2012

Quadratic and cubic reciprocity

Suzanne Rousseau
Eastern Washington University

QUADRATIC AND CUBIC RECIPROCITY

A Thesis

Presented To

Eastern Washington University

Cheney, Washington

In Partial Fulfillment of the Requirements

for the Degree

Master of Science

By

Suzanne Rousseau

Spring 2012

THESIS OF SUZANNE ROUSSEAU APPROVED BY

_____ DATE:_____

DR. DALE GARRAWAY, GRADUATE STUDY COMMITTEE

_____ DATE:_____

DR. RON GENTLE, GRADUATE STUDY COMMITTEE

_____ DATE:_____

LIZ PETERSON, GRADUATE STUDY COMMITTEE

MASTERS THESIS

In presenting this thesis in partial fulfillment of the requirements for a master's degree at Eastern Washington University, I agree that the JFK Library shall make copies freely available for inspection. I further agree that copying of this project in whole or in part is allowable only for scholarly purposes. It is understood, however, that any copying or publication of this thesis for commercial purposes, or for financial gain, shall not be allowed without my written permission.

Signature_____

Date_____

Abstract

In this thesis, we seek to prove results about quadratic and cubic reciprocity in great detail. Although these results appear in many textbooks, the proofs often contain large gaps that may be difficult for the average reader to follow. To achieve this goal, we have built up to reciprocity theory from basic principles of algebra, and whenever possible, we have tried to prove the number theoretic results of reciprocity using ideas from group theory. This thesis could potentially serve as a reference for a student who desires to study quadratic or cubic reciprocity in more detail, or as a foundation for studying higher reciprocity laws.

Acknowledgements

I would like to thank Dr. Yves Nievergelt for helping me to translate "Nachtrag zum kubischen Reciprocitätssatze" from German into English.

Contents

Chapter 1

Introduction

In mathematics, interesting topics seem to come from curious people asking themselves questions about how things relate to each other. Pierre de Fermat was interested in determining which prime numbers would divide numbers of the form $a^n - 1$, and that question eventually gave rise to Fermat's Little Theorem [7]. Leonhard Euler took Fermat's question one step further, and wondered which primes would divide numbers of the form $a^n + 1$. This led to extensive study of quadratic residues, which are defined to be integers a that satisfy the congruence $x^2 \equiv a \bmod p$, for some prime p. More specifically, Euler's question was if q is a quadratic residue of p, then do we know whether or not p is a quadratic residue of q [7], [10]? Euler answered his question in the mid-1700s, but did not prove that his answer was actually correct [10].

In 1785, Adrien-Marie Legendre took Euler's answer and rewrote it in

a theorem called the Law of Quadratic Reciprocity. Legendre tried repeatedly to prove this theorem, but was unable to come up with a proof that was completely correct. He published several proposed proofs, but each was flawed in some way [10]. Johann Carl Friedrich Gauss also discovered the Law of Quadratic Reciprocity, apparently independently, when he was 18 years old [10]. Gauss referred to this theorem publicly as the Fundamental Theorem, but in his private diary entries, he called it the Theorema Aureum, or the Golden Theorem [7], [8]. Gauss studied this topic for many years, and published six different proofs during his lifetime. After his death, two more proofs were found among his papers [7], [10]. He stated that his main reason for continuing to prove the same theorem in so many different ways, was to try to find a way to generalize it to higher powers. With his sixth proof, he was successful in that endeavor, and this search for higher reciprocity laws led to a lot of the results that comprise algebraic number theory today [7].

Each mathematician that worked on the Law of Quadratic Reciprocity used his own notation and stated the theorem slightly differently. Legendre developed what is known today as the Legendre symbol, to represent the statement "$x^2 \equiv a \mod p$", and then Euler went one step further and came up with Euler's Criterion, that gives a formula for evaluating the Legendre symbol [10]. Carl Gustav Jacob Jacobi defined a generalization of the Legendre symbol, called the Jacobi symbol, that offered yet another tool for the task of

determining whether or not quadratic congruences had solutions [18]. As of 2012, there are 240 known proofs of the Law of Quadratic Reciprocity, by a multitude of different people. A current list is kept online and maintained by Franz Lemmermeyer, a German mathematician [9].

Gauss noted in his first memoir that the theory of quadratic reciprocity was discovered easily, but that the theory of cubic and biquadratic residues is much more difficult [7]. He realized as he attempted to study these higher reciprocities that principles of arithmetic were insufficient to build up the general theory, and he further recognized that a theory of algebraic numbers was going to be required [7]. He initially begin working in the ring of Gaussian integers as the setting to prove results about cubic reciprocity, but noted in a footnote in one of his papers on biquadratic reciprocity in 1832 that cubic reciprocity is most easily handled in the ring of Eisenstein integers [14]. Jacobi formulated several theorems that dealt with cubic residues, but did not publish any proofs. He apparently presented some proofs in 1836 and 1837 in lectures in Königsberg, but the first proofs to be published were credited to Ferdinand Gotthold Max Eisenstein in 1844 [14].

The purpose of this thesis is to explore the theories of quadratic and cubic reciprocity, and to this end, we have built up to reciprocity theory from first principles of algebra. The reader who feels that he has a strong background in group theory and ring theory may want to skip the group theory

and ring theory chapters. However, because of the way we have built these ideas from the ground up, it might be helpful to begin with the basics chapter and proceed through the thesis in its entirety, as a review of many concepts that play important roles in reciprocity.

We have attempted to provide relevant examples to illustrate important concepts wherever possible, and in many cases have built upon early examples in later chapters, as a way to maintain a cohesive flow to this thesis. In some instances, theorems have been stated as propositions and offered without proof, but citations are given so that the reader may review particular proofs if desired.

Chapter 2

Basics

This chapter serves as a brief review of basic principles that will play key roles later on in this thesis. We first examine the division algorithm for the integers and define what it means for one number to divide another number. We recall the usual definition of a prime number and then review the Fundamental Theorem of Arithmetic. The definitions of least common multiple and greatest common divisor are given, and then we prove two lemmas about least common multiples that we will need later in this thesis. The fourth section in this chapter reviews relations and partitions and defines equivalence classes, least residues, and the idea of congruence modulo n. We conclude this chapter by examining the Binomial Expansion Theorem and looking at two examples that are similar to the way the theorem will be used later in this thesis.

2.1 Division Algorithm

Proposition 2.1.1 (The Division Algorithm) *Let a and n be integers with $n > 0$. Then there exist unique integers q and r such that*

$$a = nq + r, \text{ with } 0 \leqslant r < n.$$

Example 2.1.2 For $n = 3$ and $a_1 = 11$, the division algorithm indicates that $11 = 3 \cdot 3 + 2$, so $r_1 = 2$. Now let $a_2 = 12$ and $a_3 = 13$. We have $12 = 3 \cdot 4 + 0$ and $13 = 3 \cdot 4 + 1$, so $r_2 = 0$ and $r_3 = 1$. Recall that the division algorithm states that $0 \leqslant r < 3$. This constraint is independent of the choice of a, so there will always be a predictable set of remainders for a given n. In this example, we have the remainders $\{0, 1, 2\}$.

If we choose some $n \in \mathbb{N}$ and $a \in \mathbb{Z}$, then $a = nq + r$, by the division algorithm. Since $0 \leqslant r < n$, the remainders left on division of a by n form the set $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$, which is called the set of *least residues*. □

Definition 2.1.3 Let a and b be integers, with $a \neq 0$. The phrase a *divides* b means there exists $k \in \mathbb{Z}$ such that $ak = b$, and is denoted $a \mid b$. If such a k does not exist, we will say that a does not divide b and will denote it $a \nmid b$. ♢

Example 2.1.4 Since $3 \cdot 4 = 12$, $3 \mid 12$ and $4 \mid 12$, but $5 \nmid 12$, since $5k = 12$ implies that $k = 12/5$, and $12/5 \notin \mathbb{Z}$. □

2.2 Fundamental Theorem of Arithmetic

We will be giving a rigorous definition of a prime number in the ring theory chapter, but for now when we refer to prime numbers, they will be integers not equal to ± 1 whose only positive divisors are 1 and themselves. In other words, this is the definition that most of us are familiar with. So by this definition, 3 and -11 are prime, but 8 is not, since its positive divisors are 1, 2, 4, and 8.

Proposition 2.2.1 (Fundamental Theorem of Arithmetic) *Any integer not equal to* ± 1 *can be written as a unique product (up to ordering and multiplication by* ± 1*) of prime numbers.*

Example 2.2.2 We stated that 3 is prime, but it can be written as $3 = 3^1$, which is a trivial product of primes. 8 is a composite number, so it gives us a better example, as it can be written as $8 = 2 \cdot 2 \cdot 2 = 2^3$. □

Generally speaking, when we talk about giving the *prime factorization* of a number, we will use the notation $8 = 2 \cdot 2 \cdot 2$ or $a = p_1 p_2 \dots p_m$, where the p_i are not necessarily unique. If we refer to the *prime-power decomposition* of a number, the notation will be $8 = 2^3$ or $a = p_1^{a_1} p_2^{a_2} \dots p_m^{a_m}$, where the p_i are unique. Typically these factorizations or decompositions will be assumed to be in order from smallest prime to largest prime, when read from left to right.

2.3 LCM and GCD

Definition 2.3.1 The *least common multiple* of two nonzero integers a and b is the smallest positive integer that is divisible by both a and b. The least common multiple of integers a and b will be denoted by $\text{lcm}(a, b)$. $\diamondsuit$

Definition 2.3.2 Let $a, b \in \mathbb{Z}$. The *greatest common divisor* of a and b, denoted $\gcd(a, b)$, is d if and only if

1. $d \mid a$ and $d \mid b$, and

2. if $c \mid a$ and $c \mid b$, then $c \leqslant d$. $\diamondsuit$

Lemma 2.3.3 *Let $p_1, p_2, \ldots, p_m$ be distinct primes. Then the least common multiple of $p_1, p_2, \ldots, p_m$ is the product $p_1 p_2 \ldots p_m$.*

Proof: Let $a = p_1 p_2 \ldots p_m$ and suppose that b is a common multiple of $p_1, p_2, \ldots, p_m$ with $a \neq b$. Let $b = q_1 q_2 \ldots q_n$ be the prime factorization of b, where the p_i and q_j are distinct, positive primes.

Since b is a multiple of $p_1, p_2, \ldots, p_m$, clearly $p_1 \mid q_1 \ldots q_n$, which implies that there exists $k_1 \in \mathbb{Z}$ such that $p_1 k_1 = q_1 \ldots q_n$. Since each of the p_i and q_j are prime, p_1 divides at least one of the q_j. Without loss of generality, suppose $p_1 \mid q_1$. Then $p_1 l_1 = q_1$, for $l_1 \in \mathbb{Z}$. But p_1 and q_1 are prime, so $l_1 = 1$ and $p_1 = q_1$. Thus $k_1 = q_2 \ldots q_n$.

Similarly, $p_2 \mid q_2 \ldots q_n$, which implies that there exists $k_2 \in \mathbb{Z}$, such that $p_2 k_2 = q_2 \ldots q_n$. By the previous argument, p_2 divides at least one of the

remaining q_j. Without loss of generality, suppose $p_2 \mid q_2$. Then $p_2 l_2 = q_2$ for $l_2 \in \mathbb{Z}$, which implies that $l_2 = 1$ and $p_2 = q_2$. Thus $k_2 = q_3 \dots q_n$.

Repeat this argument until we have $p_m \mid q_m \dots q_n$. This implies that there is $k_m \in \mathbb{Z}$ such that $p_m k_m = q_m \dots q_n$. Again without loss of generality, suppose that the q_j that p_m divides is q_m. This will result in $p_m = q_m$, and $k_m = q_{m+1} \dots q_n$.

So now we have $a = p_1 \dots p_m$ and $b = p_1 \dots p_m k_m$. By assumption, $a \neq b$, so $k_m \neq 1$. Thus $a < b$, since k_m is the product of positive primes, and $a = p_1 \dots p_m$ is the least common multiple of $p_1, \dots, p_m$ as desired. ∎

Lemma 2.3.4 *Let a, b, and c be integers. Then*

$$\mathrm{lcm}(a, b) \mid c \text{ if and only if } a \mid c \text{ and } b \mid c.$$

Proof: Let $l = \mathrm{lcm}(a, b)$ and suppose $l \mid c$. Then since $a \mid l$, we have $a \mid c$. By a similar argument, $b \mid c$.

Now suppose that

$$a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n},$$

$$b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n},$$

$$c = p_1^{c_1} p_2^{c_2} \dots p_n^{c_n}$$

are the prime-power decompositions of a, b, and c, where each p_i is a unique prime, the p_i increase in size from smallest to largest, and some of the a_i, b_i, or c_i may be zero. Suppose $a \mid c$ and $b \mid c$. Then for each $i \in \{1, 2, \dots, n\}$,

$\max(a_i, b_i) \leqslant c_i$, where the max function takes the value of the largest of a set of numbers. Let $l = \prod_{i=1}^{n} p_i^{\max(a_i,b_i)}$. Then we have $l \mid c$ as desired. ∎

2.4 Relations and Partitions

Definition 2.4.1 A *relation* $\mathcal{R}$ on a set X is a subset of $X \times X$, and is denoted $\mathcal{R} \subseteq X \times X$. We say that x *is related to* y, denoted $x\mathcal{R}y$, if $(x, y) \in \mathcal{R}$. If $\mathcal{R}$ satisfies the following three properties for all $x, y, z \in X$, then $\mathcal{R}$ is called an *equivalence relation.*

1. **(Reflexivity)** $x\mathcal{R}x$.

2. **(Symmetry)** If $x\mathcal{R}y$, then $y\mathcal{R}x$.

3. **(Transitivity)** If $x\mathcal{R}y$ and $y\mathcal{R}z$, then $x\mathcal{R}z$. ♢

The following example establishes a relation on the integers that provides the structural framework of much of the remaining work done in this thesis.

Example 2.4.2 Let $n \in \mathbb{N}$. Then for $a, b \in \mathbb{Z}$, define a relation $\mathcal{R}$ as follows:

$$a\mathcal{R}b \text{ if and only if } n \mid (a - b).$$

We claim that the relation $\mathcal{R}$ is an equivalence relation.

Since $a - a = 0 = n \cdot 0$, we have $a\mathcal{R}a$, so $\mathcal{R}$ is reflexive.

Suppose $a\mathcal{R}b$. Then

$$
\begin{aligned}
& n \mid (a-b) && \text{(Definition of } \mathcal{R}\text{)} \\
\iff & a-b = nq, \text{ for some } q \in \mathbb{Z} && \text{(Definition of divides)} \\
\iff & -nq = b-a, \text{ for some } q \in \mathbb{Z} && \text{(Arithmetic)} \\
\iff & n(-q) = b-a, \text{ for some } q \in \mathbb{Z} && \text{(Commutative Property)} \\
\iff & n \mid (b-a) && \text{(Definition of divides)} \\
\iff & b\mathcal{R}a, && \text{(Definition of } \mathcal{R}\text{)}
\end{aligned}
$$

so $\mathcal{R}$ is symmetric.

Now suppose that $a\mathcal{R}b$ and $b\mathcal{R}c$. Then we have $a - b = nq_1$ and $b - c = nq_2$ for some $q_1, q_2 \in \mathbb{Z}$. Adding these equations together yields

$$(a-b) + (b-c) = nq_1 + nq_2 \iff a - c = n(q_1 + q_2).$$

Since $(q_1 + q_2) \in \mathbb{Z}$, we have shown that $n \mid (a-c)$ by definition of divides, so $a\mathcal{R}c$ and $\mathcal{R}$ is transitive.

It follows that $\mathcal{R}$ is an equivalence relation. □

Note that in the example above, it is implied that if $n \mid (b-a)$, then a and b leave the same remainder on division by n. This is clear if we write $a = nq_1 + r_1$ and $b = nq_2 + r_2$. Then $a - b = n(q_1 - q_2) + (r_1 - r_2)$, and it must be the case that $(r_1 - r_2) = 0$. So we could restate the relation as $a\mathcal{R}b$ if and only if the remainders of a and b are the same, or in other words, if and only if a and b have the same *least residue*.

Definition 2.4.3 A *partition* $\mathscr{P}$ of a set X consists of a potentially infinite family of nonempty subsets of X, $\mathscr{P} = \{A_1, A_2, \dots\}_{i \in I}$, for some index set I, such that

1. For all $i \in I$, $A_i \neq \varnothing$.
2. $\bigcup_{i \in I} A_i = X$.
3. For all $i \neq j$, $A_i \bigcap A_j = \varnothing$.

The subsets of $\mathscr{P}$ are called the *cells* of the partition, and for each $x \in X$, the cell containing x will be denoted by $\overline{x}$ or $[x]$. The two notations are equivalent and will be used interchangeably. In this setting, x is not unique, and a particular cell can be represented by any element in the cell. This definition is illustrated with a simple partition of the integers.

Example 2.4.4 Let $E = \{\dots, -2, 0, 2, \dots\}$ and $O = \{\dots, -3, -1, 1, 3, \dots\}$. Note that neither E nor O is empty, $E \bigcup O = \{\dots, -2, -1, 0, 1, 2, \dots\} = \mathbb{Z}$, and $E \bigcap O = \varnothing$, so all three properties are met. Thus $\mathscr{P} = \{E, O\}$ is a partition of $\mathbb{Z}$ by definition.

For any $a \in E$, we can refer to E as $\overline{a}$. Similarly, for any $b \in O$, we can refer to O as $\overline{b}$. For instance, we could choose $0 \in E$ as the representative, so $\overline{0} = E$. Likewise, if we select 1 to represent O, then $\overline{1} = O$. □

Proposition 2.4.5 (Equivalence Relations and Partitions) *Let S be a nonempty set.*

1. *If $\mathcal{T}$ is an equivalence relation on S, then there is an associated partition $\mathscr{P}_{\mathcal{T}}$ defined by the equivalence classes $\overline{a} = \{x \in S : x\mathcal{T}a\}$.*

2. *If $\mathscr{P}$ is a partition of S, then there is an associated equivalence relation $\mathcal{T}_{\mathscr{P}}$, where $a\mathcal{T}_{\mathscr{P}}b$ if and only if a and b are in the same cell of the partition.*

The proof of this proposition is omitted here, but can be found in [11].

Example 2.4.6 Each of the cells in a partition that arises from an equivalence relation is known as an *equivalence class*. Recall that if we divide an integer by a natural number n, the remainder is in the set $\{0, 1, \ldots, n-1\}$. For each $n \in \mathbb{N}$, we can partition $\mathbb{Z}$ into n cells according to the value of the remainder when an integer is divided by n. In Example 2.1.2, we saw that for $n = 3$, the remainders formed the set $\{0, 1, 2\}$, so $\mathbb{Z}$ was partitioned into three cells, $\overline{0}$, $\overline{1}$, and $\overline{2}$. These cells are called the *residue classes modulo n* in $\mathbb{Z}$ and the remainders are called the *least residues*. The equivalence relation that creates this partition of $\mathbb{Z}$ is called *congruence modulo n* and the set of least residues modulo n is $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$. This set is different from $\overline{\mathbb{Z}}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots \overline{n-1}\}$, which is the set of equivalence classes (or residue classes) of least residues. Note that it is not standard to make a distinction between $\mathbb{Z}_n$ and $\overline{\mathbb{Z}}_n$, but for the purpose of clarity in this thesis, we will consider them to be as shown above. However, in other references, $\mathbb{Z}_n$ is generally used to mean both the set of least residues and the set of equivalence classes of least residues.

The statement a *is congruent to* b *modulo* n is denoted $a \equiv b \bmod n$, and it means that a and b leave the same remainder upon division by n. It is important to note that if $a \equiv b \bmod n$, then a and b are in the same equivalence class in $\overline{\mathbb{Z}}_n$. Thus, since we showed in Example 2.1.2 that $11 \equiv 2 \bmod 3$, 11 and 2 are both elements of $\overline{2} \in \overline{\mathbb{Z}}_3$.

Notice also that if $a, b \in \mathbb{Z}_n$ then $0 \leqslant a, b < n$. The key idea is that $\mathbb{Z}_n$ contains only the n possible remainders of any integer divided by n. On the other hand, the elements of $\overline{\mathbb{Z}}_n$ are equivalence classes, so for any $\overline{a} \in \overline{\mathbb{Z}}_n$, $\overline{a} = \{\ldots, a-2n, a-n, a, a+n, a+2n, \ldots\}$. Furthermore, $\alpha \equiv \beta \bmod n$ for any $\alpha, \beta \in \overline{a}$, since for $\alpha = a + jn$ and $\beta = a + kn$, where $j, k \in \mathbb{Z}$, we have

$$\begin{aligned}(a + jn) - (a + kn) &= (a - a) + (jn - kn) \\ &= n(j - k) \\ &\equiv 0 \bmod n.\end{aligned}$$

Thus, $n \mid (\alpha - \beta)$ and it follows that $\alpha \equiv \beta \bmod n$. ∎

We have used the notation $\overline{a}$ to denote the equivalence class $\overline{a} \in \overline{\mathbb{Z}}_n$. Another notation that can be used interchangeably is $[a] \in \overline{\mathbb{Z}}_n$, where

$$[a] = \{a + in : i \in \mathbb{N}\} = \overline{a}.$$

We use both notations in this thesis, but will endeavor to make the meaning clear when there is risk of ambiguity or confusion with a particular notation.

There is an underlying idea here that may seem obvious, but is very important in this thesis, so it bears special mention. For any $a \in \mathbb{Z}$ and a specific $n \in \mathbb{N}$, there are an infinite number of values of b for which $a \equiv b \bmod n$. In other words, if $n = 4$ and $a = 11$, then $11 \equiv 3 \bmod 4$. But any integer that is of the form $4k + 3$, where $k \in \mathbb{Z}$, will also have a least residue of 3 modulo 4. Thus for $k \in \mathbb{Z}$, $11 \equiv (4k + 3) \bmod 4$. Since there are an infinite number of possible values of k to choose from in $\mathbb{Z}$, this gives us an infinite number of integers that have a least residue of 3 modulo 4.

The last thing we want to mention before moving on to the next section is that there are several statements that are consequences of the work we have done in this section. These three statements are equivalent and will be used interchangeably in this thesis.

1. $a - b = nq$.

2. $n \mid a - b$.

