theorem 2.44) says that the system of equations

$$\begin{aligned} g^k &\equiv 1 \pmod{2}, \\ g^k &\equiv 1 \pmod{n} \end{aligned}$$

is equivalent to

$$g^k \equiv 1 \pmod{2n}.$$

In particular, since k is the smallest power such that $g^k \equiv 1 \pmod{2n}$, then k is the smallest power such that $g^k \equiv 1 \pmod{n}$, so that g is also a primitive root modulo n.

Now assume we have a primitive root g modulo n. If g is even, since n is odd, the element $g + p$ is odd and is also a primitive root since it is in the same residue class as g. With g odd, we can apply the above argument in reverse to see that g is also a primitive root modulo $2n$. □

Example 3.45. Let $n = 11$, then the primitive roots are $\{2, 6, 7, 8\}$. For $2n$ the primitive roots are $\{7, 13, 17, 19\}$. The proof of Lemma 3.44 says that we have a correspondence between these sets of primitive roots. In particular, given a primitive root g modulo 11, then g or $g+11$ is a primitive root modulo 22. We see the following correspondence:

$$\begin{aligned} &2 \mapsto 2 + 11 = 13, \\ &6 \mapsto 6 + 11 = 17, \\ &7 \mapsto 7, \\ &8 \mapsto 8 + 11 = 19. \end{aligned}$$

The last ingredient we need in order to determine which moduli have primitive roots is a statement about roots of unity modulo primes.

Definition 3.46. We say that x is an *nth root of unity* if $x^n = 1$. Equivalently, x is an nth root of unity modulo n if $x^n \equiv 1 \pmod{n}$.

Example 3.47. The only roots of unity which are integers are 1 and -1

Roots of unity will be discussed in more detail in Chapter 5, section 2, as an application of the Möbius function.

Lemma 3.48. *Let p be a prime number. If $d \mid p-1$, then*

$$x^d \equiv 1 \pmod{p}$$

has exactly d solutions.

Proof. Write $p-1=md$ for some integer m, and let

$$f(x)=1+x^d+(x^d)^2+\cdots+(x^d)^{m-1}.$$

Then we have

$$x^{p-1}-1=(x^d-1)f(x),$$

and so

$$x^{p-1}-1\equiv(x^d-1)f(x)\pmod{p}.$$

Fermat's Little Theorem (Theorem 2.21) says that the left-hand side is zero for exactly $p-1=md$ distinct x values. Since p is prime, each such x value must be a zero of either (x^d-1) or $f(x)$. Each is a polynomial and of degree d and $dm-d$, respectively. Lagrange's Theorem (Theoretical Exercise 3.27) says that a polynomial of degree d can have at most d roots modulo a prime. So we must have that x^d-1 has exactly d 0's modulo p, since to have fewer would contradict that the total number must be $p-1$. □

Investigation 3.49. Lemma 3.48 assumes the modulus is prime. However, there still exist roots of unity for composite moduli.

(a) What is the appropriate generalization of the condition $d \mid p-1$ for a composite modulus?

(b) Are there the "correct" number of roots of unity?

(c) Conjecture a generalization of Lemma 3.48 for composite moduli.

First we prove the existence of primitive roots for powers of odd primes.

Proposition 3.50. *If p is an odd prime, then there is a primitive root modulo p^k for all integers $k\geq 1$.*

Proof. We first consider $k=1$. Let q be a prime that divides $p-1$. Let $m\geq 1$ be the maximal power so that $q^m \mid (p-1)$. An element of order q^m is a solution to

$$a^{q^m}\equiv 1\pmod{p},$$

and by Lemma 3.48 there are exactly q^m of them. Each such a has multiplicative order dividing q^m. If the order is less than m, then a is also a solution to

$$a^{q^j}\equiv 1 \mod p$$

for some $1\leq j<m$. There are exactly q^j such solutions for each j. Since

$$q^m>q^{m-1}+q^{m-2}+\cdots+q+1,$$

there is at least one a that has multiplicative order q^m modulo p, call it a_q. We can do this for each prime divisor q of $p-1$. Since each prime is distinct by Lemma 3.42, the product

$$\prod_{\substack{q\mid(p-1)\\ \text{distinct}}} a_q$$

has multiplicative order

$$\prod_{\substack{q\mid(p-1)\\ \text{distinct}}} q^m=p-1.$$

Now we need to consider powers p^k for $k \geq 2$. Assume that g is a primitive root modulo p. We will show that g or $g+p$ is a primitive root modulo p^k.