3. If by the division algorithm, $a = nq_1 + r_1$ and $b = nq_2 + r_2$, then $r_1 = r_2$.

2.5 Binomial Theorem

Proposition 2.5.1 (Binomial Expansion Theorem) *For all $x, y \in \mathbb{Z}$, the binomial expansion formula is*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k,$$

where the binomial coefficients are given by

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Example 2.5.2 Let $x, y \in \mathbb{Z}$. We want to expand $\big(x+y\big)^5$ using the binomial theorem. First, we will determine the coefficients.

$$\begin{aligned}
\binom{5}{0} &= \frac{5!}{0!(5-0)!} = \frac{5!}{5!} = 1 \\
\binom{5}{1} &= \frac{5!}{1!(5-1)!} = \frac{5 \cdot 4!}{4!} = 5 \\
\binom{5}{2} &= \frac{5!}{2!(5-2)!} = \frac{5 \cdot 4 \cdot 3!}{2!3!} = \frac{20}{2} = 10 \\
\binom{5}{3} &= \frac{5!}{3!(5-3)!} = \frac{4 \cdot 4 \cdot 3 \cdot 2!}{3 \cdot 2!2!} = \frac{20}{2} = 10 \\
\binom{5}{4} &= \frac{5!}{4!(5-4)!} = \frac{5 \cdot 4!}{4!1!} = 5 \\
\binom{5}{5} &= \frac{5!}{5!(5-5)!} = \frac{1}{0!} = 1
\end{aligned}$$

Thus,

$$\begin{aligned}
(x+y)^5 &= \sum_{k=0}^{5} \binom{5}{k} x^{n-k} y^k \\
&= x^5 + 5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4 + y^5.
\end{aligned}$$

□

Example 2.5.3 Let $x \in \mathbb{Z}$ and consider $(x-1)^5$.

$$\begin{aligned}\big(x+(-1)\big)^5 &= x^5 + 5x^4(-1) + 10x^3(-1)^2 + 10x^2(-1)^3 + 5x(-1)^4 + (-1)^5 \\ &= x^5 - 5x^4 + 10x^3 - 10x^2 + 5x - 1\end{aligned}$$

This example is similar to the previous one, but note that 5 is a prime number, and the first and last terms of our polynomial are not divisible by 5. However, the coefficients of the middle four terms are all multiples of 5. We will look at similar polynomials when we examine the Eisenstein Criterion later on. If the constant term was divisible by 5 but not 25, then the polynomial would be irreducible over the rational numbers. Of course that's not the case here, since the polynomial was in factored form to begin with. □

We have reviewed a lot of basic concepts in this chapter, and they will serve as a foundation to build upon. In the next chapter, we take a much closer look at congruences and modular arithmetic.

Chapter 3

Modular Arithmetic

In this chapter, we will explore in more detail some of the ideas of congruence and modular arithmetic that were introduced in Chapter 2. We begin by defining a new function and several operations that use these ideas, but that strip away unnecessary notation and allow us to focus solely on the mechanics of what is taking place in various settings. Initially we explore addition modulo n for any integers, by defining and using a function LR_n and its associated operation $+_n$. We then extend those concepts so that we can work first with representatives of equivalence classes and then the elements of $\mathbb{Z}_n$, which are already least residues modulo n.

Because modular arithmetic and congruences play such an important role in this thesis, it's crucial to establish a firm foundation before we proceed into more complicated material.

Definition 3.0.4 Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$.

1. Define $\mathrm{LR}_n : \mathbb{Z} \to \mathbb{Z}$ by $\mathrm{LR}_n(a) = r$, where $a = nq + r$ by the division algorithm, and r is the least residue of a modulo n.

2. Define $+_n : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ by $a +_n b = \mathrm{LR}_n(a + b)$. ♢

Example 3.0.5 Consider the integers 17 and 6. Then $17 +_4 6 = \mathrm{LR}_4(23) = 3$, since $23 = 4 \cdot 5 + 3$ by the division algorithm. Note that if we consider instead 16 and 12, then $16 +_4 12 = \mathrm{LR}_4(28) = 0$, because $28 = 4 \cdot 7 + 0$. In fact, it will always be the case that $\mathrm{LR}_n(kn) = 0$, for $k \in \mathbb{Z}$, since the remainder by the division algorithm will be 0. □

Theorem 3.0.6 *Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. Then $a +_n b = LR_n(a) +_n LR_n(b)$.*

Proof: Let $a = nq_1 + r_1$ and $b = nq_2 + r_2$, where $0 \leqslant r_1, r_2 < n$, by the division algorithm. There are two cases to consider.

Case 1: $0 \leqslant r_1 + r_2 < n$

$$\begin{aligned}
a +_n b &= \mathrm{LR}_n(a + b) && \text{(Definition 3.0.4)} \\
&= \mathrm{LR}_n\big(n(q_1 + q_2) + (r_1 + r_2)\big) && \text{(Substitution)} \\
&= r_1 + r_2 && \text{(Definition 3.0.4)} \\
&= \mathrm{LR}_n(r_1 + r_2) && \text{(Definition 3.0.4)} \\
&= r_1 +_n r_2 && \text{(Definition 3.0.4)} \\
&= \mathrm{LR}_n(a) +_n \mathrm{LR}_n(b) && \text{(Definition 3.0.4)}
\end{aligned}$$

Case 2: $n \leqslant r_1 + r_2$

Note that $0 \leqslant r_1, r_2 \leqslant n-1$ implies that $0 \leqslant r_1 + r_2 \leqslant 2n-2 < 2n-1$. But $n \leqslant r_1 + r_2$, so $n \leqslant r_1 + r_2 < 2n-1 \iff 0 \leqslant r_1 + r_2 - n < n-1$.

$$
\begin{aligned}
a +_n b &= \mathrm{LR}_n(a+b) && \text{(Definition 3.0.4)} \\
&= \mathrm{LR}_n\big(n(q_1+q_2) + (r_1+r_2)\big) && \text{(Substitution)} \\
&= \mathrm{LR}_n\big(n(q_1+q_2+1) + (r_1+r_2-n)\big) && \text{(Addition of 0)} \\
&= r_1 + r_2 - n && \text{(Definition 3.0.4)} \\
&= \mathrm{LR}_n(r_1+r_2) && \text{(Definition 3.0.4)} \\
&= r_1 +_n r_2 && \text{(Definition 3.0.4)} \\
&= \mathrm{LR}_n(a) +_n \mathrm{LR}_n(b) && \text{(Definition 3.0.4)}
\end{aligned}
$$

In both cases, we have $a +_n b = \mathrm{LR}_n(a) +_n \mathrm{LR}_n(b)$. Since a and b were chosen arbitrarily, the result holds for all $a, b \in \mathbb{Z}$. ∎

Example 3.0.7 If we examine 6 and 15, we see that $6 +_4 15 = 1$, by Definition 3.0.4, but by the previous theorem, $\mathrm{LR}_4(6) +_4 \mathrm{LR}_4(15) = 2 +_4 3 = 1$. It is in fact an immediate consequence of Theorem 3.0.6 that if $\mathrm{LR}_n(a) = r$ and $\mathrm{LR}_n(b) = s$, then $a +_n b = r +_n s$. □

Recall that in Chapter 2, we defined $[a] \in \overline{\mathbb{Z}}_n$ to be the equivalence class containing a, which is equivalent to $\overline{a}$. We use the notation $[a]$ here temporarily, to avoid confusion from an abundance of overlines.

Theorem 3.0.8 *Let* $[a], [a'], [b], [b'] \in \overline{\mathbb{Z}}_n$. *If* $[a] = [a']$ *and* $[b] = [b']$, *then*

$$a +_n b = a' +_n b'.$$

Proof: Since $[a] = [a']$, we have $\mathrm{LR}_n(a) = \mathrm{LR}_n(a')$, by the definition of equivalence classes. Likewise, $\mathrm{LR}_n(b) = \mathrm{LR}_n(b')$, and

$$\begin{aligned} a +_n b &= \mathrm{LR}_n(a) +_n \mathrm{LR}_n(b) && \text{(Theorem 3.0.6)} \\ &= \mathrm{LR}_n(a') +_n \mathrm{LR}_n(b') && \text{(Substitution)} \\ &= a' +_n b'. && \text{(Theorem 3.0.6)} \end{aligned}$$

It follows that addition modulo n is well defined when working with representatives of equivalence classes. ∎

Example 3.0.9 Since 17 and 6 leave the same remainder on division by 11, they are in the same residue class. Likewise, $[30] = [19] = [8]$, so

$$6 +_{11} 19 = 6 +_{11} 8 = 17 +_{11} 30.$$

It will be useful to be able to use any convenient representative from an equivalence class, and still obtain the same residue under the operation $+_n$. □

Theorem 3.0.10 *Let* $a, a' \in \mathbb{Z}$ *and* $n \in \mathbb{N}$. *If* $LR_n(a) = LR_n(a')$, *then* $LR_n(a - a') = 0$.

Proof: Let $a = nq_1 + r_1$ and $a' = nq_2 + r_2$, by the division algorithm. Suppose that $\mathrm{LR}_n(a) = \mathrm{LR}_n(a')$. Then $r_1 = r_2$, so $a - a' = n(q_1 - q_2)$.

Since $\mathrm{LR}_n\big(n(q_1 - q_2)\big) = 0$, it follows that when $\mathrm{LR}_n(a) = \mathrm{LR}_n(a')$, we have $\mathrm{LR}_n(a - a') = 0$. ∎

Example 3.0.11 We know that 17 and 6 are in the same residue class modulo 11, so $\mathrm{LR}_{11}(17) = 6 = \mathrm{LR}_{11}(6)$. Thus $\mathrm{LR}_{11}(17 - 6) = \mathrm{LR}_{11}(11) = 0$. □

In Definition 3.0.4, we defined $+_n$ to be addition of any two integers modulo n. We want to examine a similar operation now, but instead of defining the operation for all integers, we define it specifically for the elements of $\mathbb{Z}_n$, or the least residues modulo n. Since the operations are defined for different sets, we introduce a new symbol.

Definition 3.0.12 Let $n \in \mathbb{N}$ and $r, s \in \mathbb{Z}_n$. Define $\dot{+}_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ by $r \dot{+}_n s = r +_n s$. ♢

Note that $\dot{+}_n$ is well defined, since $\mathrm{LR}(a) \in \mathbb{Z}_n$.

Example 3.0.13 Choose two elements from $\mathbb{Z}_5$, say 3 and 4. Then by Definition 3.0.12, $3 \dot{+}_5 4 = 3 +_5 4 = \mathrm{LR}_5(7) = 2$. □

Example 3.0.14 Let $r, s \in \mathbb{Z}_n$. Then

$$\begin{aligned} r \dot{+}_n s &= r +_n s && \text{(Definition 3.0.12)} \\ &= \mathrm{LR}_n(r) +_n \mathrm{LR}_n(s) && \text{(Theorem 3.0.6)} \\ &= \mathrm{LR}_n(r) \dot{+}_n \mathrm{LR}_n(s). && \text{(Definition 3.0.12)} \end{aligned}$$

This result is analogous to the one established in Theorem 3.0.6. □

We want to define the operation of addition modulo n again, but this time, we define it for equivalence classes. We again introduce a new symbol for this operation, to avoid confusion.

Definition 3.0.15 Define $\overline{+}_n : \overline{\mathbb{Z}}_n \times \overline{\mathbb{Z}}_n \to \overline{\mathbb{Z}}_n$ by $[a]\overline{+}_n[b] = [a +_n b]$, where $[a], [b]$ are the equivalence classes containing a and b respectively. $\diamondsuit$

Example 3.0.16 Let $[a], [a'], [b], [b'] \in \overline{\mathbb{Z}}_n$. Suppose $[a] = [a']$ and $[b] = [b']$. Then

$$\begin{aligned} [a]\overline{+}_n[b] &= [a +_n b] && \text{(Definition 3.0.15)} \\ &= [a' +_n b'] && \text{(Theorem 3.0.8)} \\ &= [a']\overline{+}_n[b'], && \text{(Definition 3.0.15)} \end{aligned}$$

so $\overline{+}_n$ is well defined. $\square$

Example 3.0.17 The equivalence classes [17] and [30] are in $\overline{\mathbb{Z}}_{11}$, so

$$[17]\overline{+}_{11}[30] = [17 +_{11} 30] = [\mathrm{LR}_{11}(47)] = [3].$$

But [6] = [17] and [8] = [30], so if we choose 6 and 8 to represent our residue classes instead, we have $[6]\overline{+}_{11}[8] = [6 +_{11} 8] = [3]$ as well. $\square$

Recall that $\dot{+}_n$ is the operation defined for least residues and $\overline{+}_n$ is defined for equivalence class representatives. Every least residue modulo n is in a different equivalence class in $\overline{\mathbb{Z}}_n$, so each of the least residues r is an

element in the associated equivalence class $[r]$. This means that because of the way we defined $\overline{+}_n$, we could use it on the r instead of using $\dot{+}_n$.

Now that we have established that addition modulo n is well defined regardless of whether we are working with elements of $\mathbb{Z}$, $\mathbb{Z}_n$, or $\overline{\mathbb{Z}}_n$, we will simply use $+_n$ to denote addition modulo n. In later chapters, where the context is clear, we will just use $+$ for addition modular n.

We have established some very basic results about modular arithmetic here. In Chapter 4, we review group theory and use these results about modular arithmetic to introduce some groups that will be useful to us later on.

Chapter 4

Group Theory

This chapter serves as a general review of group theory that is relevant to this thesis. We begin by recalling the definition of a group and then establish some specific groups that we will be working with frequently. Next we define n^{th} roots of unity and introduce the Gaussian integers and Eisenstein integers. These three concepts are going to be major players as we develop reciprocity theory.

In Section 2, we define subgroups and do some examples using known groups. We spend some time looking at cosets and normal subgroups as well. Finally we review homomorphisms, isomorphisms, and permutation groups, and then state Cayley's Theorem.

Section 3 begins with a review of cyclic groups and generators. We give a more rigorous definition of greatest common divisor here as well, and then

establish several results about cyclic groups and greatest common divisor. We also prove theorems that tie together the notions of divides and gcd, as well as theorems that look at the relationships between gcd and modular arithmetic. We introduce Euler's φ-function in this section and then explore the group of units. We wrap up the section by proving Fermat's Little Theorem, an associated corollary, and Euler's Theorem, and then explore the notion of primitive roots of a positive integer n.

4.1 Groups

We are used to performing operations on numbers, and we are certainly familiar with addition and subtraction. If we take two numbers and add them together, the result is a single number. If we perform addition on a specific set of numbers, say $\mathbb{Z}^+$, then adding two positive integers together yields another positive integer. In other words, the result is also an element of $\mathbb{Z}^+$. Such an operation is called a *binary operation*, and addition and multiplication are two examples of binary operations. When the result is an element of the original set, we say that we have *closure under the operation*. Note that if we subtract 4 from 3, the result is -1, which is not an element of $\mathbb{Z}^+$. Thus, subtraction is not a binary operation on $\mathbb{Z}^+$, since -1 is not a positive integer. Similarly, division is not a binary operation on $\mathbb{Z}^+$, since $\dfrac{3}{4}$ is not an integer at all.

Definition 4.1.1 A *group* $\langle G, * \rangle$ is a set G, closed under a binary operation $*$, where $a * b = ab$, such that the following axioms are satisfied:

1. **(Associativity of $*$)** For all $a, b, c \in G$, $(ab)c = a(bc)$.

2. **(Identity element e for $*$)** There is an element e in G, called the *identity of* G, such that for all $x \in G$, $ex = x = xe$.

3. **(Inverse a^{-1} of a)** For each $a \in G$, there is a unique element a^{-1} in G, called the *inverse of* a, such that $aa^{-1} = e = a^{-1}a$.

A group G is called *abelian* if its binary operation is commutative. In this case, $a * b$ is usually denoted $a + b$. ♢

We will often refer to a group using only G, or some other set, rather than using the longer notation $\langle G, * \rangle$. When we use this abbreviated notation for a group, the group operation will be made clear, and in fact the $*$ is usually suppressed, so that $a * b$ is simply ab. We will occasionally denote the group identity as e_G and the group operation as $*_G$, for the sake of clarity.

Example 4.1.2 Consider the set $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ and the operation $+_n$ from Definition 3.0.4.

Based on our previous work, we can see that $\mathbb{Z}_n$ is closed under the operation $+_n$.

For any $r \in \mathbb{Z}_n$,

$$0 +_n r = \mathrm{LR}_n(0 + r) = r = \mathrm{LR}_n(r + 0) = r +_n 0,$$

thus 0 is the additive identity for $\mathbb{Z}_n$.

Next we want to establish that each element has an inverse in $\mathbb{Z}_n$.

$$\begin{aligned} r +_n (n - r) &= \mathrm{LR}_n(r + n - r) && \text{(Definition 3.0.4)} \\ &= \mathrm{LR}_n(n) && \text{(Arithmetic)} \\ &= 0, && \text{(Example 3.0.5)} \end{aligned}$$

so $(n - r)$ is the additive inverse for r modulo n, and it is unique since each $r \in \mathbb{Z}_n$ is unique.

Associativity follows automatically, since $a +_n b = \mathrm{LR}_n(a + b)$ and $+$ is associative. Also $+_n$ is commutative, since $+$ is. It follows that $\langle \mathbb{Z}_n, +_n \rangle$ is an abelian group by definition. More specifically, it is the *group of least residues modulo n*. □

Using the other operations that we defined in Chapter 3, and a similar approach, it can easily be shown that $\langle \mathbb{Z}_n, \dot{+}_n \rangle$ and $\langle \overline{\mathbb{Z}}_n, \overline{+}_n \rangle$ are also abelian groups. We will see in Section 4.3 that these three groups are *isomorphic* to each other.

There is a similar group that we will explore later on, and that is the *group of units modulo n*. It has the notation $\langle \mathbb{Z}_n^*, \cdot \rangle$, and is the set of integers without 0, under the operation multiplication modulo n. Establishing that the group of units satisfies the group axioms is similar to the work done in Example 4.1.2, albeit more difficult.

Example 4.1.3 Let $\zeta \in \mathbb{C}$ and $n \in \mathbb{N}$. Then ζ is called an n^{th} *root of unity* if $\zeta^n = 1$. The n^{th} roots of unity can be expressed as

$$1, e^{2\pi i/n}, e^{(2\pi i/n)2}, \ldots, e^{(2\pi i/n)(n-1)}.$$

Let $U_n = \{e^{2k\pi i/n} : k = 0, 1, \ldots, n-1\} = \{\zeta^0, \zeta^1, \ldots, \zeta^{n-1}\}$. For any $\zeta^i, \zeta^j \in U_n$, we have $\zeta^i \cdot \zeta^j = \zeta^{i+j}$. But $\zeta^n = 1$, so $\zeta^i \cdot \zeta^j = \zeta^{i+_n j}$, and U_n is closed under multiplication.

Associativity follows automatically by properties of exponents. Since $\zeta^0 = 1$, the multiplicative identity is in U_n. Again using properties of exponents, it's clear that ζ^{n-k} is the inverse of ζ^k. It follows that the n^{th} roots of unity form a group by definition.

Observe that ζ^1 *generates* all of the n^{th} roots of unity in the sense that if α is an n^{th} root of unity, then $\alpha = \zeta^k$ for some k. The ζ that generate the group of the n^{th} roots of unity are called *primitive roots of unity.* An example of a primitive n^{th} root of unity is of the form $\zeta = e^{2\pi i/n}$. □

We will explore the roots of unity more later on, but for now it is enough to know that they form a group.

Example 4.1.4 In this example, we examine complex numbers of the form $a + bi$, where $a, b \in \mathbb{Z}$. It is clear that $\{a + bi : a, b \in \mathbb{Z}\}$ forms an abelian group under ordinary addition, with $0 + 0i$ the additive identity and $-(a + bi)$ the unique inverse of $a + bi$. The elements of this group have a special name, the

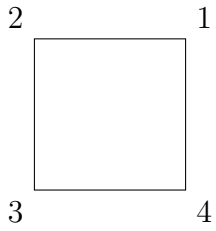
Gaussian integers. □

We will be working with the Gaussian integers more later on. There is another subset of the complex numbers, called the Eisenstein integers, that will play a major role in our work with cubic reciprocity toward the end of this thesis.

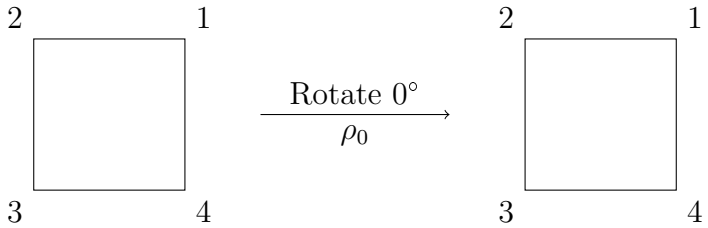
Example 4.1.5 Recall from the definition of roots of unity that if $\zeta \in \mathbb{C}$ and $\zeta^n = 1$, then ζ is an n^{th} root of unity. Consider the equation $x^3 = 1$. Certainly $x^3 - 1 = (x-1)(x^2+x+1) = 0$. From Example 4.1.3, we know that a primitive 3^{rd} root of unity has the form $e^{2\pi i/3}$. Because the cube root of unity plays an important role in mathematics, it is denoted by a special symbol, ω. Thus $\omega = e^{2\pi i/3}$, and in fact it can be established by using the quadratic formula to solve $x^2 + x + 1 = 0$ that $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ and $\omega^2 = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$. Thus the three roots of $x^3 = 1$ are given by $x = 1$, $x = \omega$, and $x = \omega^2$. □

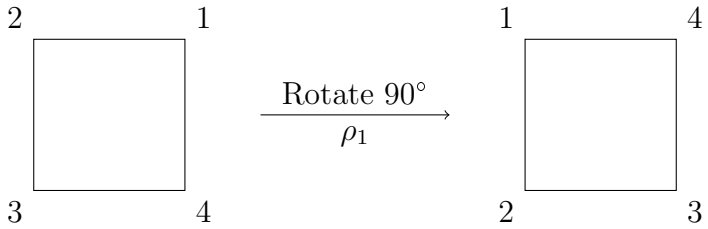
Example 4.1.6 Consider the complex numbers of the form $a + b\omega$, where $a, b \in \mathbb{Z}$. It is clear that $\{a + b\omega : a, b \in \mathbb{Z}\}$ forms an abelian group under ordinary addition of complex numbers. The elements of this group are called the *Eisenstein integers*. We will see in Chapter 5 that the Eisenstein integers form a ring, and then we will establish some properties that will be useful in our work with cubic reciprocity. □

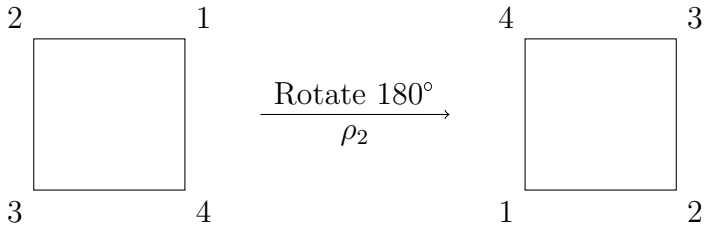
Example 4.1.7 Consider the square with vertices numbered 1 through 4, as shown below.

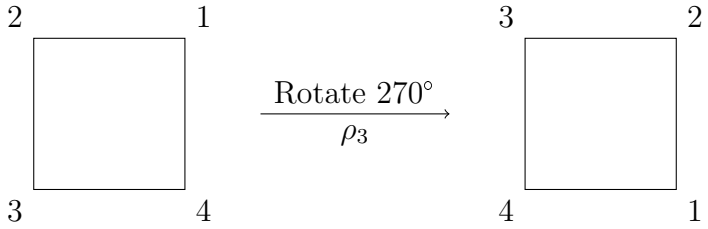


Consider the counterclockwise rotations of this square. We want to pay close attention to where the numbered vertices get sent with each rotation.

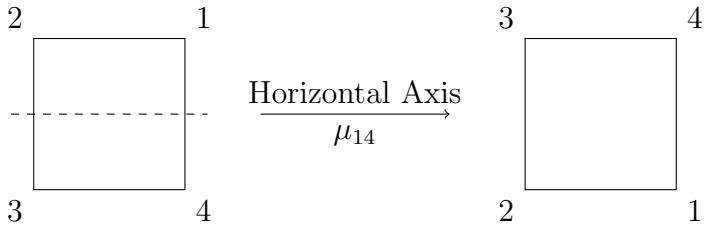


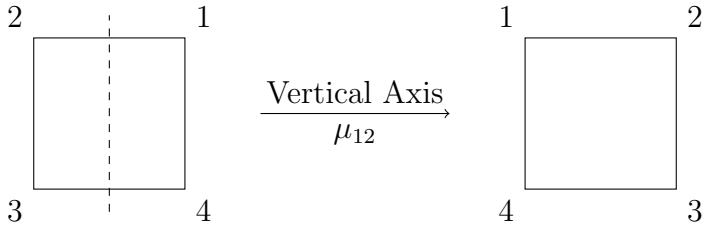


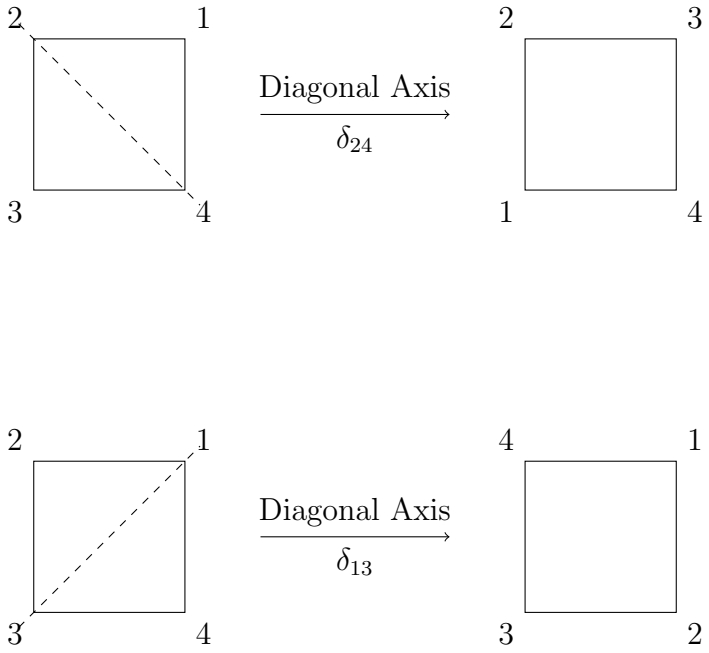




Next we examine the flips of our square. We first flip it about a horizontal axis, then about a vertical axis. The last two flips will be about the diagonals through vertices 2, 4 and vertices 1, 3 respectively.







If we consider each motion to be a function, then the operation on this set is function composition, so for $\delta_{24}\rho_2$, we would first rotate the square 180° and then flip it along the diagonal through vertices 2 and 4.

The group table shows all combinations of motions of the square of the form ab, where the entry in the top row is the first motion performed on the square, and the entry in the lefthand column is the second motion.

	ρ_0	ρ_1	ρ_2	ρ_3	μ_{14}	μ_{12}	δ_{24}	δ_{13}
ρ_0	ρ_0	ρ_1	ρ_2	ρ_3	μ_{14}	μ_{12}	δ_{24}	δ_{13}
ρ_1	ρ_1	ρ_2	ρ_3	ρ_0	δ_{24}	δ_{13}	μ_{12}	μ_{14}
ρ_2	ρ_2	ρ_3	ρ_0	ρ_1	μ_{12}	μ_{14}	δ_{13}	δ_{24}
ρ_3	ρ_3	ρ_0	ρ_1	ρ_2	δ_{13}	δ_{24}	μ_{14}	μ_{12}
μ_{14}	μ_{14}	δ_{24}	μ_{12}	δ_{13}	ρ_0	ρ_2	ρ_1	ρ_3
μ_{12}	μ_{12}	δ_{13}	μ_{14}	δ_{24}	ρ_2	ρ_0	ρ_3	ρ_1
δ_{24}	δ_{24}	μ_{12}	δ_{13}	μ_{14}	ρ_3	ρ_1	ρ_0	ρ_2
δ_{13}	δ_{13}	μ_{14}	δ_{24}	μ_{12}	ρ_1	ρ_3	ρ_2	ρ_0

It can be seen easily that every motion appears exactly once in each row and each column, so the set of motions on the square is closed under composition of functions. However, the motions are not commutative, since $\delta_{24}\mu_{14} = \rho_1$ and $\mu_{14}\delta_{24} = \rho_3$.

Notice that for any b in the set, $\rho_0 b = b = b\rho_0$, so the identity element is the rotation by 0°, or ρ_0.

We can see that each of the rotations has a unique inverse that is contained in the set, since each row and each column contains ρ_0, thus we can see exactly which elements combined to result in the identity in each case.

Because the operation is function composition, and composition of functions is associative, we get the associative property automatically.

It follows that this set of rotations and flips on a square forms a group, and in fact it is called the dihedral group of order 8, which is denoted D_4. It might seem counterintuitive, but generally the dihedral group of order $2n$ is denoted D_n, although some references will denote it as D_{2n}. In this thesis, we will use the former notation. □

4.2 Subgroups

Definition 4.2.1 Let G be a group and let H be a nonempty subset of G. H is a *subgroup* of G, denoted $H \leqslant G$, if the following conditions are satisfied.

1. H contains e_G.
2. If $a, b \in H$, then $a *_G b \in H$.
3. If $a \in H$, then $a^{-1} \in H$. ♢

Example 4.2.2 Recall that $Z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$. Clearly $\{0, 2, 4, 6\}$ is a nonempty subset of $\mathbb{Z}_8$, and it contains 0, which is the identity of $\mathbb{Z}_8$. It is easy to see that our subset is closed under addition modulo 8. Note that $2 +_8 6 = 8 \equiv 0 \bmod 8$ and $4 +_8 4 = 8 \equiv 0 \bmod 8$, so each nonidentity element contains an inverse in the subset. Thus, $\{0, 2, 4, 6\}$ is a subgroup of $\mathbb{Z}_8$. □

Example 4.2.3 Recall that $D_4 = \{\rho_0, \rho_1, \rho_2, \rho_3, \mu_{14}, \mu_{12}, \delta_{24}, \delta_{13}\}$ is the set of rotations and flips of a square from Example 4.1.7. If we examine $\{\rho_0, \mu_{14}\}$,

we see that this is a nonempty subset of D_4, and it contains ρ_0, which is the identity motion. Clearly this subset is closed under the function composition of D_4, and $\mu_{14}\mu_{14} = \rho_0$, so μ_{14} is its own inverse. It follows that $\{\rho_0, \mu_{14}\}$ is a subgroup of D_4. □

Definition 4.2.4 Let H be a subgroup of a group G and let $a \in G$. The subset $aH = \{ah : h \in H\}$ of G is the *left coset* of H containing a and the subset $Ha = \{ha : h \in H\}$ of G is the *right coset* of H containing a. ♢

Recall that we have suppressed the group operation in our general notation, so $ah = a + h$ if the group operation is addition and $ah = a \cdot h$ if the operation is multiplication.

Example 4.2.5 Let $G = \mathbb{Z}_8$ and $H = \{0, 2, 4, 6\}$. The left cosets of H are

$$0 +_8 H = \{0, 2, 4, 6\}$$

$$1 +_8 H = \{1, 3, 5, 7\}$$

$$2 +_8 H = \{2, 4, 6, 0\}$$

$$3 +_8 H = \{3, 5, 7, 1\}$$

$$4 +_8 H = \{4, 6, 0, 2\}$$

$$5 +_8 H = \{5, 7, 1, 3\}$$

$$6 +_8 H = \{6, 0, 2, 4\}$$

$$7 +_8 H = \{7, 1, 3, 5\}.$$

Note that when $a \in \mathbb{Z}_8$ is even, $a +_8 H$ is a permutation of the elements in H and when $a \in \mathbb{Z}_8$ is odd, $a +_8 H$ is a permutation of the coset $1 +_8 H$.

Likewise, it can be easily shown that the right cosets are permutations of H when a is even and permutations of $H +_8 1 = \{1, 3, 5, 7\}$ when a is odd. For any given $a \in \mathbb{Z}_8$, the left and right cosets are identical. This will always be the case when G is an abelian group, as $\mathbb{Z}_8$ is, since $ah = ha$ for all $a, h \in G$ when G is abelian. The cosets of H form a partition of $\mathbb{Z}_8$ into its even and odd elements. Furthermore, the left and right cosets are the same size. □

Proposition 4.2.6 *Let H be a subgroup of a finite group G.*

1. *The cosets of H form a partition of G and the left and right cosets are the same size. In fact, one of the cosets is H itself.*

2. *The order of H is a divisor of the order of G.* **(Lagrange's Theorem)**

The proof of this proposition is omitted here, but it can be found in [6].

Example 4.2.7 Let $H = \{0, 2, 4, 6\}$ and let $G = \mathbb{Z}_8$. We saw previously that H is a subgroup of G. Note that there are 8 elements in $\mathbb{Z}_8$, 4 elements in H, and $4 \mid 8$. □

Definition 4.2.8 A subgroup H of a group G is *normal* if its left and right cosets coincide, that is, if $gH = Hg$ for all $g \in G$. This will be denoted by $H \trianglelefteq G$. ♢

$H = \{0, 2, 4, 6\}$ is a normal subgroup of $\mathbb{Z}_8$, since we saw earlier that the left and right cosets are identical.

Example 4.2.9 In Example 4.2.3, we showed that $H = \{\rho_0, \mu_{14}\}$ is a subgroup of D_4. In Example 4.1.7, we saw that D_4 is not an abelian group and since $\delta_{24}H = \{\rho_0, \rho_1\}$ and $H\delta_{24} = \{\rho_0, \rho_3\}$, the subgroup $H = \{\rho_0, \mu_{14}\}$ is not normal. □

Theorem 4.2.10 *Let H be a subgroup of a group G. Then left coset multiplication is well defined by the equation*

$$(aH)(bH) = (ab)H$$

if and only if H is a normal subgroup of G.

Recall from Proposition 4.2.6 that the left cosets of H partition G, so $x \in aH$ implies that $xH = aH$ and $y \in H$ implies that $yH = H$.

Proof: Let $H \leqslant G$ and let $a \in G$. Suppose first that left coset multiplication is well defined by $(aH)(bH) = (ab)H$. Our goal is to show that $aH = Ha$, which implies that H is normal.

Let $x \in aH$ and let $a^{-1} \in a^{-1}H$. Then

$$(xH)(a^{-1}H) = (xa^{-1})H$$

and

$$(aH)(a^{-1}H) = (aa^{-1})H = eH = H.$$

Since coset multiplication is well defined, $(xa^{-1})H = H$, which means that $xa^{-1} = h$, for some $h \in H$. This implies that $x = ha$ for some h, so $x \in Ha$, and $aH \subseteq Ha$. By a symmetric argument, $Ha \subseteq aH$. It follows that $aH = Ha$, so H is a normal subgroup of G.

Now suppose that H is a normal subgroup of G. Our goal is to show that choosing different representatives from aH and bH does not yield different cosets, and thus that left coset multiplication is well defined.

Let $h_1 b \in Hb$. Since H is normal, $Hb = bH$. This implies that $h_1 b \in bH$ as well, so $h_1 b = bh_3$ for some $h_3 \in H$. Thus for $bh_2 \in bH$,

$$\begin{aligned}
(ah_1)(bh_2) &= a(h_1 b)h_2 && \text{(Associative Property)} \\
&= a(bh_3)h_2 && \text{(Substitution)} \\
&= (ab)(h_3 h_2). && \text{(Associative Property)}
\end{aligned}$$

Since $h_3 h_2 \in H$, $(ab)(h_3 h_2) \in (ab)H$, so $ah_1 bh_2 \in (ab)H$ and $(ab)H = (ah_1 bh_2)H$. Thus left coset multiplication is well defined. It follows that coset multiplication is well defined if and only if H is a normal subgroup of G. ∎

Definition 4.2.11 Let G and G' be groups and let $\varphi : G \to G'$ be a function. If the *homomorphism property*,

$$\varphi(x *_G y) = \varphi(x) *_{G'} \varphi(y),$$

holds for all $x, y \in G$, then φ is called a *group homomorphism*.

If φ is both one-to-one and onto, then φ is an *isomorphism*. If such a φ exists, then G and G' are *isomorphic* structures, denoted $G \cong G'$. $\diamondsuit$

Note that if φ is an isomorphism, then there exists $\varphi^{-1} : G' \to G$ such that $\varphi \circ \varphi^{-1}(a) = a$ and $\varphi^{-1} \circ \varphi(b) = b$.

Example 4.2.12 We saw in Example 4.2.5 that $H = \{0, 2, 4, 6\}$ is a group under the operation addition modulo 8. We claim that H is isomorphic to $\mathbb{Z}_4$. Define $\varphi : H \to \mathbb{Z}_4$ by $\varphi(h) = \dfrac{h}{2}$. Then φ is clearly one-to-one and onto.

Suppose $a, b \in H$. Let $a = 2i$ and $b = 2j$, where $i, j \in \{0, 1, 2, 3\}$. Then

$$\begin{aligned}
\varphi(a + b) &= \varphi(2i + 2j) && \text{(Substitution)} \\
&= \varphi\big(2(i + j)\big) && \text{(Distributive Property)} \\
&= i + j && \text{(Definition of } \varphi\text{)} \\
&= \varphi(a) + \varphi(b). && \text{(Definition of } \varphi\text{)}
\end{aligned}$$

Thus the homomorphism property holds, and it follows that φ is an isomorphism by definition, so $H = \{0, 2, 4, 6\} \cong \mathbb{Z}_4$ as claimed. $\square$

Example 4.2.13 Let X be an arbitrary set and consider the set F of all functions $f : X \to X$, such that f is both one-to-one and onto. Let $f \in F$ and $y \in X$. Then there is some $x \in X$, such that $f(x) = y$, since f is onto.

Since f is a bijection, there exists $f^{-1} : X \to X$, such that

$$f \circ f^{-1}(y) = f(x) = y$$

and

$$f^{-1} \circ f(x) = f^{-1}(y) = x.$$

Clearly f^{-1} is one-to-one and onto, so $f^{-1} \in F$. Suppose there is another function $f' \in F$, such that $f' \circ f(x) = x$ and $f \circ f'(y) = y$. Then

$$f \circ f^{-1}(y) = f \circ f'(y) \iff f^{-1} \circ f \circ f^{-1}(y) = f^{-1} \circ f \circ f'(y) \iff f^{-1}(y) = f'(y).$$

By a similar argument,

$$f' \circ f(x) = x = f^{-1} \circ f(x) \iff f'(y) = x = f^{-1}(y).$$

But y is arbitrary, so $f^{-1} = f'$. Thus each function $f \in F$ has a unique inverse $f^{-1} \in F$.

Suppose $h(x) = x$ for all $x \in X$. Then h is clearly one-to-one and onto, so $h \in F$. Note that $h \circ f(x) = h(y) = y$ and $f \circ h(x) = f(x) = y$, so h is the identity function.

We know that the composition of functions is associative, so we have associativity in F. Suppose f and g are two functions that are both one-to-one and onto. Then $f \circ g$ and $g \circ f$ are both clearly one-to-one and onto. Thus the composition of bijections is itself a bijection, so F is closed.

It follows that F is a group under function composition. □

Definition 4.2.14 Let X be a set and let $f : X \to X$ be a function. Then a *permutation group on* X is a subgroup of the set of all functions f that are both one-to-one and onto. ♢

Example 4.2.15 Recall that we worked with the rotations and flips of a square in Example 4.1.7. We want to think about that example in a slightly different way now. Instead of working with vertices on a square, we want to consider the set $\{1, 2, 3, 4\}$. If we define a function σ by

$$\sigma(1) = 4$$

$$\sigma(2) = 1$$

$$\sigma(3) = 2$$

$$\sigma(4) = 3,$$

then we have permuted the four elements. In *standard notation*, this is given by

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}.$$

Each column is read from the top down, and it says 1 goes to 4, 2 goes to 1, 3 goes to 2, and 4 goes to 3. This same function written in *cycle notation* is

$$\sigma = (1\ 4\ 3\ 2).$$

Then read from left to right, it also says 1 goes to 4, 4 goes to 3, 3 goes to 2, and 2 goes back to 1.

If we take the vertices of the square from Example 4.1.7 and use cycle notation to denote where each number (vertex) is sent, we will have the

following eight elements.

$$\rho_0 = (1)(2)(3)(4)$$

$$\rho_1 = (1\ 2\ 3\ 4)$$

$$\rho_2 = (1\ 3)(2\ 4)$$

$$\rho_3 = (1\ 4\ 3\ 2)$$

$$\mu_{14} = (1\ 4)(2\ 3)$$

$$\mu_{12} = (1\ 2)(3\ 4)$$

$$\delta_{24} = (1\ 3)$$

$$\delta_{13} = (2\ 4)$$

These eight elements form a subgroup of the symmetric group on 4 elements, which is denoted S_4 and contains twenty-four elements in total. We've already shown that the motions of the square form a group of order 8, and since we can also write those motions using this notation, it is easy to see that they are actually isomorphic to this subgroup of S_4. This result leads nicely to Cayley's Theorem. □

Proposition 4.2.16 (Cayley's Theorem) *Every group is isomorphic to a group of permutations.*

The proof of Cayley's Theorem can be found in [6], but is omitted here.

4.3 Cyclic Groups and the Greatest Common Divisor

Example 4.3.1 Let $a \in G$. Then consider $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$. Clearly $a^0 = e \in \langle a \rangle$, so $\langle a \rangle$ is nonempty and contains the identity element of G. If $a^n \in \langle a \rangle$, then $a^{-n} \in \langle a \rangle$ is its unique inverse. Since $a^n a^m = a^{m+n}$ and $m + n \in \mathbb{Z}$, $\langle a \rangle$ is closed. The associative property holds for elements of $\langle a \rangle$, since it holds in G. Thus $\langle a \rangle$ is a subgroup of G. □

Definition 4.3.2 Let G be a group and let $a \in G$. Then $\{a^n : n \in \mathbb{Z}\}$ is called the *cyclic subgroup of G generated by a*, and is denoted $\langle a \rangle$. If $\langle a \rangle = G$, then we say that *a generates G* and is a *generator for G*, and G is called a *cyclic group*. ♢

Lagrange's Theorem says that the order of a subgroup divides the order of the group, so $|\langle a \rangle|$ divides $|G|$, since $\langle a \rangle$ is a subgroup of G.

Theorem 4.3.3 *Let G be a cyclic group with generator a. If the order of G is infinite, then G is isomorphic to $\langle \mathbb{Z}, + \rangle$. If G has finite order n, then G is isomorphic to $\langle \mathbb{Z}_n, +_n \rangle$.*

Proof: Assume that G is a cyclic group with generator a.

Suppose first that the order of G is infinite. Then there does not exist $m \in \mathbb{N}$ such that $a^m = e$. We claim that if $j \neq k$, for $j, k \in \mathbb{Z}$, then $a^j \neq a^k$.

Suppose that $a^j = a^k$, and assume without loss of generality that $j > k$. Then we have

$$\begin{aligned} & a^j = a^k \\ \iff & a^j a^{-k} = e && \text{(Right multiplication by } a^{-k}\text{)} \\ \iff & a^{j-k} = e. && \text{(Properties of exponents)} \end{aligned}$$

But G has infinite order and $j - k \in \mathbb{N}$, thus it can't be true that $a^{j-k} = e$, so it must be the case that whenever j and k are distinct, a^j and a^k are also distinct. This means that every element in G can be expressed as a^m for a unique value of m in the integers. Thus we can define a map $\varphi : G \to \mathbb{Z}$ by $\varphi(a^i) = i$ for $i \in \mathbb{Z}$. This is everywhere defined by the given map and uniquely defined based on our work above, so φ is a well defined function.

Now for $a^j, a^k \in G$,

$$\begin{aligned} \varphi(a^j *_G a^k) &= \varphi(a^{j+k}) && \text{(Binary operation on } G\text{)} \\ &= j + k && \text{(Definition of } \varphi\text{)} \\ &= \varphi(a^j) + \varphi(a^k), && \text{(Definition of } \varphi\text{)} \end{aligned}$$

so φ is a homomorphism.

Define a map $\varphi : \mathbb{Z} \to G$ by $\varphi^{-1}(i) = a^i$. Since G is infinite, this map is everywhere defined. It is also clearly uniquely defined by its definition, so φ^{-1} is well defined, and is thus a function. Since

$$\varphi \circ \varphi^{-1}(i) = \varphi(a^i) = i$$

and

$$\varphi^{-1} \circ \varphi(a^i) = \varphi^{-1}(i) = a^i,$$

ϕ is both one-to-one and onto. It follows that φ is an isomorphism, so $G \cong \mathbb{Z}$.