We proceed by induction: $k=1$ is true since g is a primitive root modulo p, so assume that $g^{\varphi(p^k)} \equiv 1 \pmod{p^k}$. Let m be the multiplicative order of g modulo p^{k+1}, so by Euler's formula (Theorem 2.31) we must have $m \mid \varphi(p^{k+1}) = p^k(p-1)$. We then have two possibilities $m = \varphi(p^{k+1})$ and we are done, or $m = \varphi(p^k)$ and we are not done. We break the proof into two cases. First assume that

$$g^{p-1} \not\equiv 1 \pmod{p^2}.$$

Then, we can show by induction (Theoretical Exercise 3.28) that

$$g^{\varphi(p^k)} \not\equiv 1 \pmod{p^{k+1}}.$$

Consequently, $m = \varphi(p^{k+1})$.

Now assume

$$g^{p-1} \equiv 1 \pmod{p^2}.$$

Consider $g+p$, which is in the same residue class as g modulo p, so it is still a primitive root modulo p. We compute

$$(g+p)^{p-1} \equiv g^{p-1} + (p-1)pg^{p-2} \not\equiv 1 \pmod{p^2}.$$

In particular, the multiplicative order of $(g+p)$ must be $\varphi(p^{k+1})$. □

Notice that the proof is not constructive in the sense that given a prime p, it does not produce a primitive root. We are reduced to trying every possible residue class to find a primitive root. However, given a prime power p^k, if we can find a primitive root g modulo p, then at least one of g or $g+p$ is primitive root modulo p^k for each $k \geq 2$. (See also Theoretical Exercise 3.28.)

Example 3.51.

- We compute that 6 is a primitive root modulo 13. Checking the condition in the proof, we see that $6^{12} \equiv 144 \not\equiv 1 \pmod{13^2}$, and we can check that 6 is a primitive root modulo 13^k for all $k \geq 1$.
- For $p = 37$ we have 18 as a primitive root. This primitive root satisfies $18^{36} \equiv 1 \pmod{37^2}$, so that 18 is not a primitive root modulo 37^k for $k \geq 2$, but that $18 + 37 = 55$ is a primitive root modulo 37^k for $k \geq 2$.

We can now bring all our work in this section together to state exactly which moduli have a primitive root.

Theorem 3.52 (Primitive root theorem). *A positive integer n has a primitive root if and only if $n = 2, 4, p^k$, or $2p^k$ for an odd prime p and a positive integer k.*

Proof. For $n = 2$ or 4 we can simply observe that 1 is a primitive root modulo 2 and 3 is a primitive root modulo 4. For $n = 2^3 = 8$ there are no primitive roots. Now we proceed by induction on the power 2^k for $k \geq 3$ to show there are no primitive roots by showing that every odd integer has multiplicative order dividing $2^{k-2} < \varphi(2^k) = 2^{k-1}$. For the base case $k = 3$, we check that every odd residue class modulo 8 has multiplicative order dividing 2. For the induction assumption, we assume that every odd residue class modulo 2^k has multiplicative order dividing 2^{k-2}. In particular, for each odd a,

$$a^{2^{k-2}} = 1 + m2^k$$

for some integer m. Squaring both sides, we see that

$$a^{2^{k-1}} = 1 + m2^{k+1} + m^2 2^{2k} \equiv 1 \pmod{2^{k+1}}.$$

This shows that any odd integer a has multiplicative order modulo $2^{k-1} < 2^k$ so is not a primitive root. Then, by induction, $n = 2^k$ for $k \geq 3$ does not have a primitive root.