Recall that $G = \langle a \rangle$ and suppose now that G has finite order n. Then $a^n = e$. Let $s \in \mathbb{Z}$. By the division algorithm, $s = nq + r$, where $0 \leqslant r < n$. Thus

$$a^s = a^{nq+r} = a^{nq}a^r = (a^n)^q a^r = e^q a^r = a^r.$$

Suppose without loss of generality that $j, k \in \mathbb{Z}$ such that $0 \leqslant k < j < n$. As we saw previously, if $a^j = a^k$, then $a^{j-k} = e$, and since $0 \leqslant k < j < n$, we have $0 < j-k < n$. But since a is a generator of G, n is the smallest positive integer such that $a^n = e$, thus it can't be the case that $a^j = a^k$ for distinct values of j and k. It follows that the elements $a^0, a^1, a^2, \ldots, a^{n-1}$ are all distinct. Since there are n such elements, they must be all of the elements in G, because $|G| = n$. As we did above, define a map $\varphi : G \to \mathbb{Z}_n$ by $\varphi(a^i) = i$, where $i \in \{0, 1, 2, \ldots, n-1\}$. This map is well-defined, as shown previously.

Let $a^j, a^k \in G$. Then

$$\begin{aligned}
\varphi(a^j *_G a^k) &= \varphi(a^{j+k}) && \text{(Binary operation on } G\text{)} \\
&= j +_n k && \text{(Definition of } \varphi\text{)} \\
&= \varphi(a^j) +_n \varphi(a^k), && \text{(Definition of } \varphi\text{)}
\end{aligned}$$

thus the homomorphism property holds for φ.

Define a map $\varphi^{-1} : \mathbb{Z}_n \to G$ by $\varphi^{-1}(i) = a^i$. Since G is cyclic, this map is everywhere defined. It is clear that it is also uniquely defined, and thus is a well defined function. Since

$$\varphi \circ \varphi^{-1}(i) = \varphi(a^i) = i$$

and

$$\varphi^{-1} \circ \varphi(a^i) = \varphi^{-1}(i) = a^i,$$

φ is both one-to-one and onto, and it follows that φ is an isomorphism. Thus $G \cong \mathbb{Z}_n$. ∎

Example 4.3.4 Let $n = 4$. Then $\langle 4 \rangle = \{\dots, -8, -4, 0, 4, 8, \dots\}$ has infinite order. The group $\langle 4 \rangle$ is denoted $4\mathbb{Z}$, and since every element in $4\mathbb{Z}$ is an integer, $4\mathbb{Z} \subseteq \mathbb{Z}$. We can define $\varphi : 4\mathbb{Z} \to \mathbb{Z}$ by $\varphi(4k) = k$. It is easy to see that φ is both one-to-one and onto, so by Theorem 4.3.3, $4\mathbb{Z} \cong \mathbb{Z}$. □

Example 4.3.5 $\langle \mathbb{Z}_n, +_n \rangle$ is a cyclic group, because 1 is always a generator, for any $n \in \mathbb{N}$. To illustrate this, suppose $n = 3$. Then $1 +_3 1 = 2$ and $1 +_3 1 +_3 1 = 3 \equiv 0 \bmod 3$, so $\langle 1 \rangle = \mathbb{Z}_3$.

Notice also that $2 +_3 2 = 4 \equiv 1 \bmod 3$ and $2 +_3 2 +_3 2 = 6 \equiv 0 \bmod 3$, so 2 is a generator of $\mathbb{Z}_3$ as well.

Suppose now that $n = 4$. 1 is a generator for $\mathbb{Z}_4$, but now we have $2 +_4 2 \equiv 0 \bmod 4$, $2 +_4 2 +_4 2 \equiv 2 \bmod 4$, and $2 +_4 2 +_4 2 +_4 2 \equiv 0 \bmod 4$, so 2 is not a generator. The difference here is that 2 and 4 are not relatively

prime. If we look at 3, we see that $3 +_4 3 \equiv 2 \bmod 4$, $3 +_4 3 +_4 3 \equiv 1 \bmod 4$, and $3 +_4 3 +_4 3 +_4 3 \equiv 0 \bmod 4$, so $\langle 3 \rangle = \mathbb{Z}_4 = \langle 1 \rangle$.

In general, 1 will always generate $\mathbb{Z}_n$, and the other generators will be the positive integers less than and relatively prime to n. □

Example 4.3.6 In Chapter 3, we made the comment that $\langle \mathbb{Z}_n, +_n \rangle$, $\langle \mathbb{Z}_n, \dot{+}_n \rangle$, and $\langle \overline{\mathbb{Z}}_n, \overline{+}_n \rangle$ are all isomorphic to each other. We have seen that $\langle \mathbb{Z}_n, \dot{+}_n \rangle$ and $\langle \overline{\mathbb{Z}}_n, \overline{+}_n \rangle$ both have order n, so by Theorem 4.3.3, each of the two groups is isomorphic to $\langle \mathbb{Z}_n, +_n \rangle$, and thus they are isomorphic to each other. □

Example 4.3.7 Recall that in Example 4.1.3, we showed that the n^{th} roots of unity form a group. We also mentioned that ζ^1 generates U_n for any $n \in \mathbb{N}$, so U_n is a cyclic group. □

Theorem 4.3.8 *A subgroup of a cyclic group is cyclic.*

Proof: Let $\langle a \rangle = G$ and let H be a subgroup of G. We must consider two cases.

Case 1: H is the trivial subgroup.

Clearly $H = \{e\} = \langle e \rangle$, so H is cyclic.

Case 2: H is non-trivial.

Since $H \neq \{e\}$, $G = \langle a \rangle$, and H is closed under taking inverses, there is some $n \in \mathbb{N}$ such that $a^n \in H$. Let m be the smallest such n.

We claim that $H = \langle a^m \rangle$, so we must show that every $h \in H$ is some power of a^m. Since $a^m \in H$, $\langle a^m \rangle \subseteq H$, thus we need only show that $H \subseteq \langle a^m \rangle$.

Let $h' \in H$. Since $H \leqslant G$, $h' \in G$ as well, so $h' = a^n$ for some $n \in \mathbb{N}$. By the division algorithm, $n = mq + r$ for some $q, r \in \mathbb{Z}$, where $0 \leqslant r < m$. Then

$$a^n = a^{mq+r} = a^{mq}a^r = (a^m)^q a^r.$$

But $a^n = (a^m)^q a^r \iff a^r = a^n(a^m)^{-q}$. Now, H is a group, and $a^n, a^m \in H$, so $(a^m)^{-q}$ and $a^n(a^m)^{-q}$ are both contained in H as well. Thus $a^r \in H$. But m was the smallest positive integer such that $a^m \in H$ and $0 \leqslant r < m$, so $r = 0$. Hence $n = mq$, and

$$h' = a^n = a^{mq} = (a^m)^q,$$

so h' is a power of a^m. It follows that H is cyclic. ∎

Example 4.3.9 Let $a, b \in \mathbb{Z}^+$ and consider $S = \{ar + bs : r, s \in \mathbb{Z}\}$. Clearly $S \subseteq \mathbb{Z}$, and if $r = 0$ and $s = 0$, then $0 \in S$, so S is nonempty and contains the additive identity. Also, for any $ar + bs \in S$, the element $-(ar + bs) \in S$ as well, so each element has a unique inverse in S. Closure under addition and the associative property come along for free from $\mathbb{Z}$, thus S is a subgroup of $\mathbb{Z}$, and by Theorem 4.3.8, S is cyclic. Hence, there is some $d \in S$ such that $\langle d \rangle = \{ar + bs : r, s \in \mathbb{Z}\}$. □

Definition 4.3.10 Let a and b be two positive integers. The positive generator d of the cyclic group $\langle d \rangle = \{ar + bs : r, s \in \mathbb{Z}\}$ under addition is called the

greatest common divisor of a and b. This will be denoted by $d = \gcd(a, b)$. If $d = 1$, then a and b are said to be *relatively prime*. $\diamondsuit$

We defined $\gcd(a, b)$ in Chapter 2. We state it as a theorem now, and prove that the two conditions must hold if $\gcd(a, b) = d$, for some d.

Theorem 4.3.11 *Let $a, b \in \mathbb{Z}^+$. Then $\gcd(a, b) = d$ if and only if*

1. *$d \mid a$ and $d \mid b$*

2. *if $c \mid a$ and $c \mid b$, then $c \mid d$.*

Proof: Suppose $\gcd(a, b) = d$. If $r = 1$ and $s = 0$, then $a \in \langle d \rangle$, so $d \mid a$. Similarly $d \mid b$.

Now suppose that $c \mid a$ and $c \mid b$. Then $cj = a$ and $ck = b$, for some $j, k \in \mathbb{Z}$. Since $d \in \langle d \rangle$, there exist $r, s \in \mathbb{Z}$ such that $d = ar + bs$, so

$$\begin{aligned} d &= ar + bs \\ &= cjr + cks && \text{(Substitution)} \\ &= c(jr + ks), && \text{(Distributive Property)} \end{aligned}$$

which implies that $c \mid d$ by definition of divides.

Finally, suppose that the two conditions hold. Then d is a common divisor of both a and b, and if c is another a common divisor of a and b, $c \mid d$. So we have $ck = d$, for some $k \in \mathbb{Z}$. Since c and d are both positive

by definition, and $k \neq 0$, this implies that $c \leqslant d$. Thus, if d satisfies both properties, it must be the greatest common divisor of a and b. ∎

Theorem 4.3.12 *If* $d \mid ab$ *and* $\gcd(a, d) = 1$*, then* $d \mid b$.

Proof: Since $\gcd(a, d) = 1$, there exist integers x and y such that $dx + ay = 1$, by Theorem 4.3.11. Multiplying this equation by b on both sides yields

$$
\begin{aligned}
& bdx + bay = b && \\
\iff & dbx + aby = b && \text{(Commutative Property)} \\
\iff & dbx + dky = b && (d \mid ab \iff dk = ab \text{ for some } k \in \mathbb{Z}) \\
\iff & d(bx + ky) = b. && \text{(Associativity Property)}
\end{aligned}
$$

Since the integers are closed under addition and multiplication, $bx + ky \in \mathbb{Z}$, so by the definition of divides, $d \mid b$. ∎

Lemma 4.3.13 *If* $\gcd(a, m) = 1$ *and* $a \equiv b \bmod m$*, then* $\gcd(b, m) = 1$.

Example 4.3.14 Let $a = 2$, $b = 11$, and $m = 9$. Then $\gcd(2, 9) = 1$ and $11 \equiv 2 \bmod 9$, as required. Since 11 is prime, $\gcd(11, 9) = 1$.

Now let $a = 6$, $b = 2$, and $m = 4$. Then $6 \equiv 2 \bmod 4$, but this time $\gcd(6, 4) = 2 \neq 1$, and $\gcd(2, 4) = 2 \neq 1$ as well. Thus, it is a necessary condition to have $\gcd(a, m) = 1$. □

Proof: Assume $\gcd(a, m) = 1$. Then there exist $x, y \in \mathbb{Z}$ such that $ax + my = 1$. Assume also that $a \equiv b \bmod m$. Then $a = b + km$ for some $k \in \mathbb{Z}$, and

$$\begin{aligned} & ax + my = 1 \\ \iff & (b + km)x + my = 1 && \text{(Substitution)} \\ \iff & bx + mkx + my = 1 && \text{(Distributive Property)} \\ \iff & bx + (kx + y)m = 1, && \text{(Distributive Property)} \end{aligned}$$

so $\gcd(b, m) = 1$, by Theorem 4.3.11. ∎

Definition 4.3.15 (Euler's φ-function) Let n be a positive integer. Then $\varphi(n)$ denotes the number of positive integers k such that $1 \leqslant k \leqslant n$ and $\gcd(k, n) = 1$. This φ is called *Euler's φ-function.* ♢

Example 4.3.16 Let $n = 6$. The positive integers a, such that $1 \leqslant a \leqslant 6$ and $\gcd(a, 6) = 1$ are 1 and 5, so $\varphi(6) = 2$.

Let $n = 7$. Since 7 is prime, every positive integer less than 7 is relatively prime to it, so $\varphi(7) = 6$. In general, if p is prime, $\varphi(p) = p - 1$. □

Example 4.3.17 Let $\mathbb{Z}_n^* = \{a : \gcd(a, n) = 1\}$. We claim that $\mathbb{Z}_n^*$ is a group under the operation multiplication modulo n. Suppose $a, b \in \mathbb{Z}_n^*$. Then we

have $ax_1 + ny_1 = 1$ and $bx_2 + ny_2 = 1$, by Theorem 4.3.11. Thus

$$
\begin{aligned}
& ax_1 \cdot bx_2 = 1 - ny_2 - ny_1 + n^2 y_1 y_2 && \text{(Multiply the equations together)} \\
\iff & ab(x_1 x_2) = 1 - n(y_1 + y_2 - ny_1 y_2) && \text{(Commutative, Distributive Laws)} \\
\iff & ab(x_1 x_2) + n(y_1 + y_2 - ny_1 y_2) = 1 && \text{(Arithmetic)} \\
\iff & \gcd(ab, n) = 1. && \text{(Theorem 4.3.11)}
\end{aligned}
$$

From the work above, we can see that $ab \in \mathbb{Z}_n^*$ whenever $a, b \in \mathbb{Z}_n^*$, so $\mathbb{Z}_n^*$ is closed under multiplication modulo n.

Clearly $\gcd(1, n) = 1$, so $1 \in \mathbb{Z}_n^*$, thus the multiplicative identity is an element of $\mathbb{Z}_n^*$.

Choose $a \in \mathbb{Z}_n^*$. Then $a \neq 0$, $\gcd(a, n) = 1$, and $ax + ny = 1$, for some $x, y \in \mathbb{Z}$. This implies that $ax = 1 - ny$, so $ax \equiv 1 \bmod n$. But $ax + ny = 1$ also implies that $\gcd(x, n) = 1$. Thus both x and a are relatively prime to n, so $x \in \mathbb{Z}_n^*$, and the multiplicative inverse of a is x.

Since each $a \in \mathbb{Z}_n^*$ is an integer, and the operation is ordinary multiplication modulo n, the associative property holds automatically, and it follows that $\langle \mathbb{Z}_n^*, \cdot \rangle$ is a group. Since every element in $\mathbb{Z}_n^*$ is less than and relatively prime to n, there are $\varphi(n)$ elements in $\mathbb{Z}_n^*$. We call $\mathbb{Z}_n^*$ the *group of units*. The order of the group of units is $\varphi(n)$.

In general, $\mathbb{Z}_n^*$ is not cyclic, although it is for certain values of n. For example, $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$ is not cyclic, since $3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \bmod 8$, so none

of the elements generate the entire group. On the other hand, $\mathbb{Z}_6^* = \{1, 5\}$ is cyclic, since $5^1 = 5$ and $5^2 \equiv 1 \bmod 6$. If p is prime, then $\mathbb{Z}_p^*$ is always a cyclic group [6]. □

Example 4.3.18 Suppose p is prime. Recall that the $(p-1)^{st}$ roots of unity are the $p-1$ solutions to the equation $x^{p-1} = 1$, and are the elements $\{1, \zeta^1, \ldots, \zeta^{p-2}\}$. We showed in Example 4.1.3 that $U_{p-1} = \{1, \zeta^1, \ldots, \zeta^{p-2}\}$ is a cyclic group. We also know from Example 4.3.17 that $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$ forms a cyclic group under multiplication modulo p, and thus there is some element γ that generates $\mathbb{Z}_p^*$. Both groups have $p-1$ elements, and Theorem 4.3.3 states that a finite cyclic group of order n is isomorphic to Z_n. Thus, U_{p-1} and $\mathbb{Z}_p^*$ are both isomorphic to $\mathbb{Z}_{p-1}$, so they are isomorphic to each other, and the map $\varphi : \mathbb{Z}_p^* \to U_{p-1}$ defined by $\varphi(\gamma^i) = \zeta^i$ is an isomorphism. □

Theorem 4.3.19 *If* $ac \equiv bc \bmod m$ *and* $\gcd(c, m) = d$, *then* $a \equiv b \bmod (m/d)$.

Proof: By definition of congruence, $m \mid (ac - bc) \iff m \mid c(a-b)$. Thus $mk = c(a-b)$ for some $k \in \mathbb{Z}$. Since $d \mid c$, $d \mid m$, and $d \neq 0$, we can divide both sides of the equation by d. This yields $(m/d)k = (c/d)(a-b)$, so $(m/d) \mid (c/d)(a-b)$. But $\gcd(c/d, m/d) = 1$, so $\frac{m}{d} \nmid \frac{c}{d}$, and $(m/d) \mid (a-b)$ by Theorem 4.3.12. It follows that $a \equiv b \bmod (m/d)$. ∎

Corollary 4.3.20 *If* $ac \equiv bc \bmod m$ *and* $\gcd(c, m) = 1$, *then* $a \equiv b \bmod m$.

Proof: This result follows immediately from Theorem 4.3.19. ∎

Theorem 4.3.21 *Let $a \in \mathbb{Z}$ and $n \in \mathbb{N}$. The following are equivalent.*

1. $\gcd(a, n) = 1$.

2. *a is a generator of $\mathbb{Z}_n$.*

3. *a has a multiplicative inverse modulo n.*

Proof: $\boxed{1 \Rightarrow 2}$ Assume that $\gcd(a, n) = 1$ and assume without loss of generality that $a < n$. Our goal is to show that each element in $\{a, 2a, \ldots, na\}$ is unique modulo n. Suppose that two of the elements are congruent modulo n. Then $ab \equiv ac \bmod n$, for some $b, c \in \{1, 2, \ldots, n\}$. By Corollary 4.3.20, $b \equiv c \bmod n$. But $1 \leqslant b, c \leqslant n$, which implies that $b = c$. Therefore, each of the least residues modulo n of $\{a, 2a, \ldots, na\}$ is unique. Since there are n such elements, they are a permutation of $\{0, 1, \ldots, n-1\}$, and it follows that a generates $\mathbb{Z}_n$.

$\boxed{2 \Rightarrow 3}$ Assume that a is a generator of $\mathbb{Z}_n$. Then $\langle a \rangle = \{0, 1, \ldots, n-1\}$, which implies that $ak \equiv 1 \bmod n$, for some $1 \leqslant k \leqslant n-1$, since $1 \in \langle a \rangle$. But $ak \equiv 1 \bmod n$ implies that a has a multiplicative inverse modulo n.

$\boxed{3 \Rightarrow 1}$ Assume that a has a multiplicative inverse modulo n. Then

$$
\begin{aligned}
& a \cdot a^{-1} \equiv 1 \bmod n \\
\iff & a \cdot a^{-1} = 1 + kn, \text{ for } k \in \mathbb{Z} && \text{(Definition of congruent)} \\
\iff & a \cdot a^{-1} - kn = 1 && \text{(Arithmetic)} \\
\iff & \gcd(a, n) = 1. && \text{(Theorem 4.3.11)}
\end{aligned}
$$

It follows that the three statements are equivalent. ∎

Lemma 4.3.22 *If* $\gcd(a, n) = 1$ *and* $r_1, r_2, \ldots, r_{\varphi(n)}$ *are the positive integers less than and relatively prime to* n*, then the least residues modulo* n *of* $ar_1, ar_2, \ldots, ar_{\varphi(n)}$ *are a permutation of* $r_1, r_2, \ldots, r_{\varphi(n)}$*.*

Proof: This is a direct consequence of the fact that $\mathbb{Z}_n^*$ is a group. The permutation is just one row of the group table, and as such, each element is unique. ∎

Theorem 4.3.23 (Fermat's Little Theorem) *If* p *is prime and* $\gcd(a, p) = 1$*, then*

$$a^{p-1} \equiv 1 \bmod p.$$

Proof: Suppose that $\gcd(a, p) = 1$ for some $a \in \mathbb{Z}$ and some prime p. Without loss of generality, assume that $a \in \mathbb{Z}_p^*$. If this is not the case, then $a = pq + r$ for some $q, r \in \mathbb{Z}$, which implies that $a \equiv r \bmod p$, and we can just work with r instead. Since the order of $\mathbb{Z}_p^*$ is $p - 1$, $a^{p-1} \equiv 1 \bmod p$. ∎

Example 4.3.24 Let $p = 3$ and $a = 8$. Then $\gcd(3, 8) = 1$. We want to examine a^{p-1} modulo p, so we have $8^{3-1} = 64 \equiv 1 \bmod 3$. The important things to note are that 3 is prime and 8 and 3 are relatively prime, which gives us the result we are looking for.

We repeat this example with $p = 2$ and $a = 8$. Again 2 is prime, but

now $\gcd(2, 8) = 2$ and $8^{2-1} = 8 \equiv 0 \bmod 2$. In this example, 2 and 8 are not relatively prime, and we do not get the desired result.

Now suppose $p = 9$ and $a = 2$. 9 is not prime, but $\gcd(9, 2) = 1$. This time $2^{9-1} = 256 \equiv 4 \bmod 9$. In this third example, 2 and 9 are relatively prime, but 9 is not prime, so the result is not 1. □

Corollary 4.3.25 *If p is prime, then $a^p \equiv a \bmod p$ for all a.*

Proof: If $a = 0$, then clearly $a^p \equiv 0 \bmod p$. Suppose that $a \neq 0$. If $\gcd(a, p) = 1$, then

$$a^{p-1} \equiv 1 \bmod p \qquad \text{(Fermat's Little Theorem)}$$

$$\iff a^p \equiv a \bmod p, \qquad \text{(Multiplication by } a\text{)}$$

as desired. ∎

Theorem 4.3.26 (Euler's Theorem) *Suppose $n \geqslant 1$ and $\gcd(a, n) = 1$. Then $a^{\varphi(n)} \equiv 1 \bmod n$.*

Proof: Let $a \in \mathbb{Z}$ such that $\gcd(a, n) = 1$. Then without loss of generality, $a \in \mathbb{Z}_n^*$. Since the order of $\mathbb{Z}_n^* = \varphi(n)$, $a^{\varphi(n)} \equiv 1 \bmod n$. ∎

Example 4.3.27 Let $a = 7$ and $n = 6$. Examination of $7^{\varphi(6)}$ modulo 6 yields $7^2 = 49 \equiv 1 \bmod 6$. □

Definition 4.3.28 Let $a \in \mathbb{Z}_n^*$. Then if $\langle a \rangle = \mathbb{Z}_n^*$, we say that a is a *primitive root of* n, and $\{a, a^2, \ldots, a^{\varphi(n)}\}$ is a permutation of $\mathbb{Z}_n^*$. ♢

Example 4.3.29 Recall that $\mathbb{Z}_n^*$ is the group of units, and the group operation is multiplication modulo n. The elements in $\mathbb{Z}_n^*$ are the elements that have a multiplicative inverse modulo n.

Consider $\mathbb{Z}_{19}^*$. Our goal is to find a generator of this group, if one exists.

k	1	2	3	4	5	6	7	8	9
$2^k \bmod 19$	2	4	8	16	13	7	14	9	18
k	10	11	12	13	14	15	16	17	18
$2^k \bmod 19$	17	15	11	3	6	12	5	10	1

It can easily be seen from the table that 2 generates every element of $\mathbb{Z}_{19}^*$, thus $\langle 2 \rangle = \mathbb{Z}_{19}^*$, so $\mathbb{Z}_{19}^*$ is a cyclic group. By similar calculations, the other generators of the group are 3, 10, 13, 14, and 15. Each of these generators is a primitive root of 19, by Definition 4.3.28. □

Note that there are six generators of $\mathbb{Z}_{19}^*$ and since $\mathbb{Z}_{19}^*$ contains eighteen elements, $\mathbb{Z}_{19}^* \cong \mathbb{Z}_{18}$, where $\mathbb{Z}_{18}$ has $\varphi(18) = 6$ generators.

Chapter 5

Ring Theory

Chapter 5 serves as a review of ring theory and examines at various properties of rings and fields. We begin with the definition of a ring and then provide a list of small definitions that pertain to rings. We give a more rigorous definition of prime in this section, and then examine the notion of irreducible. We define Unique Factorization Domains and then explore specific rings and fields. We conclude the first section with a proof of the Eisenstein Criterion that deals with reducibility of polynomials with integer coefficients over the rational numbers.

In Section 2, we define subrings and ideals, and then spend some time reviewing ring homomorphisms and isomorphisms. We look at the definitions of kernel and factor rings and then prove the Fundamental Homomorphism Theorem for rings. We wrap up the chapter with a look at prime and maximal

ideals and several related theorems.

Section 3 begins by defining a Euclidean domain and then looking at division algorithms for specific rings, before defining the Euclidean algorithm. We also establish the Euclidean algorithm for the ring of Gaussian integers, $\mathbb{Z}[i]$.

The fourth section is devoted to an in-depth examination of the ring of Eisenstein integers, $\mathbb{Z}[\omega]$. Because this ring plays such an important role in cubic reciprocity, it is crucial that we develop a solid foundation to use later. We define the specific complex conjugate for an Eisenstein integer and then define the norm in this setting. We develop a Euclidean algorithm for $\mathbb{Z}[\omega]$ as well, and then conclude the section with a theorem that establishes the six units in this ring.

The final section of Chapter 5 defines algebraic numbers and algebraic integers and then states a proposition that is given without proof in this thesis. We conclude with a theorem about algebraic integers that we will need later. Throughout this chapter, we have tried to tie examples back into previous work, to forge connections and develop content that will be used in the future.

5.1 Rings

Definition 5.1.1 A *ring* $\langle R, +, \cdot \rangle$ is a set R together with two binary operations, $+$ and $\cdot$, defined on R such that the following axioms are satisfied:

1. $\langle R, + \rangle$ is an abelian group.

2. Multiplication is associative.

3. For all $a, b, c \in R$,

   (a) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ (left distributive property), and

   (b) $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ (right distributive property). $\diamondsuit$

Example 5.1.2 Consider the set $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ together with the operations addition and multiplication modulo n. Recall that in Example 4.1.2, we showed that $\langle \mathbb{Z}_n, + \rangle$ was an abelian group. The associative and distributive properties hold when working in the integers under multiplication, so they hold in $\mathbb{Z}_n$ as well. Thus $\langle \mathbb{Z}_n, +, \cdot \rangle$ is a ring, where the operations are both modulo n. □

The following is a collection of small definitions concerning rings. They have been put together for the sake of organization and compactness.

Definition 5.1.3 Let R be a ring. The following definitions apply to R.

- R is a *commutative ring* if the multiplication in R is commutative.

- If R has a multiplicative identity element, then R is a *ring with unity* and the multiplicative identity element 1 is called *unity*. Note that 1 is just the notation for the identity.

- If $a, b \in R$ are both nonzero and $a \cdot b = 0$, then a and b are called *zero divisors* or *divisors of zero.*

- An *integral domain* is a commutative ring with unity $1 \neq 0$ containing no zero divisors.

- If R is a ring with unity $1 \neq 0$, an element $a \in R$ has a *multiplicative inverse* a^{-1} if there exists an $a^{-1} \in R$ such that $aa^{-1} = 1 = a^{-1}a$. If such an a^{-1} exists, it is unique.

- If R is a ring with unity $1 \neq 0$, an element $u \in R$ is a *unit* of R if it has a multiplicative inverse in R.

- If R is a ring, $a, b \in R$ are *associates* if $a = bu$, where u is a unit in R.

- If every nonzero element of an integral domain is a unit, then R is a *field.*

- If there exists a positive integer n, such that $n \cdot a = 0$ for all $a \in R$, then the least such positive integer is the *characteristic of* R. If no such n exists, then R is *characteristic* 0. ♢

Theorem 5.1.4 *Let R be a ring and let $a, b, c \in R$ with $a \neq 0$. Then the cancellation laws hold if and only if R contains no zero divisors.*

1. *If $ab = ac$, then $b = c$. (Left cancellation law)*

2. *If $ba = ca$, then $b = c$. (Right cancellation law)*

Proof: Suppose that the cancellation laws hold in R. Suppose also that $ab = 0$ for some $a, b \in R$. If $a \neq 0$, then $a \cdot b = a \cdot 0$ implies that $b = 0$. Likewise, if $b \neq 0$, then $a \cdot b = 0 \cdot b$ implies that $a = 0$. Thus, there are no zero divisors in R if the cancellation laws hold.

Suppose now that R contains no divisors of zero, and suppose also that $ab = ac$, where $a \neq 0$. Then

$$\begin{aligned} & ab = ac \\ \iff & ab - ac = 0 && \text{(Subtraction Property of Equality)} \\ \iff & a(b - c) = 0, && \text{(Distributive Property)} \end{aligned}$$

but $a \neq 0$ and R has no zero divisors, so $b - c = 0$, which implies that $b = c$.

Suppose that $ba = ca$, where $a \neq 0$. By a symmetric argument, we have $b - c = 0$, so again $b = c$. It follows that if R has no zero divisors, the cancellation laws hold. ∎

Probably the most familiar ring to most of us is $\mathbb{Z}$. Since multiplication is commutative in the integers, $\mathbb{Z}$ is a commutative ring. The integer 1 is the multiplicative identity, so the integers are a ring with unity 1. There are no zero divisors in the integers, so the cancellation laws hold. Thus by definition, the integers are an integral domain whose only units are 1 and -1. We will explore this idea a bit more with the following definitions and examples.

We are now in a position to offer a more rigorous definition of prime than the one that we have been using up to this point.

Definition 5.1.5 Suppose p is a nonzero nonunit element of an integral domain D. Then p is *prime* if for all $a, b \in D$, $p \mid ab$ implies that either $p \mid a$ or $p \mid b$. $\diamondsuit$

Definition 5.1.6 Let p be a nonzero nonunit element of an integral domain D. Then p is an *irreducible* of D if every factorization $p = ab$ in D has the property that either a or b is a unit. $\diamondsuit$

The definition of prime in this setting is a bit different from what we are used to, but the definition of irreducible probably looks familiar, as it is more like our "typical" definition of prime. Because primes are going to play a huge role in the reciprocity chapters of this thesis, it's very important that the notions of prime and irreducible are clear.

Definition 5.1.7 An integral domain D is a *unique factorization domain*, abbreviated UFD, if the following conditions are satisfied.

1. Every nonzero, nonunit element of D can be factored into a product of a finite number of irreducibles.

2. If $p_1 p_2 \dots p_r$ and $q_1 q_2 \dots q_s$ are two factorizations of the same element of D into irreducibles, then $r = s$ and the q_j can be renumbered so that p_i and q_i are associates. $\diamondsuit$

Example 5.1.8 Suppose p is a prime element in a unique factorization domain, D. Assume that $p = ab$, where $a, b \in D$. Then clearly $p \mid ab$, so either

$p \mid a$ or $p \mid b$. Without loss of generality, assume that $p \mid a$. Then $pk = a$ for some $k \in D$. Thus $p = ab = pkb$. Since D is a ring, the cancellation laws hold, thus $p = pkb$ implies that $1 = kb$, which implies that b is a unit. Thus p is irreducible, and it follows that if p is a prime element in a unique factorization domain, then p is irreducible. □

Example 5.1.9 Assume that D is a unique factorization domain and suppose p is irreducible in D. Let $a, b \in D$ and assume that $p \mid ab$. Then $pk = ab$ for some $k \in D$. Since D is a unique factorization domain, we can factor ab into a product of irreducibles, so $pk = p_1 p_2 \dots p_r q_1 q_2 \dots q_s u$, where u is a unit in D. But p is irreducible, so p is either one of the p_i or one of the q_j, which implies that $p \mid a$ or $p \mid b$, thus p is prime in D. It follows that if p is irreducible in a unique factorization domain, then p is prime. □

Recall that in Chapter 2, we stated the Fundamental Theorem of Arithmetic. Essentially it said that given any $a \in \mathbb{Z}$, where $a \neq \pm 1$, $a = p_1 p_2 \dots p_k$ is the unique product of prime numbers, up to ordering and multiplication by ± 1. Now that we have seen that prime implies irreducible in a unique factorization domain, this could be restated. If a is a nonzero, nonunit element in a ring, R, then $a = p_1 p_2 \dots p_k$ is the unique product of irreducibles. In each of the unique factorization domains that we will be working in throughout this thesis, primes and irreducibles will be the same.

Example 5.1.10 Let a, b, c be elements in a unique factorization domain, D.

Assume that a is irreducible and suppose that $a \mid bc$. Then there exists $k \in D$, such that $ak = bc$. Let $b = p_1 p_2 \dots p_m$, $c = q_1 q_2 \dots q_n$, and $k = r_1 r_2 \dots r_l$ be the prime factorizations of b, c, and k. Then $a \prod_{i=1}^{l} r_i = \prod_{i=1}^{m} p_i \prod_{i=1}^{n} q_i$.

Now each side of the equation is a product of irreducibles in D. Since factorization in D is unique, a (or a unit multiple of a) must be one of the irreducible factors on the right hand side of the equation. Thus $a \mid b$ or $a \mid c$, and a is prime. Hence, if a is an irreducible element in a unique factorization domain, then a is prime. □

Example 5.1.11 Let $a \in \mathbb{Z}$, such that $a \neq \pm 1$. Then by the Fundamental Theorem of Arithmetic, $a = p_1 p_2 \dots p_k$ is the unique product of k irreducibles. Since a was chosen arbitrarily, this result holds for any such $a \in \mathbb{Z}$. Thus the integers are a unique factorization domain, by definition. □

Theorem 5.1.12 *In the ring $\mathbb{Z}_n$, the divisors of zero are precisely the nonzero elements that are not relatively prime to n.*

Proof: Let $a \in \mathbb{Z}_n$, with $a \neq 0$. Suppose first that $\gcd(a, n) = d$, where $d \neq 1$. Then

$$\frac{an}{d} = \frac{an}{d} \qquad \text{(Identity)}$$

$$\iff a\left(\frac{n}{d}\right) = \left(\frac{a}{d}\right) n \qquad \text{(Associative Property)}$$

$$\iff a\left(\frac{n}{d}\right) \equiv 0 \bmod n. \qquad \text{(Example 3.0.5)}$$

But $a \neq 0$ and $\frac{n}{d} \neq 0$ since n is nonzero, therefore a is a zero divisor in $\mathbb{Z}_n$.

Suppose now that $a \in \mathbb{Z}_n$ and $\gcd(a, n) = 1$. If there is $b \in \mathbb{Z}_n$ such that $ab \equiv 0 \mod n$, then $n \mid ab$. Since $\gcd(a, n) = 1$, we have $n \mid b$ by Theorem 4.3.12. But $b \in \{0, 1, \ldots, n-1\}$, so $b = 0$, thus a is not a zero divisor in $\mathbb{Z}_n$. ∎

Recall that Theorem 4.3.21 states that $\gcd(a, n) = 1$ if and only if a has a multiplicative inverse. We know that if a has a multiplicative inverse in a ring, then a is a unit. Thus the units in a ring can not be zero divisors.

Example 5.1.13 Let p be a prime and consider $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$. Certainly $\langle \mathbb{Z}_p, +, \cdot \rangle$ is a ring, and since the elements are integers, the multiplication is commutative and the multiplicative identity is the usual integer 1. The elements in $\mathbb{Z}_p$ are all less than and relatively prime to p, so by Theorem 5.1.12 $\mathbb{Z}_p$ can contain no zero divisors. Thus $\mathbb{Z}_p$ is an integral domain by definition. For any $a \neq 0 \in \mathbb{Z}_p$, $\gcd(a, p) = 1$, so by Theorem 4.3.21, a has a multiplicative inverse. But since we chose a arbitrarily, every nonzero element of $\mathbb{Z}_p$ has a multiplicative inverse and thus is a unit. It follows that for any prime p, $\mathbb{Z}_p$ is a field. □

Corollary 5.1.14 *If p is prime, then $\mathbb{Z}_p$ has no zero divisors.*

Proof: This result follows immediately from Example 5.1.13. ∎

We are going to do a fair bit of work with fields in general, but we

will also need to use the rational numbers, so we use the following example to establish that $\mathbb{Q}$ is a field.

Note that the rational numbers, $\mathbb{Q}$, the real numbers, $\mathbb{R}$, and the complex numbers, $\mathbb{C}$ are all fields that we are familiar with.

Example 5.1.15 Recall that in Example 4.1.4, we proved that the Gaussian Integers, $\mathbb{Z}[i] \subseteq \mathbb{C}$ form an abelian group. Since multiplication is associative in $\mathbb{C}$ and the distributive laws hold in $\mathbb{C}$, both hold in $\mathbb{Z}[i]$ as well, and it follows that $\mathbb{Z}[i]$ is a ring.

If we look at $\mathbb{Q}[i]$ instead, then the elements are of the form $\frac{a}{b} + \frac{c}{d}i$, where $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$. This set is also a subset of the complex numbers, and as such, all of the properties of $\mathbb{C}$ hold. Thus $\mathbb{Q}[i]$, the Gaussian Rationals, is a ring under complex addition and multiplication.

Similarly, we saw in Example 4.1.6 that the Eisenstein Integers, $\mathbb{Z}[\omega]$, form an abelian group under addition. It is easy to see that $\mathbb{Z}[\omega]$ is closed under multiplication, since $\omega^2 = -1 - \omega$. Again, this is a subset of $\mathbb{C}$, so it also forms a ring.

If we consider $\mathbb{Q}[\omega]$, where the elements are of the form $\frac{a}{b} + \frac{c}{d}\omega$, with $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$, then we have a ring under complex addition and multiplication, and we call this ring the Eisenstein Rationals. □

5.1.1 Rings of Polynomials

Let $\mathbb{F}$ be a field. Then $\mathbb{F}[x]$ is the set of all polynomials in x with coefficients from the field $\mathbb{F}$. For example, $\frac{1}{2}x^2 - 2x + \frac{3}{4}$ and $x^3 + 5x^2 + 2x + 7$ are both contained in $\mathbb{Q}[x]$. Since $\mathbb{Q}$ is an abelian group under addition and addition of polynomials is commutative, $\mathbb{Q}[x]$ is abelian under polynomial addition. We know from experience that polynomial multiplication is associative and that the distributive laws hold when working with polynomials, thus $\mathbb{Q}[x]$ forms a ring. The fact that $\mathbb{Q}[x]$ is a ring isn't unique to $\mathbb{Q}$, and in fact $\mathbb{F}[x]$ forms a ring for any field $\mathbb{F}$.

We are going to work with rings of polynomials to establish some results that will be useful later.

Theorem 5.1.16 *If $f(x) \in \mathbb{F}[x]$ is a polynomial of degree n, then $f(x) = 0$ has at most n roots.*

Example 5.1.17 Let $f(x) = x^2 + 2x - 15$. Then $f(x) \in \mathbb{Q}[x]$. Using basic algebra to factor $f(x)$ yields $f(x) = (x - 3)(x + 5)$. Thus

$$x^2 + 2x - 15 = 0$$

$$\iff (x - 3)(x + 5) = 0.$$

But there are no zero divisors in $\mathbb{Q}$, so either $x - 3 = 0$ or $x + 5 = 0$. The first equation yields $x = 3$, and the second yields $x = 5$. There are no other solutions. □

Proof: Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a degree n polynomial in $\mathbb{F}[x]$. We use induction on n.

Suppose $n = 1$. Then $f(x) = a_1 x + a_0 = 0$ has exactly one solution, namely $x = -\dfrac{a_0}{a_1}$, which is unique by properties of $\mathbb{F}$.

Assume that the result holds for polynomials of degree $n-1$ and suppose that $f(x)$ is a degree n polynomial. There are two possibilities, either $f(x) = 0$ has no solution, or it has at least one solution.

Suppose first that $f(x) = 0$ has no solution. Then the result holds, since $0 < n$.

Suppose next that $f(x) = 0$ has at least one solution, and call it r. Then $(x - r)$ is a factor of $f(x)$, so $f(x) = (x - r) \cdot g(x) = 0$, where $g(x)$ is a polynomial of degree $n - 1$. By our inductive assumption, $g(x) = 0$ has at most $n - 1$ solutions, and $x - r = 0$ has exactly one solution. It follows that $f(x) = 0$ has at most n solutions. ∎

Proposition 5.1.18 (Division Algorithm for Polynomials in $\mathbb{F}[x]$) *Let $f(x)$ and $g(x)$ be two polynomials in $\mathbb{F}[x]$, where the degree of $g(x)$ is greater than 0. Then there are unique polynomials $q(x)$ and $r(x)$ in $\mathbb{F}[x]$, such that $f(x) = g(x) \cdot q(x) + r(x)$, where either $r(x) = 0$ or the degree of $r(x)$ is less than the degree of $g(x)$.*

This proof is omitted here, but it can be found in [6].

Definition 5.1.19 A nonconstant polynomial $f(x) \in \mathbb{F}[x]$ is *irreducible over*

$\mathbb{F}$, or is an *irreducible polynomial in* $\mathbb{F}[x]$, if $f(x)$ cannot be expressed as a product $g(x) \cdot h(x)$ of two polynomials $g(x)$ and $h(x)$ in $\mathbb{F}[x]$ both of lower degree than the degree of $f(x)$. If $f(x) \in \mathbb{F}[x]$ is a nonconstant polynomial that is not irreducible over $\mathbb{F}$, then $f(x)$ is *reducible over* $\mathbb{F}$. $\diamondsuit$

Note that this definition of irreducible polynomial is analogous to the definition of irreducible element, since the constant polynomials are the units in $\mathbb{F}[x]$.

Example 5.1.20 Let $f(x) = x^2 + 1 \in \mathbb{Q}[x]$. We know that one factorization of this polynomial is $x^2 + 1 = (x - i)(x + i)$, but we want to establish that this factorization is unique. Suppose $x^2 + 1 = (x - r)(x - s)$ for some r, s. Observe that

$$\begin{aligned} x^2 + 1 &= (x - r)(x - s), \text{ for some } r, s \\ &= x^2 - (r + s)x + rs. \end{aligned}$$

But there is no x term in $x^2 + 1$, which implies that $r + s = 0$, and thus $r = -s$. We also know that $rs = 1$, so combining these results implies that

$$\begin{aligned} & rs = 1 \\ \iff & -r^2 = 1 && (s = -r) \\ \iff & r^2 = -1 && \text{(Multiplication Property of Equality)} \\ \iff & r = \pm i. && \text{(Square Root Property)} \end{aligned}$$

So in this instance, $x^2 + 1 = (x - i)(x + i)$ is a unique factorization in $\mathbb{C}[x]$. Since $i, -i \notin \mathbb{Q}$, $x^2 + 1$ is irreducible in $\mathbb{Q}[x]$. □

Proposition 5.1.21 *If $\mathbb{F}$ is a field and $f(x) \in \mathbb{F}[x]$, then $f(x)$ factors uniquely in $\mathbb{F}[x]$.*

This proof is omitted here, but it can be found in [6].

Example 5.1.22 Let $f(x) = x^3 - 1 \in \mathbb{Q}[x]$. We can use the difference of cubes factoring method to come up with $f(x) = (x - 1)(x^2 + x + 1)$. Thus $f(x)$ is reducible over $\mathbb{Q}$ by definition, and this factorization is unique by Proposition 5.1.21.

Now we want to examine the second polynomial factor from above, so let $g(x) = x^2+x+1 \in \mathbb{Q}[x]$. This factors as $g(x) = (x-\omega)(x-\omega^2)$, which is also unique, and is thus irreducible over $\mathbb{Q}$, since the complex numbers $\omega, \omega^2 \notin \mathbb{Q}$. Recall that we previously defined ω to be the cube root of unity, or a root of the equation $x^3 = 1$. □

Proposition 5.1.23 *Let $f(x) \in \mathbb{Z}[x]$. Then $f(x)$ is reducible in $\mathbb{Z}[x]$ if and only if it is reducible in $\mathbb{Q}[x]$.*

This is stated without proof in this thesis, but the proof can be found in [6].

Example 5.1.24 If we refer to $f(x) = x^2 + 1$ from Example 5.1.20, we know

already that it is irreducible over the rationals, but $i, -i \notin \mathbb{Z}$, so it is also irreducible over the integers. □

Theorem 5.1.25 (Eisenstein Criterion) *Let p be a prime. Suppose that $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + ax + a_0 \in \mathbb{Z}[x]$, where*

- $a_n \not\equiv 0 \bmod p$
- $a_i \equiv 0 \bmod p$ *for all* $0 < i < n$
- $a_0 \not\equiv 0 \bmod p^2$.

Then $f(x)$ is irreducible over $\mathbb{Q}$.