Proposition 3.50 states that powers of odd primes have primitive roots, so we are left to consider the case where n is divisible by two distinct odd primes. In this case we can write $n = mp^k$ for an odd prime p and an integer $m \geq 3$ with $\gcd(m, p) = 1$. The Euler totient function is multiplicative (Lemma 5.7), so we compute

$$\varphi(n) = \varphi(m)\varphi(p^k),$$

where both $\varphi(m)$ and $\varphi(p^k)$ are even. In particular by Euler's formula (Theorem 2.31) we have the following two congruences for any a relatively prime to n:

$$a^{\varphi(n)/2} \equiv (a^{\varphi(m)})^{\varphi(p^k)/2} \equiv 1 \pmod{m},$$
$$a^{\varphi(n)/2} \equiv (a^{\varphi(p^k)})^{\varphi(m)/2} \equiv 1 \pmod{p^k}.$$

By the Chinese remainder theorem (Theorem 2.44), these congruences imply that

$$a^{\varphi(n)/2} \equiv 1 \pmod{n},$$

and, thus, a is not a primitive root. □

COMPUTATIONAL EXERCISES

3.1. Find all the residue classes which are quadratic residues modulo 61.

3.2. Find all the primes $p < 1000$ for which 17 is a quadratic residue.

✍ **3.3.** Compute the following Legendre symbols.

a. $\left(\frac{328}{13}\right)$

b. $\left(\frac{420}{17}\right)$

✍ **3.4.** Compute the following Jacobi symbols $\left(\frac{a}{n}\right)$. Determine whether a is quadratic residue or nonresidue modulo n.

a. $\left(\frac{42}{15}\right)$

b. $\left(\frac{117}{35}\right)$

3.5. Determine all the quadratic residues modulo 1624.

✍ **3.6.** Find all solutions to

$$x^2 \equiv 1 \pmod{35}.$$

3.7. We say that the set of points $(x_1, \ldots, x_n)$ satisfying

$$x_1^2 + \cdots + x_n^2 = 1$$

is a hypersphere of dimension n and radius 1. Count the number of points on the hypersphere modulo p for $n = 1, 2, 3, 4$ and $p = 3, 5, 7, 11$.

3.8. Count 8th roots of unity.

a. Find all the solutions to $x^8 \equiv 1 \pmod{31}$.

b. Find all the primes p less than 100 for which the equation

$$x^8 \equiv 1 \pmod{p}$$

has eight solutions.

✍ **3.9.** Assume that 5 is a primitive root modulo 23. Find all solutions to

$$x^4 \equiv 2 \pmod{23}.$$

3.10. Find all the solutions to $x^{12} \equiv 87 \pmod{101}$.

3.11. Determine the mth power residues modulo 11 for $m = 2, 3, 4, 5, 6$. In other words, determine all the a such that $x^m \equiv a \pmod{11}$.

✍ **3.12.** Determine the list of moduli n with $2 \le n \le 30$ that do not have a primitive root.

3.13. Determine all the primitive roots modulo 38.

✍ **3.14.** Determine a primitive root modulo 5^{10}.

THEORETICAL EXERCISES

3.15. Let $p > 2$ be a prime. Prove that $\left(\frac{-1}{p}\right) = 1$ if and only if $p \equiv 1 \pmod{4}$.

3.16. Prove that 7 is a quadratic residue modulo a prime $p > 2$ if and only if $p \equiv \pm 1$, ± 3, or $\pm 9 \pmod{28}$.

3.17. For distinct odd primes p and q, prove that p is a quadratic residue modulo q if and only if p^{-p} is a quadratic residue modulo q.

3.18.

a. Let $p > 2$ be a prime. Prove that $\left(\frac{3}{p}\right) = 1$ if and only if $p \equiv 1 \pmod{3}$.

b. Prove that $\left(\frac{-3}{p}\right) = 1$ if and only if $p \equiv 1 \pmod{3}$. *Hint*: Let g be a primitive root for p, and consider the solutions to

$$x^3 - 1 \equiv (x-1)(x^2 + x + 1) \equiv 0 \pmod{p}$$

in terms of g.

Conclude that $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$.

3.19.

a. Let $n = pq$ for distinct odd primes p and q. Prove that a is a quadratic residue modulo n if and only if a is a quadratic residue modulo both p and q. Conclude that the number of quadratic residues modulo n is $\frac{(p-1)(q-1)}{4}$.

b. Let $n = \prod_{i=1}^{m} p_i$ be a product of distinct odd primes. Prove that a is a quadratic residue modulo n if and only if it is a quadratic residue modulo each p_i, $1 \leq i \leq m$.

3.20. Prove Theorem 3.22. Let n and m be a positive integers. Let a and b be integers with $\gcd(ab, n) = 1$.

a. If $a \equiv b \pmod{n}$, then $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.

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

c. $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$.

d. $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$.

e. If $\gcd(n, m) = 1$, then

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}.$$

3.21. Let n and m be positive integers. Let x and a be integers such that

$$x^m \equiv a \pmod{n}.$$

Prove that $\gcd(x, n) = 1$ if and only if $\gcd(a, n) = 1$.

3.22. Let n be a positive integer. We define the *Carmichael function* $\lambda(n)$ as the smallest positive integer such that

$$a^{\lambda(n)} \equiv 1 \pmod{n}$$

for all a with $\gcd(a, n) = 1$.

Prove that n has a primitive root if and only if $\lambda(n) = \varphi(n)$.

3.23. Use primitive roots to prove Euler's criterion (Theorem 3.10).

3.24. Let n be a positive integer. Prove that if there is one, then there are $\varphi(\varphi(n))$ primitive roots modulo n.

3.25. Prove that for a prime p and a positive integer n, if g is a primitive root modulo p^n, then g is a primitive root modulo p.

3.26. Let n be a positive integer that has a primitive root g. Prove that g^m is a primitive root modulo n if and only if m is relatively prime to $\varphi(n)$.

3.27. Lagrange's Theorem: Let p be a prime. Let $f(x)$ be a polynomial of degree d with integer coefficients and with at least one coefficient not divisible by p. Prove that

$$f(x) \equiv 0 \pmod{p}$$

has at most d solutions. *Hint*: Try using induction on the degree of f.

3.28. Let p be an odd prime with primitive root g. Prove that if $g^{p-1} \not\equiv 1 \pmod{p^2}$, then $g^{\varphi(p^k)} \not\equiv 1 \pmod{p^{k+1}}$ for all $k \geq 1$.

EXPLORATION EXERCISES

3.29 (Quadratic residues)**.** Consider the following inverse problem for quadratic residues. Given a nonsquare integer a, determine the set of moduli n such that a is a quadratic residue modulo n.

a. Assume that $p = 2^k$ for a positive integer k.

b. Assume that p is an odd prime power.

c. Assume that $n = pq$ is the product of distinct primes.

d. Consider any n.

3.30 (Higher order reciprocity)**.**

a. Cubic reciprocity: $x^3 \equiv a \pmod{p}$.
1. Define an equivalent of the Legendre symbol. Can you find a criterion like Euler's criterion (Theorem 3.10)?
2. State a version of cubic reciprocity (Theorem 3.13 and Theorem 3.14).
3. What about cubic Jacobi symbols?

b. Higher order reciprocities: $x^n \equiv a \pmod{p}$ for $n > 3$. Consider the same questions as for cubic reciprocity.

3.31 (Roots of unity modulo n)**.** We say that a is an *mth root of unity modulo n* if

$$a^m \equiv 1 \pmod{n}.$$

We will be counting roots of unity modulo various n, so define $C(m, n)$ to be the number of mth roots of unity modulo n. In particular, we are counting the number of solutions to

$$x^m - 1 \equiv 0 \pmod{n}.$$

a. Consider the values $C(\lambda(n), n)$, where $\lambda(n)$ is the Carmichael function (see Theoretical Exercise 3.22).

b. Given positive integers k, m, n with $m \mid n$, what can you say about $C(k, m)$ and $C(k, n)$?

c. Given positive integers k, m, n, what can you say about $C(k, mn)$?

d. Given positive integers k, m, n, what can you say about $C(km, n)$ in terms of $C(k, n)$ and $C(m, n)$? Perhaps consider first the case where $\gcd(k, m) = 1$.

e. Let n be a positive integer, and let p be a prime. What can you say about $C(p^k, n)$ for $k \geq 1$?

If m is the smallest positive integer such that $a^k \equiv 1 \pmod{n}$, we say that a is a *primitive mth root of unity.*

f. Can you say anything about the number of primitive mth roots modulo n?

g. For which integers m are there primitive mth roots of unity modulo a prime p?

h. For which integers m are there primitive mth roots of unity modulo a composite n. What if you assume there are primitive roots modulo n? What if there are not?

3.32 (mth roots)**.** Number of mth roots.

a. For prime moduli, half of all (nonzero) residue classes are squares. How many are cubes? Fourth powers? mth powers?

b. What about composite moduli?

c. How many solutions can $x^m \equiv a \pmod{p}$ have?

d. What about composite moduli?