Example 5.1.26 Let $p = 5$ and let $f(x) = x^3 - 5$. Then if we examine the coefficients, $1 \not\equiv 0 \bmod 5$, $-5 \equiv 0 \bmod 5$, and $-5 \not\equiv 0 \bmod 25$. Clearly $\sqrt[3]{5}$ is one root of $f(x)$, so $x - \sqrt[3]{5}$ is a factor. Polynomial long division reveals that we can factor $f(x)$ as

$$f(x) = \left(x - \sqrt[3]{5}\right)\left(x^2 + \sqrt[3]{5}x + \sqrt[3]{25}\right),$$

and we could then use the quadratic formula on the second factor. However, it's clear that none of the coefficients are rational, thus $f(x)$ is reducible over the irrationals, but is irreducible over $\mathbb{Q}$. □

Proof: Let p be prime. Suppose that $f(x) = a_n x^n + \ldots ax + a_0 \in \mathbb{Z}[x]$ is a polynomial such that $a_n \not\equiv 0 \bmod p$, $a_0 \not\equiv 0 \bmod p^2$, and each $a_i \equiv 0 \bmod p$,

for $0 < i < n$. By Proposition 5.1.23, if $f(x)$ is reducible in $\mathbb{Q}[x]$, it is also reducible in $\mathbb{Z}[x]$, so by contraposition, it is sufficient to show that $f(x)$ is irreducible in $\mathbb{Z}[x]$.

Assume that $f(x)$ is reducible in $\mathbb{Z}[x]$ into nontrivial factors, and let $f(x) = g(x) \cdot h(x)$ be that factorization. Let $g(x) = b_r x^r + \cdots + b_0$ and $h(x) = c_s x^s + \cdots + c_0$. Then we know that $b_r, c_s \neq 0$, $r + s = n$, and neither $r = 0$ nor $s = 0$, so $0 < r, s < n$. But $a_0 \neq 0 \bmod p^2$, which implies that $b_0 \equiv 0 \bmod p$ and $c_0 \equiv 0 \bmod p$ are not both true, since $a_0 = b_0 \cdot c_0$.

Suppose without loss of generality that $b_0 \not\equiv 0 \bmod p$ and $c_0 \equiv 0 \bmod p$. We know that $a_n \not\equiv 0 \bmod p$, so it must be the case that $b_r \not\equiv 0 \bmod p$ and $c_s \not\equiv 0 \bmod p$, since $a_n = b_r \cdot c_s$. Let m be the smallest value of i such that $c_i \not\equiv 0 \bmod p$. Then if we examine a_m, we have

$$a_m = b_0 c_m + b_1 c_{m-1} + \cdots + \begin{cases} b_m c_0, & \text{if } r \geqslant m \\ b_r c_{m-r}, & \text{if } r < m. \end{cases}$$

Recall that $b_0 \not\equiv 0 \bmod p$ and $c_m \not\equiv 0 \bmod p$, so $a_m \not\equiv 0 \bmod p$, since $c_{m-1}, \ldots, c_0 \equiv 0 \bmod p$. But $a_i \equiv 0 \bmod p$ for $0 < i < n$, so it must be the case that $m = n$. This forces $s = n$ as well, because m was the smallest i for which $c_i \not\equiv 0 \bmod p$, which contradicts the fact that $s < n$. It follows that our assumption that $f(x)$ is reducible into nontrivial factors in $\mathbb{Z}[x]$ must have been false, and thus $f(x)$ is irreducible over $\mathbb{Z}$. Hence, by Proposition 5.1.23, $f(x)$ is also irreducible over $\mathbb{Q}$. ∎

Lemma 5.1.27 *Let $\mathbb{F}$ be a field and let $f(x) \in \mathbb{F}[x]$. If $c \in \mathbb{F}$ and $f(x+c)$ is irreducible in $\mathbb{F}[x]$, then $f(x)$ is irreducible in $\mathbb{F}[x]$.*

Proof: Suppose $f(x) \in \mathbb{F}[x]$ is reducible over $\mathbb{F}$. Then there exist polynomials $g(x), h(x) \in \mathbb{F}[x]$, such that $f(x) = g(x) \cdot h(x)$. This also means that $f(x+c) = g(x+c) \cdot h(x+c)$, where $g(x+c)$ and $h(x+c)$ have the same degrees as $g(x)$ and $h(x)$, respectively. Thus, $g(x+c)$ and $h(x+c)$ are both nontrivial polynomials, so $f(x+c)$ is reducible over $\mathbb{F}$ whenever $f(x)$ is. Thus, by contraposition, it follows that if $f(x+c)$ is irreducible over $\mathbb{F}$, then $f(x)$ is irreducible over $\mathbb{F}$. ∎

We see this Lemma at work in the proof of the following theorem.

Theorem 5.1.28 *Let p be prime. Then the polynomial*

$$f(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

is irreducible over $\mathbb{Q}$.

Proof: By Proposition 5.1.23, it is sufficient to show that $f(x)$ is irreducible over $\mathbb{Z}$. Consider $f(x+1)$.

$$\begin{aligned} f(x+1) &= \frac{(x+1)^p - 1}{(x+1) - 1} && \text{(Substitution)} \\ &= \frac{(x^p + px^{p-1} + \cdots + px + 1) - 1}{x} && \text{(Binomial Expansion Theorem)} \\ &= x^{p-1} + px^{p-2} + \cdots + p. && \text{(Polynomial division)} \end{aligned}$$

Recall that by the Binomial Expansion Theorem, the coefficients of every term in the final polynomial above are of the form

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p \cdot (p-1)!}{k!(p-k)!} = p \cdot \frac{(p-1)!}{k!(p-k)!},$$

which implies that p divides every coefficient except the first one, which is 1. So since $1 \not\equiv 0 \bmod p$ and $p \not\equiv 0 \bmod p^2$, the conditions are met to apply Eisenstein's Criterion. Thus $f(x+1)$ is irreducible over $\mathbb{Q}$, and by Lemma 5.1.27, $f(x)$ is irreducible over $\mathbb{Q}$ as well. ∎

Recall from our work with roots of unity that ω, the cube root of unity, is a root of $p(x) = x^3 - 1$. In fact, the three roots of this polynomial are ω, ω^2, and 1. In the theorem, we started with the polynomial $q(x) = x^p - 1$, which has the p^{th} root of unity as one of its roots. In fact, the p roots are $1, \zeta^{p-1}, \zeta^{p-2}, \ldots,$ and ζ, where ζ is the p^{th} root of unity.

After dividing $x^p - 1$ by $x - 1$, we are left with $f(x) = x^{p-1} + \cdots + x + 1$, which has $\zeta^{p-1}, \zeta^{p-2}, \ldots,$ and ζ as its roots. Since each of these is a complex number, it should make sense that this polynomial is not reducible over $\mathbb{Q}$.

5.2 Subrings and Ideals

Definition 5.2.1 Let R be a ring whose binary operations are $+$ and $\cdot$. Let H be a subset of R. Then H is a *subring* of R if the following properties hold.

1. $\langle H, + \rangle$ is an abelian group.

2. If $a, b, c \in H$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

3. For all $a, b, c \in H$,

   $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ (Left Distributive Law) and

   $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ (Right Distributive Law). $\diamondsuit$

In general, to prove that H is a subring of R, it is only necessary to show that H is closed under addition and multiplication, and that H is an abelian group under addition. The associative and distributive laws hold from the ring R.

Recall that in Definition 4.2.11, we introduced homomorphisms and isomorphisms. The definition deliberately referred to algebraic binary structures in general, because these morphisms apply to rings as well as groups. The only real difference between homomorphisms of groups and rings is that when working with rings, the homomorphism property must hold under multiplication as well as addition. In other words, for all $a, b \in R$, $\varphi(a+b) = \varphi(a)+\varphi(b)$ and $\varphi(ab) = \varphi(a)\varphi(b)$.

We previously showed that $\mathbb{Z}_n$ is a ring under the operations addition and multiplication modulo n. We now revisit the function LR_n that was introduced earlier.

Example 5.2.2 Recall the function LR_n that was defined in Chapter 3. We said that $\mathrm{LR}_n : \mathbb{Z} \to \mathbb{Z}_n$, where $\mathrm{LR}_n(a) = r$ and r is the remainder left upon

division of a by n. We saw previously that for $a, b \in \mathbb{Z}$,

$$\mathrm{LR}_n(a+b) = \mathrm{LR}_n(a) +_n \mathrm{LR}_n(b).$$

Let $a = nq_1 + r_1$ and $b = nq_2 + r_2$, by the division algorithm for integers. Then $ab = n(nq_1q_2 + q_1r_2 + q_2r_1) + r_1r_2$, so

$$\begin{aligned}
\mathrm{LR}_n(ab) &= \mathrm{LR}_n(r_1r_2) && \text{(Definition of } \mathrm{LR}_n\text{)} \\
&= \mathrm{LR}_n\big(\mathrm{LR}_n(a)\mathrm{LR}_n(b)\big) && \text{(Substitution)} \\
&= \mathrm{LR}_n(a) \cdot_n \mathrm{LR}_n(b), && \text{(Definition of } \mathrm{LR}_n\text{)}
\end{aligned}$$

which is in $\mathbb{Z}_n$. Thus $\mathrm{LR}_n : \mathbb{Z} \to \mathbb{Z}_n$ is a ring homomorphism. □

Theorem 5.2.3 *Let H be a subring of the ring R. Multiplication of additive cosets of H is well defined by the equations*

$$(a+H)(b+H) = ab + H \text{ and } (H+a)(H+b) = H + ab$$

if and only if $ah, hb \in H$ for all $a, b \in R$ and $h \in H$.

Proof: Suppose first that multiplication of additive cosets of H is well defined by the given equations. Let $a \in R$ and consider the coset product $(a+H)(0+H)$. If we take $a \in (a+H)$ and $0 \in (0+H)$, we have

$$\begin{aligned}
(a+H)(0+H) &= a0 + aH + H0 + HH && \text{(Substitution)} \\
&= 0 + H && (H \text{ is closed}) \\
&= H. && \text{(Additive Identity)}
\end{aligned}$$

If we choose $h \in H$ instead of 0, then

$$(a + H)(h + H) = ah + aH + Hh + HH = ah + H,$$

so $ah \in H$ for all $h \in H$, since multiplication is well defined. A similar argument using $(0 + H)(b + H)$ shows that $hb \in H$ for all $h \in H$.

Suppose that $ah, hb \in H$ for all $a, b \in R$ and all $h \in H$. Let $h_1, h_2 \in H$. Then $a + h_1$ and $b + h_2$ are representatives of the cosets $a + H$ and $b + H$ containing a and b respectively. Multiplying these representatives together yields

$$(a + h_1)(b + h_2) = ab + ah_2 + h_1b + h_1h_2.$$

But $ah_2 \in H$, $h_1b \in H$, and $h_1h_2 \in H$, so $(a + h_1)(b + h_2) \in ab + H$. By a symmetric argument, $(h_1 + a)(h_2 + b) \in H + ab$. Thus multiplication of additive cosets is well defined when H is a subring of R. ∎

Definition 5.2.4 An additive subgroup N of a ring R satisfying the properties

$$aN \subseteq N \text{ and } Nb \subseteq N \text{ for all } a, b \in R$$

is called an *ideal*. ♢

This definition of an ideal means that we could reword Theorem 5.2.3 to state that multiplication of additive cosets of H is well defined if and only if H is an ideal.

Example 5.2.5 $\mathbb{Z}_8$ forms a ring, and $H = \{0, 2, 4, 6\}$ is a subgroup of $\mathbb{Z}_8$ under addition modulo 8, by Example 4.2.2. Suppose $a \in \mathbb{Z}_8$ and $b \in H$. Then ab is even, since b is, so $ab \in H$. Similarly, $ba \in H$, so H is an ideal of $\mathbb{Z}_8$. □

Definition 5.2.6 Let $\varphi : R \to R'$ be a ring homomorphism. The subring

$$\varphi^{-1}[0'] = \{r \in R : \varphi(r) = 0'\} = \ker(\varphi)$$

is called the *kernel* of φ. ♢

The kernel of any homomorphism is just the set of all elements in the first structure that get mapped to the additive identity of the second structure.

Example 5.2.7 Consider the ring homomorphism $\mathrm{LR}_n : \mathbb{Z} \to \mathbb{Z}_n$. By the definition of kernel, $\ker(\mathrm{LR}_n) = \{a \in \mathbb{Z} : \varphi(a) = 0\}$. Recall that $\mathbb{Z}_n$, contains only the elements $\{0, 1, \ldots, n-1\}$, so all of the integers that are multiples of n are equivalent to 0 modulo n. Thus $\ker(\mathrm{LR}_n) = \{kn : k \in \mathbb{Z}\}$. □

Being able to work with the kernel of a homomorphism can be very handy at times. It can sometimes be tricky to show that a homomorphism is one-to-one, but showing that the kernel contains only the identity element is another way to establish one-to-oneness.

Theorem 5.2.8 *Let N be an ideal of a ring R. Then $\gamma : R \to R/N$ given by $\gamma(x) = x + N$ is a ring homomorphism and* $\ker(\gamma) = N$.

Proof: γ is a function, so we need only show that it is also a homomorphism.

$$\begin{aligned}
\gamma(r+s) &= (r+s)+N && \text{(Definition of } \gamma\text{)} \\
&= (r+N)+(s+N) && \text{(Addition of cosets)} \\
&= \gamma(r)+\gamma(s) && \text{(Definition of } \gamma\text{)}
\end{aligned}$$

and

$$\begin{aligned}
\gamma(rs) &= (rs)+N && \text{(Definition of } \gamma\text{)} \\
&= (r+N)(s+N) && \text{(Multiplication of cosets)} \\
&= \gamma(r)\gamma(s). && \text{(Definition of } \gamma\text{)}
\end{aligned}$$

Thus the homomorphism property holds for both addition and multiplication, and it follows that γ is a homomorphism. Since $N = [0]$ and homomorphisms always map identity elements to identity elements, clearly $\ker(\gamma) = N$. ∎

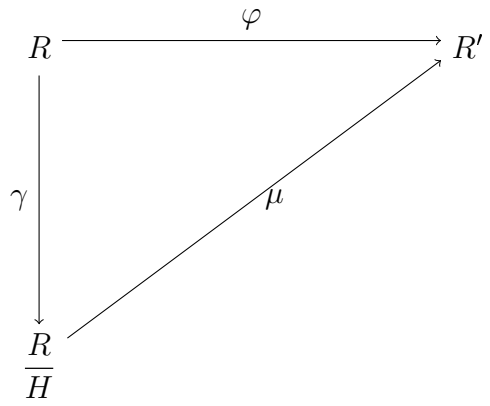
Theorem 5.2.9 (Fundamental Homomorphism Theorem) *Suppose that $\varphi : R \to R'$ is a ring homomorphism with $\ker(\varphi) = H$. Then the additive cosets of H form the factor ring R/H whose binary operations are defined by choosing representatives. That is, the sum of two cosets is defined by*

$$(a+H)+(b+H) = (a+b)+H,$$

and the product of two cosets is defined by

$$(a+H)(b+H) = (ab)+H.$$

The map $\mu : R/H \to \varphi[R]$ *defined by* $\mu(a + H) = \varphi(a)$ *is an isomorphism and if* $\gamma : R \to R/H$ *is the homomorphism given by* $\gamma(r) = r + H$*, then* $\varphi(r) = \mu\gamma(r)$ *for each* $r \in R$*.*



Proof: Let $h_1, h_2 \in H$. Consider $(a+h_1) \in a+H$ and $(b+h_2) \in b+H$.

$$(a + h_1) + (b + h_2) = (a + b) + (h_1 + h_2).$$

We know from group theory that addition is well defined if and only if $\langle H, + \rangle$ is abelian, which we have by definition. Also, we know from Theorem 5.2.3 that coset multiplication is well defined if and only if H is an ideal. Thus it is sufficient to show that $\ker(\varphi) = H$ is an ideal of R.

Let $a \in \ker(\varphi)$ and $r \in R$. Then we know that $\varphi(a) = 0$, and we need to show that $ra \in \ker(\varphi)$.

$$\begin{aligned} \varphi(ra) &= \varphi(r)\varphi(a) && \text{(Homomorphism Property)} \\ &= \varphi(r) \cdot 0' && (a \in \ker(\varphi)) \\ &= 0', \end{aligned}$$

so $ra \in \ker(\varphi)$ as required, and $\ker(\varphi)$ is an ideal, so coset multiplication is well defined.

It remains to show that R/H is a ring. We've already shown that R/H is closed under addition and multiplication, and since $\langle R, + \rangle$ is an abelian group, $\langle R/H, + \rangle$ is as well. Thus, we need only show that multiplication is associative and that the left and right distributive laws hold.

Let $a, b, c \in R$ and $h_1, h_2, h_3 \in H$. Then

$$\begin{aligned}
&\big((a + h_1)(b + h_2)\big)(c + h_3) \\
&= (ab + ah_2 + h_1 b + h_1 h_2)(c + h_3) && \text{(Distributive Property)} \\
&= abc + abh_3 + ah_2 c + ah_2 h_3 + h_1 bc + h_1 bh_3 + h_1 h_2 c + h_1 h_2 h_3 \\
& && \text{(Distributive Property)} \\
&= (a + h_1)(bc + bh_3 + h_2 c + h_2 h_3) && \text{(Distributive Property)} \\
&= (a + h_1)\big((b + h_2)(c + h_3)\big), && \text{(Distributive Property)}
\end{aligned}$$

and multiplication is associative.

Finally, for $a, b, c \in R$ and $h_1, h_2, h_3 \in H$, we have

$$\begin{aligned}
&(a + h_1)\big((b + h_2) + (c + h_3)\big) \\
&= (a + h_1)(b + c + h_2 + h_3) \\
&= ab + ac + ah_2 + ah_3 + h_1 b + h_1 c + h_1 h_2 + h_1 h_3 && \text{(Distributive Property)} \\
&= ab + ah_2 + h_1 b + h_1 h_2 + ac + ah_3 + h_1 c + h_1 h_3 && \text{(Commutativity)} \\
&= (a + h_1)(b + h_2) + (a + h_1)(c + h_3), && \text{(Distributive Property)}
\end{aligned}$$

so the left distributive law holds. A similar calculation shows that the right distributive law holds as well, and it follows that R/H is a ring, as desired.

Now we need to examine the map μ that is described in the hypothesis. We have $\mu : R/H \to \varphi[R]$ defined by $\mu(a + H) = \varphi(a)$. This is everywhere defined by the given map, so suppose $(a + H) = (b + H)$. From group theory, we know that $(a + H) = \{x : \varphi(x) = \varphi(a)\} = [a]$. So since the cosets $[a]$ and $[b]$ are equal, $b \in (a + H)$. Now, $\mu\big([a]\big) = \varphi(a)$ and $\mu\big([b]\big) = \varphi(b)$, and since $b \in (a + H)$, $\varphi(b) = \varphi(a)$, so μ is uniquely defined, and is thus well defined.

We need to show that the homomorphism properties hold for μ. Suppose $a, b \in R$. Then

$$\mu(a + b) = \varphi(a + b) = \varphi(a) + \varphi(b) = \mu(a) + \mu(b)$$

and

$$\mu(ab) = \varphi(ab) = \varphi(a)\varphi(b) = \mu(a)\mu(b),$$

so μ is a ring homomorphism.

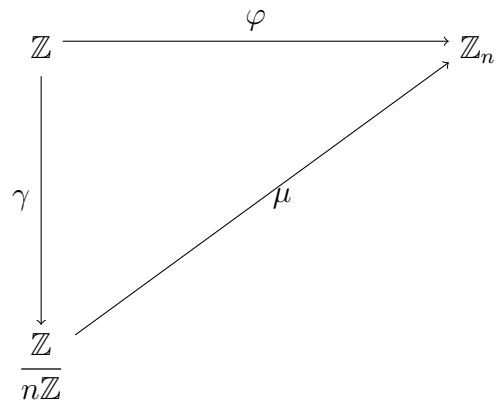
To show that μ is one-to-one, we will examine $\ker(\mu)$. Suppose that for some $[a] \in R/H$, $\mu\big([a]\big) = 0$. Then

$$\begin{aligned} & \mu\big([a]\big) = 0 \\ \iff & \varphi(a) = 0 && \text{(Definition of } \mu) \\ \iff & a \in H && \text{(Definition of } \ker(\varphi)) \end{aligned}$$

But $[a]$ is the zero coset when $a \in H$, so $[a]$ is the identity in R/H, and μ is one-to-one.

To show that μ is also onto, let $\varphi(r)$ be an arbitrary element in $\varphi[R]$. Then $r + H \in R/H$ and $\mu(r + H) = \varphi(r)$ by the definition of μ, so μ is onto. It follows that μ is an isomorphism as desired. By Theorem 5.2.8, γ is a homomorphism, so $\varphi(r) = \mu\gamma(r)$ for each $r \in R$. ∎

Example 5.2.10 Let $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ be as in Example 5.2.7. Let $a \in \mathbb{Z}$, so by the division algorithm, $a = nq + r \in \mathbb{Z}$, and $\varphi(a) = r$. From our previous work, we know that φ is a ring homomorphism with $\ker(\varphi) = \{kn : k \in \mathbb{Z}\} = n\mathbb{Z}$. So by the Fundamental Homomorphism Theorem, μ is an isomorphism,



which implies that $\dfrac{\mathbb{Z}}{n\mathbb{Z}} \cong \mathbb{Z}_n$. □

Definition 5.2.11 An ideal $N \neq R$ in a commutative ring R is a *prime ideal* if $ab \in N$ implies that either $a \in N$ or $b \in N$ for $a, b \in R$. ♢

Our current definition of a prime element of an integral domain bears a striking similarity to the definition of prime ideal. Recall that our definition

of prime says that if $p \mid ab$, then either $p \mid a$ or $p \mid b$. We can relate this to the Gaussian integers, since we know that $2 = (1-i)(i+i)$, but $2 \nmid (1-i)$ and $2 \nmid (1+i)$.

Example 5.2.12 Let $n = 12$. Then $12\mathbb{Z}$ is an ideal of $\mathbb{Z}$ and $12 \in 12\mathbb{Z}$. However, neither 3 nor 4 is an element of the ideal since it contains only integer multiples of 12, thus $12\mathbb{Z}$ is not a prime ideal.

Suppose now that $n \in \mathbb{N}$ is prime. Then $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$. Suppose $ab \in n\mathbb{Z}$, where $a, b \in \mathbb{Z}$. Then $ab = kn$, for some $k \in \mathbb{Z}$, so $\dfrac{ab}{n} = k$, which is an integer, and at least one of either a or b must have been a multiple of n to begin with since n is prime, which means that either $a \in n\mathbb{Z}$ or $b \in n\mathbb{Z}$. □

Theorem 5.2.13 *Let R be a commutative ring with unity, and let $N \neq R$ be an ideal in R. Then R/N is an integral domain if and only if N is a prime ideal in R.*

Proof: $\boxed{\Rightarrow}$ Suppose R/N is an integral domain. Let $a, b \in R$. If $ab \in N$, then $[ab] = [a][b] = [0]$, which implies that either $[a] = [0]$ or $[b] = [0]$. This in turn implies that either $a \in N$ or $b \in N$, and it follows that N is a prime ideal.

$\boxed{\Leftarrow}$ Suppose N is a prime ideal and $[a][b] = [0]$. Then $[ab] = [0]$, which implies that $ab \in N$. But N is a prime ideal, so either $a \in N$ or $b \in N$, which implies that $[a] = [0]$ or $[b] = [0]$, and it follows that R/N is an integral domain. ∎

Example 5.2.14 Consider $\varphi_i : \mathbb{Z}[x] \to \mathbb{C}$. φ_i is an *evaluation homomorphism*, and it basically replaces each x in a polynomial with i.

The kernel of φ_i is the set of all polynomials in $\mathbb{Z}[x]$ that are mapped to $0 \in \mathbb{C}$. Thus it is the set of all polynomials with integer coefficients that have i as a root. Since complex roots of polynomials that have real coefficients come in conjugate pairs, if i is a root, then $-i$ is also a root. If i and $-i$ are roots of a polynomial in $\mathbb{Z}[x]$, then it follows that $x^2 + 1$ is a factor of the polynomial, thus we can denote the kernel of φ_i by

$$\ker(\varphi_i) = \big\{P(x) \cdot (x^2 + 1) : P(x) \in \mathbb{Z}[x]\big\}.$$

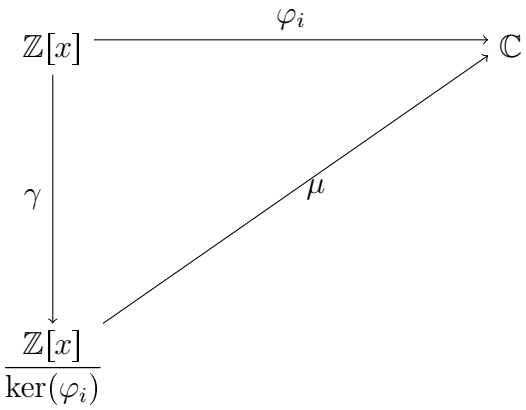
But this is the ideal generated by $x^2 + 1$, which is denoted $\langle x^2 + 1\rangle$. The polynomial of smallest degree in this set is x^2+1 itself, since x^2+1 is irreducible in $\mathbb{Z}[x]$, and so we can say that the coset containing $x^2 + 1$, is equal to the zero coset, or $[x^2 + 1] = [0]$. So

$$\begin{aligned} & [x^2 + 1] = [0] \\ \iff & [x^2] = [-1] \\ \iff & [x] \text{ behaves like } \sqrt{-1}. \end{aligned}$$

In other words, in this setting, $x = \sqrt{-1}$, which implies that $x^2 = -1$. Now, if we look at $\dfrac{\mathbb{Z}[x]}{\langle x^2 + 1\rangle}$, we can essentially replace every x^2 that appears in any polynomial in $\mathbb{Z}[x]$ with -1, thus the cosets in $\dfrac{\mathbb{Z}[x]}{\langle x^2 + 1\rangle}$ are all of the form $[a + bx]$.

But if φ_i replaces each leftover x with an i, then for any representative of $[a+bx] \in \dfrac{\mathbb{Z}[x]}{\langle x^2+1\rangle}$, we have $\mu\big([a+bx]\big) = \varphi_i(a+bx) = a+bi$. Thus the image of φ_i is given by $\{a+bi : a,b \in \mathbb{Z}\} \subset \mathbb{C}$. The result is that $\dfrac{\mathbb{Z}[x]}{\langle x^2+1\rangle} \cong \mathbb{Z}[i] = \{a+bi : a,b \in \mathbb{Z}\}$.

We can also see this using the Fundamental Homomorphism Theorem,



where μ is the isomorphism from $\mathbb{Z}[x]$ into $\mathbb{C}$. □

Example 5.2.15 Recall that ω is the cube root of unity. We want to examine a variation of the previous example. Let $\varphi_\omega : \mathbb{Z}[x] \to \mathbb{C}$ be an evaluation homomorphism. The kernel of φ_ω is the set of all polynomials in $\mathbb{Z}[x]$ that are mapped to $0 \in \mathbb{C}$. Thus, it is the set of polynomials that have ω as a root. In Example 4.1.5, we stated that it can be shown via the quadratic formula that ω and ω^2 are the roots of x^2+x+1. We will explore the relationship between ω and ω^2 more in Section 5.4, but for now assume that whenever ω is a root of a polynomial in $\mathbb{Z}[x]$, ω^2 is another root. It follows then that if ω is a root of a polynomial in $\mathbb{Z}[x]$, then x^2+x+1 is a factor of the polynomial. Thus

we can denote $\ker(\varphi_\omega)$ by

$$\ker(\varphi_\omega) = \big\{P(x) \cdot (x^2 + x + 1) : P(x) \in \mathbb{Z}[x]\big\}.$$

But this is the ideal $\langle x^2 + x + 1\rangle$, generated by $x^2 + x + 1$. The smallest polynomial in this set is $x^2 + x + 1$ itself, since $x^2 + x + 1$ is irreducible in $\mathbb{Z}[x]$, so it is a prime ideal. But since $x^2 + x + 1$ is in the kernel, we have $[x^2 + x + 1] = [0]$. So

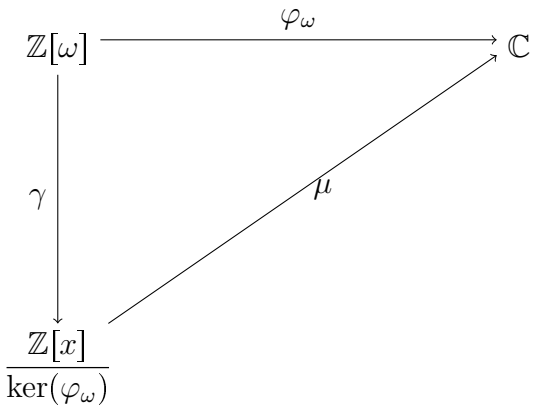
$$[x^2 + x + 1] = [0]$$

$$\iff [x^2] = [-x - 1].$$

Thus, we can take any polynomial from $\mathbb{Z}[x]$ and replace every x^2 with $-x-1$, so that every coset in $\dfrac{\mathbb{Z}[x]}{\langle x^2 + x + 1\rangle}$ is of the form $[a + bx]$.

Then φ_ω takes polynomials of the form $a + bx$ and evaluates them at $x = \omega$. So for any representative of $[a+bx]$, $\mu\big([a+bx]\big) = \varphi_\omega(a+bx) = a+b\omega$. Thus the image of φ_ω is given by $\{a + b\omega : a, b \in \mathbb{Z}\} \subset \mathbb{C}$. Recall that this set is called the Eisenstein integers. Since we can repeat this process for any polynomial in $\mathbb{Z}[x]$, the result is that $\dfrac{\mathbb{Z}[x]}{\langle x^2 + x + 1\rangle} \cong \mathbb{Z}[\omega] = \{a+b\omega : a, b \in \mathbb{Z}\}$.

If we apply the Fundamental Homomorphism as in the previous example, we have



where μ is again the isomorphism from $\mathbb{Z}[\omega]$ into $\mathbb{C}$. □

Definition 5.2.16 Let R be a ring. If M is a proper ideal of R such that no other proper ideal in R contains M, then M is a *maximal ideal*. ♢

Proposition 5.2.17 *Let R be a commutative ring with unity. Then M is a maximal ideal of R if and only if R/M is a field.*

The proof of this proposition can be found in [6].

Example 5.2.18 We previously showed that $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$, and that $\mathbb{Z}_n$ is a field only when n is prime. If we put these two results together, then in $\mathbb{Z}$, the maximal ideals are strictly the $n\mathbb{Z}$ for which n is prime. □

Theorem 5.2.19 *Every maximal ideal in a commutative ring R with unity is a prime ideal.*

Proof: Suppose that M is a maximal ideal of a ring R. Then by Proposition 5.2.17, $\frac{R}{M}$ is a field. By Definition 5.1.3, this implies that $\frac{R}{M}$ is an integral domain, and by Theorem 5.2.13, M is a prime ideal. ∎

Theorem 5.2.20 *An ideal $\langle p(x) \neq 0 \rangle$ of $\mathbb{F}[x]$ is maximal if and only if $p(x)$ is irreducible over $\mathbb{F}$.*

Proof: $\boxed{\Rightarrow}$ Suppose $\langle P(x) \rangle$ is not a maximal ideal of $\mathbb{F}[x]$. Then

$$\langle P(x) \rangle \subset \langle R(x) \rangle \subset \mathbb{F}[x],$$

which implies that $P(x) = R(x)S(x)$, so $P(x)$ is reducible over $\mathbb{F}$. Thus not maximal implies not irreducible.

$\boxed{\Leftarrow}$ Suppose that $P(x)$ is reducible over $\mathbb{F}$. Then $P(x) = R(x)S(x)$, which implies that $\langle P(x) \rangle \subset \langle R(x) \rangle \subset \mathbb{F}[x]$, so $\langle P(x) \rangle$ is not maximal. Thus not irreducible implies not maximal. ∎

5.3 Euclidean Domains

Definition 5.3.1 A *Euclidean norm* on an integral domain D is a function ν mapping the nonzero elements of D into the nonnegative integers such that the following conditions are satisfied:

1. For all $a, b \in D$ with $b \neq 0$, there exist q and r in D such that $a = bq + r$, where either $r = 0$ or $\nu(r) < \nu(b)$.

2. For $a, b \in D$, where neither a nor b is 0, $\nu(a) \leqslant \nu(ab)$.

An integral domain D is a *Euclidean domain* if there exists a Euclidean norm on D. ♢

Example 5.3.2 Let $a, b \in \mathbb{Z}$ and $b \neq 0$. By the division algorithm for integers, there exist q and r such that $a = bq + r$. If a is a multiple of b, then $r = 0$. Otherwise, note that since $0 \leqslant r < b$, we have $|r| < |b|$, where this is the usual absolute value function. Thus Condition 1 is satisfied.

Now, if $a \neq 0$ as well, then $|a| \geqslant 1$, so $|ab| = |a| \cdot |b|$, and $|ab| \geqslant |a|$. This satisfies condition 2. It follows that for $a \neq 0 \in \mathbb{Z}$, if we define $\nu(a) = |a|$, then absolute value is a Euclidean norm on $\mathbb{Z}$. □

The following proposition is a generalization of Theorem 5.2.20.

Proposition 5.3.3 *In a Euclidean domain D, an ideal $\langle a \rangle$ is maximal if and only if a is irreducible in D.*

The proof of this proposition can be found in [6].

Proposition 5.3.4 *A Euclidean domain is a unique factorization domain.*

The proof of this proposition can be found in [6].

Recall that the elements in $\mathbb{Z}[x]$ are polynomials with integer coefficients with unknown x. We want to work in a similar setting, but instead of polynomials, we want to work with the Gaussian integers, $a + bi \in \mathbb{C}$, where $a, b \in \mathbb{Z}$. We denote this as $\mathbb{Z}[i]$, where the elements are all Gaussian integers. The following example runs through the properties that define a Euclidean norm, and we establish that such a norm exists here, and thus that the Gaussian integers form a Euclidean domain.

Example 5.3.5 Let $\alpha = a+bi \in \mathbb{Z}[i]$. Define $N(\alpha) = (a+bi)(a-bi) = a^2+b^2$.

Let $\beta = c + di \neq 0$. Then $N(\beta) = c^2 + d^2$, so $N(\beta) \geqslant 1$. For all $\alpha, \beta \neq 0 \in \mathbb{Z}[i]$, $N(\alpha) = a^2 + b^2$ and

$$\begin{aligned}
N(\alpha\beta) &= N\big((a+bi)(c+di)\big) && \text{(Substitution)} \\
&= N\big((ac-bd)+(ad+bc)i\big) \\
&\qquad \text{(Distributive, Associative, Commutative Properties)} \\
&= (ac-bd)^2 + (ad+bc)^2 && \text{(Definition of } N\text{)} \\
&= (ac)^2 - 2abcd + (bd)^2 + (ad)^2 + 2abcd + (bc)^2 \\
&\qquad \text{(Distributive Property)} \\
&= (ac)^2 + (bd)^2 + (ad)^2 + (bc)^2 && \text{(Arithmetic in } \mathbb{Z}\text{)} \\
&= (a^2+b^2)(c^2+d^2) && \text{(Distributive Property)} \\
&= N(a+bi)N(c+di) && \text{(Definition of } N\text{)} \\
&= N(\alpha)N(\beta). && \text{(Substitution)}
\end{aligned}$$

So

$$N(\alpha\beta) = N(\alpha)N(\beta) \geqslant N(\alpha)$$

since $N(\beta) \geqslant 1$, thus Property 2 of a Euclidean norm is satisfied.

Showing that Property 1 holds is equivalent to showing that there is a division algorithm in this setting. Let $\alpha, \beta \in \mathbb{Z}[i]$, with $\alpha = a + bi$ and $\beta = c + di \neq 0$. We need to find $\gamma, \rho \in \mathbb{Z}[i]$ so that $\alpha = \beta\gamma + \rho$, where either

$\rho = 0$ or $N(\rho) < N(\beta)$. Note that this resembles the division algorithm for $\mathbb{Z}$.

$$\begin{aligned}\frac{\alpha}{\beta} &= \left(\frac{a+bi}{c+di}\right)\left(\frac{c-di}{c-di}\right) && \text{(Multiply by complex conjugate)}\\ &= \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i. \\ & && \text{(Distributive, Associative, Commutative Properties)}\end{aligned}$$

Let $r = \dfrac{ac+bd}{c^2+b^2}$ and $s = \dfrac{bc-ad}{c^2+d^2}$, so $\dfrac{\alpha}{\beta} = r + si$. Recall that the division algorithm is looking for something of the form $\alpha = \beta\gamma + \rho$, where either $\rho = 0$ or $N(\rho) < N(\beta)$. Thus we examine $\rho = \alpha - \beta\gamma$.

Choose $t, u \in \mathbb{Z}$ so that the integers t and u are as close as possible to the rational numbers r and s respectively. Let $\gamma = t + ui$ and $\rho = \alpha - \beta\gamma$. If $\rho = 0$, then we're finished. Otherwise, observe that $\big|r-t\big| \leqslant \dfrac{1}{2}$ and $\big|s-u\big| \leqslant \dfrac{1}{2}$ by the construction of our γ. So

$$\begin{aligned}N\left(\frac{\alpha}{\beta} - \gamma\right) &= N\big((r+si) - (t+ui)\big) && \text{(Substitution)}\\ &= N\big((r-t) + (s-u)i\big) \\ & && \text{(Distributive, Associative, Commutative Properties)}\\ &= (r-t)^2 + (s-u)^2 && \text{(Definition of } N\text{)}\\ &\leqslant \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 && \text{(Substitution)}\\ &= \frac{1}{2}. && \text{(Arithmetic in } \mathbb{Q}\text{)}\end{aligned}$$

Thus taking the norm of both sides of $\rho = \alpha - \beta\gamma$ yields

$$\begin{aligned} N(\rho) &= N(\alpha - \beta\gamma) && \text{(Substitution)} \\ &= N\left(\beta\left(\frac{\alpha}{\beta} - \gamma\right)\right) && \text{(Distributive Property)} \\ &= N(\beta) \cdot N\left(\frac{\alpha}{\beta} - \gamma\right) && \text{(By work above)} \\ &\leqslant N(\beta) \cdot \frac{1}{2}, && \text{(Substitution)} \end{aligned}$$

so $N(\rho) < N(\beta)$, which is the desired result. Thus Property 1 of a euclidean norm holds, and it follows that N is a Euclidean norm on $\mathbb{Z}[i]$. By this division algorithm on $\mathbb{Z}[i]$, we can express $\alpha \in \mathbb{Z}[i]$ in the form $\alpha = \beta\gamma + \rho$. □

Example 5.3.6 The above example gave us a division algorithm for the Gaussian integers. So consider $3 + 2i$ and $1 + i$. $N(3 + 2i) = 9 + 4 = 13$ and $N(1+i) = 1+1 = 2$. We want to find $\gamma, \rho \in \mathbb{Z}[i]$ such that $3+2i = (1+i)\gamma+\rho$. As shown in the previous example, we either need $\rho = 0$ or $N(\rho) < N(1 + i)$.

$$\begin{aligned} \frac{3+2i}{1+i} &= \left(\frac{3+2i}{1+i}\right)\left(\frac{1-i}{1-i}\right) && \text{(Rationalize the denominator)} \\ &= \frac{3-3i+2i+2}{1-(-1)} && \text{(Distributive Property)} \\ &= \frac{5-i}{2} && \text{(Arithmetic)} \\ &= \frac{5}{2} - \frac{1}{2}i. && \text{(Arithmetic)} \end{aligned}$$

So $\dfrac{3+2i}{1+i} = \dfrac{5}{2} - \dfrac{1}{2}i$. Now we need to find integers t and u that are as close as possible to $\dfrac{5}{2}$ and $-\dfrac{1}{2}$ respectively. Let $t = 3$ and $u = 0$. Then using the

process described in Example 5.3.5, $\gamma = 3$ and $\rho = (3+2i) - (1+i)(3) = -i$. Now $N(-i) = 1$, which is less than $N(1+i) = 2$, as required. Thus

$$3 + 2i = (1+i)(3) - i$$

by the division algorithm for the Gaussian integers. □

Proposition 5.3.7 (Euclidean Algorithm) *Let D be a Euclidean domain with a Euclidean norm ν, and let a and b be nonzero elements of D. Let r_1 be as in Condition 1 for a Euclidean norm, that is $a = bq_1 + r_1$, where either $r_1 = 0$ or $\nu(r_1) < \nu(b)$. If $r_1 \neq 0$, let r_2 be such that $b = r_1q_2 + r_2$, where either $r_2 = 0$ or $\nu(r_2) < \nu(r_1)$. In general, let r_{i+1} be such that $r_{i-1} = r_iq_{i+1} + r_{i+1}$, where either $r_{i+1} = 0$ or $\nu(r_{i+1}) < \nu(r_i)$. Then the sequence $r_1, r_2, \ldots$ must terminate with some $r_i = 0$. If $r_1 = 0$, then b is the gcd of a and b. If $r_1 \neq 0$ and r_s is the first $r_i = 0$, then the gcd of a and b is r_{s-1}. Furthermore, if $\gcd(a, b) = d$, then there exist s and t in D such that $as + bt = d$.*

This proof can be found in [6].

Example 5.3.8 We want to examine polynomials in $\mathbb{Q}[x]$ and show that a division algorithm exists in this setting. Let $f(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots a_0$ and $g(x) = b_mx^m + b_{m-1}x^{m-1} + \cdots + b_0 \in \mathbb{Q}[x]$, where a_n and b_m are both nonzero rational numbers and $m > 0$. We claim that if these things are true, then there exist unique polynomials $q(x), r(x) \in \mathbb{Q}[x]$, such that $f(x) = g(x) \cdot q(x) + r(x)$, where either $r(x) = 0$ or the degree of $r(x)$ is less than m.

Let $S = \{f(x) - g(x) \cdot s(x) : s(x) \in \mathbb{Q}[x]\}$. If $0 \in S$, then there exists some $s(x)$ such that $f(x) - g(x) \cdot s(x) = 0$, so $f(x) = g(x) \cdot s(x)$. If $q(x) = s(x)$ and $r(x) = 0$, then we have established the existence of $q(x)$ and $r(x)$. Otherwise, let $r(x) \in S$ be a polynomial with the smallest degree in S. There may be multiple polynomials of this same lowest degree, so just choose one of them. Then $f(x) = g(x) \cdot q(x) + r(x)$ for some $q(x) \in \mathbb{Q}[x]$. We need to show that the degree of $r(x)$ is less than m.

If $r(x) = c_l x^l + c_{l-1} x^{l-1} + \cdots + c_0$, with each $c_i \in \mathbb{Q}$ and $c_l \neq 0$, then if $l \geqslant m$,

$$\begin{aligned} & f(x) - g(x) \cdot q(x) = r(x) \\ \iff & f(x) - g(x) \cdot q(x) - \left(\frac{c_l}{b_m}\right) x^{l-m} \cdot g(x) = r(x) - \left(\frac{c_l}{b_m}\right) x^{l-m} \cdot g(x). \end{aligned}$$

The right side of this equation is a polynomial of degree less than l, of the form $r(x) - c_l x^l - p(x)$, with the degree of $p(x)$ less than l. But we can rewrite the left side of the equation as $f(x) - g(x)\left(q(x) + \left(\frac{c_l}{b_m}\right) x^{l-m}\right)$, thus it is contained in S. However, $r(x)$ was a polynomial of lowest degree in S, and since $r(x) - c_l x^l - p(x)$ is of degree smaller than l, this is a contradiction. Thus $l < m$ as desired.

It remains to show that $q(x)$ and $r(x)$ are unique, so suppose that $f(x) = g(x) \cdot q_1(x) + r_1(x)$ and $f(x) = g(x) \cdot q_2(x) + r_2(x)$. Then subtracting one from the other yields

$$g(x) \cdot q_1(x) + r_1(x) - g(x) \cdot q_2(x) - r_2(x) = 0.$$

This implies that $g(x)\big(q_1(x)-q_2(x)\big) = r_2(x)-r_1(x)$. But recall that either the degrees of $r_1(x)$ and $r_2(x)$ are less than the degree of $g(x)$ or $r_2(x)-r_1(x) = 0$. So either $\deg\Big(g(x)\big(q_1(x) - q_2(x)\big)\Big) > \deg\big(r_2(x) - r_1(x)\big)$, or both sides of the equation are zero. The first case is clearly impossible since the two sides are equal. Thus $q_1(x) - q_2(x) = 0$, which implies that $q_1(x) = q_2(x)$ and $r_2(x) - r_1(x) = 0$, which implies that $r_1(x) = r_2(x)$. It follows that $q(x)$ and $r(x)$ are unique. □

Definition 5.3.9 Let R be a commutative ring with unity and let $a, b \in R$. If there exists $c \in R$, such that $b = ac$, then a *divides* b, or a *is a factor of* b. We denote this $a \mid b$. ♢

Since we've shown previously that we have a Euclidean norm in $\mathbb{Z}[i]$, we can use the Euclidean algorithm to find a greatest common divisor of two Gaussian integers.

Example 5.3.10 We want to find a greatest common divisor of $6 + 10i$ and $1+5i$ in $\mathbb{Z}[i]$ using the division algorithm that we established in Example 5.3.5.

$$6 + 10i = (1 + 5i)(2 - i) + (-1 + i)$$

$$1 + 5i = (-1 + i)(2 - 3i) + 0.$$

So

$$\alpha = 6 + 10i$$

$$\beta = 1 + 5i$$

$$\rho_1 = -1 + i$$

$$\rho_2 = 0.$$

Thus, $-1 + i$ is a greatest common divisor of $6 + 10i$ and $1 + 5i$. □

5.4 The Ring $\mathbb{Z}[\omega]$

Recall from our previous work that ω is the cube root of unity, and is thus a solution to the equation $x^3 = 1$. We are going to work extensively with $\mathbb{Z}[\omega]$ in the cubic reciprocity chapter, so now that we know that it forms a ring, we want to establish some properties and other nice things for it. This will make our work later a lot more straightforward, since we will be able to refer back to this section.

Definition 5.4.1 Let $\alpha = a + b\omega \in \mathbb{Z}[\omega]$, where $a, b \in \mathbb{Z}$. Then the *complex conjugate of* α is $\overline{\alpha} = a + b\overline{\omega} = a + b\omega^2 = (a - b) - b\omega$, and the *norm of* α is given by

$$N(\alpha) = \alpha\overline{\alpha} = a^2 - ab + b^2,$$

where $\omega = \dfrac{-1 + \sqrt{-3}}{2}$, $\omega^2 = \dfrac{-1 - \sqrt{-3}}{2}$, and $\omega^3 = 1$. ♢

Note that $N(a+b\omega) = |a+b\omega|^2$.

Example 5.4.2 Let $\alpha = a + b\omega \neq 0$. Then $N(\alpha) = a^2 - ab + b^2$ by Definition 5.4.1. We claim that $N(\alpha) \geqslant 1$.

$$\begin{aligned}
N(\alpha) &= a^2 - ab + b^2 && \text{(Definition of } N\text{)} \\
&= \left(a^2 - ab + \left(\frac{b}{2}\right)^2\right) + b^2 - \left(\frac{b}{2}\right)^2 && \text{(Complete the square)} \\
&= \left(a - \frac{b}{2}\right)^2 + \frac{4b^2}{4} - \frac{b^2}{4} && \text{(Factor)} \\
&= \left(a - \frac{b}{2}\right)^2 + \frac{3b^2}{4}, && \text{(Arithmetic)}
\end{aligned}$$

which is clearly nonnegative as long as $\alpha = a + b\omega \neq 0$. □

Theorem 5.4.3 *Let $\alpha, \beta \in \mathbb{Z}[\omega]$. Then $N(\alpha\beta) = N(\alpha)N(\beta)$.*

Proof: Let $\alpha, \beta \in \mathbb{Z}[\omega]$. Then

$$\begin{aligned}
N(\alpha\beta) &= \alpha\beta \cdot \overline{\alpha\beta} && \text{(Definition of } N\text{)} \\
&= \alpha\beta\overline{\alpha}\overline{\beta} && \text{(Properties of conjugates)} \\
&= \alpha\overline{\alpha}\beta\overline{\beta} && \text{(Commutativity in } \mathbb{C}\text{)} \\
&= N(\alpha)N(\beta), && \text{(Definition of } N\text{)}
\end{aligned}$$

which is the desired result. ∎

Example 5.4.4 We claim that the norm N given by Definition 5.4.1 is a Euclidean norm.

Property 2 of Euclidean norms requires that for all $\alpha, \beta \in \mathbb{Z}[\omega]$, where $\alpha, \beta \neq 0$, $N(\alpha) \leqslant N(\alpha\beta)$.

Let $\alpha = a + b\omega \neq 0$ and $\beta = c + d\omega \neq 0$. We know $N(\alpha\beta) = N(\alpha)N(\beta)$ by Theorem 5.4.3. We also know that $N(\alpha), N(\beta) \geqslant 1$ by Example 5.4.2 and $N(\alpha), N(\beta) \in \mathbb{Z}$ by Definition 5.4.1, thus

$$N(\alpha) \leqslant N(\alpha)N(\beta) = N(\alpha\beta).$$

To show that Property 1 holds, let $\alpha = a + b\omega$ and $\beta = c + d\omega \neq 0$. We need to find $\gamma, \rho \in \mathbb{Z}[\omega]$, such that $\alpha = \beta\gamma + \rho$ with $\rho = 0$ or $N(\rho) < N(\beta)$. Since $\beta \neq 0$, we can examine $\dfrac{\alpha}{\beta}$.

$$\begin{aligned} \frac{\alpha}{\beta} &= \frac{a + b\omega}{c + d\omega} \cdot \frac{(c - d) - d\omega}{(c - d) - d\omega} && \text{(Multiply by conjugate; Definition 5.4.1)} \\ &= \frac{ac - ad + bd}{c^2 - cd + d^2} + \frac{bc - ad}{c^2 - cd + d^2}\omega. && \text{(Arithmetic)} \end{aligned}$$

Let $r = \dfrac{ac - ad + bd}{c^2 - cd + d^2}$ and $s = \dfrac{bc - ad}{c^2 - cd + d^2}$. Then $\dfrac{\alpha}{\beta} = r + s\omega$. Recall that the division algorithm is looking for something of the form $\alpha = \beta\gamma + \rho$, where either $\rho = 0$ or $N(\rho) < N(\beta)$. Thus we examine $\rho = \alpha - \beta\gamma$.

Choose $t, u \in \mathbb{Z}$ such that the integers t and u are as close as possible to the rational numbers r and s respectively. Let $\gamma = t + u\omega$ and $\rho = \alpha - \beta\gamma$. If $\rho = 0$, then we're finished. Otherwise, we have $\left|r - t\right| \leqslant \dfrac{1}{2}$ and $\left|s - u\right| \leqslant \dfrac{1}{2}$,

by the construction of γ. So

$$\begin{aligned}
N\left(\frac{\alpha}{\beta}-\gamma\right) &= N\big((r+s\omega)-(t+u\omega)\big) && \text{(Substitution)}\\
&= N\big((r-t)+(s-u)\omega\big) && \text{(Arithmetic)}\\
&= (r-t)^2-(r-t)(s-u)+(s-u)^2 && \text{(Definition of } N\text{)}\\
&\leqslant \left(\frac{1}{2}\right)^2-(r-t)(s-u)+\left(\frac{1}{2}\right)^2 && \text{(Substitution)}\\
&= \frac{1}{2}-(r-t)(s-u). && \text{(Arithmetic)}
\end{aligned}$$

But $\big|r-t\big|\cdot\big|s-u\big| \leqslant \frac{1}{2}\cdot\frac{1}{2}$ is equivalent to $-\frac{1}{4} \leqslant (r-t)(s-t) \leqslant \frac{1}{4}$. Thus we have $0 < N\left(\frac{\alpha}{\beta}-\gamma\right) \leqslant \frac{3}{4}$.

Now, since $\rho = \alpha - \beta\gamma$,

$$\begin{aligned}
N(\rho) &= N(\alpha-\beta\gamma) && \text{(Apply } N \text{ to both sides)}\\
&= N\left(\beta\left(\frac{\alpha}{\beta}-\gamma\right)\right) && \text{(Distributive Property)}\\
&= N(\beta)N\left(\frac{\alpha}{\beta}-\gamma\right) && \text{(Theorem 5.4.3)}\\
&\leqslant N(\beta)\cdot\frac{3}{4}, && \text{(Substitution)}
\end{aligned}$$

which implies that $N(\rho) < N(\beta)$, and Property 2 is satisfied. It follows that N is a Euclidean norm, by definition, and now we will be able to express $\alpha \in \mathbb{Z}[\omega]$ in the form $\alpha = \beta\gamma + \rho$. □

Example 5.4.5 The previous example allows us to represent the Eisenstein integers in the form $\alpha = \beta\gamma + \rho$, which is very similar to $a = bq + r$ by the

division algorithm in $\mathbb{Z}$. Let $\alpha = 6 + \omega$ and $\beta = 5 + 2\omega$. Then by the process laid out above, $\dfrac{6+\omega}{5+2\omega} = \dfrac{20}{19} - \dfrac{7}{19}\omega$.

Now we need to choose $t, u \in \mathbb{Z}$ to be as close as possible to $\dfrac{20}{19}$ and $\dfrac{7}{19}$, respectively, so let $t = 1$ and $u = 0$. Then $\rho = (6+\omega)-(5+2\omega)(1+0\omega) = 1-\omega$ and $\gamma = 1 + 0\omega$. Thus $\underbrace{6 + \omega = (5 + 2\omega)(1 + 0\omega) + (1 - \omega)}_{\alpha=\beta\gamma+\rho}$. □

Example 5.4.6 Let $\alpha = 6 + \omega$ and $\beta = 5 + 2\omega$ as in the previous example. We want to take our work one step further and find a greatest common divisor of α and β. We need to continue the process outlined in Example 5.4.4.

$$6 + \omega = (5 + 2\omega)(1) + (1 - \omega)$$

$$5 + 2\omega = (1 - \omega)(3 + 2\omega) - \omega$$

$$1 - \omega = (-\omega)(2 + \omega) + 0$$

Thus

$$\alpha = 6 + \omega$$

$$\beta = 5 + 2\omega$$

$$\rho_1 = 1 - \omega$$

$$\rho_2 = -\omega$$

$$\rho_3 = 0.$$

It follows that $-\omega$ is a greatest common divisor of $6 + \omega$ and $5 + 2\omega$. □

Theorem 5.4.7 *Let $\alpha \in \mathbb{Z}[\omega]$. $\mathbb{Z}[\omega]$ is a Euclidean domain with $N(\alpha) = \alpha\overline{\alpha}$.*

Proof: In Example 5.1.15, we showed that $\mathbb{Z}[\omega]$ is a ring. Since $\mathbb{Z}[\omega]$ is a subset of $\mathbb{C}$, some of the properties of $\mathbb{C}$ are "inherited". Multiplication is commutative and there is a multiplicative identity in $\mathbb{Z}[\omega]$, specifically the element $1+0\omega$. Since there are no zero divisors in $\mathbb{C}$, there are no zero divisors in $\mathbb{Z}[\omega]$. Thus $\mathbb{Z}[\omega]$ is an integral domain, and since by Example 5.4.4, we have established a Euclidean norm, $\mathbb{Z}[\omega]$ is a Euclidean domain by definition. ∎

Since $\mathbb{Z}[\omega]$ is a Euclidean domain, by Theorem 5.3.4, it is also a unique factorization domain. This is important, because it means that the notions of prime and irreducible are interchangeable in this setting.

Recall that the units in a ring are the elements that have multiplicative inverses in the ring. In the integers, the units are 1 and -1, but there are actually six units in $\mathbb{Z}[\omega]$, and this theorem finds them all and gives a criterion for establishing whether or not an element in $\mathbb{Z}[\omega]$ is a unit.

Theorem 5.4.8 *Suppose $\alpha \in \mathbb{Z}[\omega]$. Then α is a unit in $\mathbb{Z}[\omega]$ if and only if $N(\alpha) = 1$. Furthermore, the units in $\mathbb{Z}[\omega]$ are 1, -1, ω, $-\omega$, ω^2, and $-\omega^2$.*

Proof: $\boxed{\Rightarrow}$ Assume $\alpha, \overline{\alpha} \in \mathbb{Z}[\omega]$ and suppose $N(\alpha) = 1$. Then $\alpha\overline{\alpha} = 1$, which implies that $\overline{\alpha}$ is the multiplicative inverse of α, so α is a unit by definition.

$\boxed{\Leftarrow}$ Suppose α is a unit. Then there exists $\beta \in \mathbb{Z}[\omega]$, such that $\alpha\beta = 1$, by definition of unit. We can take the norm of both sides of this equation, and since $N(\alpha\beta) = N(\alpha) \cdot N(\beta)$, this yields $N(\alpha) \cdot N(\beta) = 1$. But by definition of

norm, both $N(\alpha)$ and $N(\beta)$ are positive integers, thus $N(\alpha) = 1$.

It remains to establish the units in $\mathbb{Z}[\omega]$. Suppose that $\alpha = a + b\omega$ is a unit. Then, by the work above, $N(\alpha) = a^2 - ab + b^2 = 1$. Now we have

$$\begin{aligned}
& a^2 - ab + b^2 = 1 \\
\iff & 4a^2 - 4ab + 4b^2 = 4 && \text{(Multiplicative Property of Equality)} \\
\iff & 4a^2 - 4ab + b^2 + 3b^2 = 4 && \text{(Arithmetic)} \\
\iff & (2a - b)^2 + 3b^2 = 4. && \text{(Distributive Property)}
\end{aligned}$$

This last equation gives us several possibilities.

If $b = 0$, then $2a = \pm 2$, which implies that $a = \pm 1$ and $\alpha = 1 + 0\omega$ or $\alpha = -1 + 0\omega$.

If $b = \pm 1$, then $2a - b = \pm 1$. Note that b can not be larger, since $|b| > 1$ implies that $(2a - b)^2 + 3b^2 > 4$. Solving these four equations gives us the remaining four units. When $b = 1$, $\alpha = 1 + \omega$ or $\alpha = \omega$ and when $b = -1$, $\alpha = -\omega$ or $\alpha = -1 - \omega$. But $\omega^2 + \omega + 1 = 0$, so $\omega^2 = -1 - \omega$ and $-\omega^2 = 1 + \omega$. Thus, the six units are 1, -1, ω, $-\omega$, ω^2, and $-\omega^2$. ∎

We will see in Chapter 10 that if $\alpha \in \mathbb{Z}[\omega]$ and $N(\alpha) = p$, for some prime $p \in \mathbb{Z}$, then α is irreducible in $\mathbb{Z}[\omega]$. We haven't yet developed all of the tools that we need to prove this, so for now we make do with a simple example and the assumption that it is true, and we will provide a proof later.

Example 5.4.9 Consider $2 + \omega$. By Definition 5.4.1, $N(2 + \omega) = 3$. Suppose

$2 + \omega = \alpha\beta$ for $\alpha, \beta \in \mathbb{Z}[\omega]$. Then

$$\begin{aligned} 3 &= N(2+\omega) \\ &= N(\alpha\beta) && \text{(Substitution)} \\ &= N(\alpha)N(\beta). && \text{(Theorem 5.4.3)} \end{aligned}$$

But 3 is prime, so this implies that one of $N(\alpha)$ or $N(\beta)$ is a unit. As we will see in Chapter 10, this means that either α or β is itself a unit, and it follows that $2+\omega$ is irreducible in $\mathbb{Z}[\omega]$. A similar argument reveals that $3+\omega$ is also irreducible. □

Example 5.4.10 We want to construct a particular ring that will be useful in the cubic reciprocity chapter. Let $1-\omega \in \mathbb{Z}[\omega]$ and note that it is prime, since $N(1-\omega) = 3$. We have worked a little bit with factor rings already, and now we want to consider $\dfrac{\mathbb{Z}[\omega]}{(1-\omega)\mathbb{Z}[\omega]}$. Recall that $(1-\omega)\mathbb{Z}[\omega]$ is all of the Eisenstein multiples of $1-\omega$. Since the elements of factor rings are cosets, and we are modding the Eisenstein integers out by $1-\omega$, it follows that $[1-\omega] = [0]$. In other words, the coset containing $1-\omega$ is the same as the coset containing 0. We can do arithmetic on cosets, so that $[1-\omega] = [0]$ implies that $[1] = [\omega]$. Thus, since every coset in this ring is of the form $[a+b\omega]$, we can essentially substitute 1 for ω, and then every coset can be written as $[a+b\omega] = [a+b]$. Since in the Eisenstein integers, $a, b \in \mathbb{Z}$, this means that every coset can be reduced to contain only integers.

Consider the map $\varphi : \mathbb{Z} \to \dfrac{\mathbb{Z}[\omega]}{(1-\omega)\mathbb{Z}[\omega]}$, defined by $\varphi(n) = [n]$. Then $\ker(\varphi) = \{n \in \mathbb{Z} : (1-\omega) \mid n\}$. Note that if $(1-\omega) \mid n$, then $N(1-\omega) \mid N(n)$. But $N(1-\omega) = 3$ and $N(n) = n^2$, so this implies that $3 \mid n^2$. Since 3 is prime, it must be the case that $3 \mid n$. Thus the kernel of φ contains all integer multiples of 3, so for any $k \in \mathbb{Z}$, $[3k] = [0]$.

Conversely, since $3 = (1-\omega)(1-\overline{\omega})$, φ sends 3 to $[0]$, so the kernel of φ is $3\mathbb{Z}$. Thus by the Fundamental Homomorphism Theorem, we have

$$\mathbb{Z}_3 \cong \frac{\mathbb{Z}}{3\mathbb{Z}} \cong \frac{\mathbb{Z}[\omega]}{(1-\omega)\mathbb{Z}[\omega]}.$$

This result is huge, because we have reduced cosets containing ω to cosets containing only integers, and now every multiple of 3 is in the 0 coset, so there are only three equivalence classes in this ring, specifically $[0], [1], [2]$. This idea will show up again when we start exploring cubic reciprocity. □

5.5 Algebraic Numbers and Algebraic Integers

Definition 5.5.1 An *algebraic number* is a complex number α that is a root of a polynomial $a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_n = 0$, where $a_0, a_1, a_2, \ldots, a_n \in \mathbb{Q}$, and $a_0 \neq 0$. An *algebraic integer* ω is a complex number that is a root of a polynomial $x^n + b_1x^{n-1} + \cdots + b_n = 0$, where $b_1, b_2, \ldots, b_n \in \mathbb{Z}$. ♢

Proposition 5.5.2 *Let α be an algebraic number and ω be an algebraic integer.*

1. *The set of algebraic numbers forms a field.*

2. *The set of algebraic integers forms a ring, which will be denoted by* Ω.

The proof of this proposition is omitted here, but can be found in [8].

Theorem 5.5.3 *If* $\omega_1, \omega_2 \in \Omega$ *and* $p \in \mathbb{Z}$ *is a prime, then*

$$(\omega_1 + \omega_2)^p \equiv \omega_1^p + \omega_2^p \bmod p.$$

Proof: By the binomial expansion theorem,

$$(\omega_1 + \omega_2)^p = \sum_{i=0}^{p} \binom{p}{i} \omega_1^{p-i} \omega_2^i.$$

But recall that $\binom{p}{i} = \dfrac{p!}{i!(p-i)!}$, so p clearly divides every term that has a coefficient of the form $\binom{p}{i}$ for each $1 \leqslant i \leqslant p-1$. Thus we are left with only the first and last terms, so $(\omega_1 + \omega_2)^p \equiv \omega_1^p + \omega_2^p \mod$ p. ∎

Example 5.5.4 Let $\xi_1, \xi_2 \in \Omega$ and suppose $p = 3$. Then

$$\begin{aligned} \left(\xi_1 + \xi_2\right)^3 &= \sum_{i=0}^{3} \binom{3}{i} \xi_1^{3-i} \xi_2^i \qquad \text{(Binomial expansion theorem)} \\ &= \xi_1^3 + 3\xi_1^2\xi_2 + 3\xi_1\xi_2^2 + \xi_2^3 \\ &\equiv \xi_1^3 + \xi_2^3 \bmod 3. \end{aligned}$$

This example demonstrates that we can add non-integers together modulo some prime integer. This idea is going to be set aside for now, but we will need to use it in a later chapter. □

Chapter 6

Solutions to Congruences

We begin Chapter 6 by exploring the solvability of specific congruences. We look at linear congruences first and establish when solutions will exist. We then briefly look at the solutions of a quadratic congruence modulo p, where p is prime. We also begin to examine higher power congruences and then prove Wilson's Theorem, which gives criteria for establishing whether or not a number is prime. We wrap up Section 0 with a definition of n^{th} power residues.

In Section 1, we develop some results about congruences and then use them to prove the Chinese Remainder Theorem. One of the results gives us a method to take a congruence of the form $x^n \equiv a \bmod m$ and write it as a system of n^{th} power congruences. This system resembles the system from the Chinese Remainder Theorem, but in this case they are not restricted to being linear congruences. We end this chapter by beginning to explore solvability of

particular n^{th} power congruences.

Theorem 6.0.5 *If* $\gcd(a, m) = d$*, then* $ax \equiv b \bmod m$ *has a solution if and only if* $d \mid b$*. If a solution exists, there are exactly* d *of them.*

Proof: Let $m \in \mathbb{N}$ and let $a, b \in \mathbb{Z}_m$. Suppose that s is a solution to $ax \equiv b \bmod m$. Then

$$\begin{aligned} & as \equiv b \bmod m && (s \text{ is a solution}) \\ \iff & as - b = km, \text{ for some } k \in \mathbb{Z} && (\text{Definition of congruent}) \\ \iff & b = as - km. && (\text{Arithmetic}) \end{aligned}$$

But we know that d divides both a and m, since $d = \gcd(a, m)$, thus d divides the right side of the above equation. This implies that d divides b as well. Hence, if we have a solution to the congruence, then d divides b.

Suppose now that d divides b. Let $a = a'd$, $b = b'd$, and $m = m'd$, where $a', b', m' \in \mathbb{Z}$. Then

$$\begin{aligned} & as \equiv b \bmod m && (s \text{ is a solution}) \\ \iff & as - b = km && (\text{Definition of congruent}) \\ \iff & a'ds - b'd = km'd && (\text{Substitution}) \\ \iff & d(a's - b') = dkm' && (\text{Distributive Property}) \\ \iff & a's - b' = km'. && (\text{Left cancellation in } \mathbb{Z}) \end{aligned}$$

Notice that this indicates that $as - b$ is a multiple of m if and only if $a's - b'$ is a multiple of m'. Thus the solutions of $ax = b \in \mathbb{Z}_m$ are the elements modulo m' that yield solutions to $a'x \equiv b' \bmod m'$.

Since $\gcd(a', m') = 1$, a' is a unit in $\mathbb{Z}_{m'}$, so $(a')^{-1}b'$ is a solution, and $(a')^{-1}b' \in \mathbb{Z}_{m'}$ is unique. Let s be this unique solution to $a'x \equiv b' \bmod m'$. Since $s \equiv (s + jm') \bmod m'$ for any $j \in \mathbb{Z}$, the solutions in $\mathbb{Z}_m$ are exactly the integers

$$s, s + m', s + 2m', \ldots, s + (d-1)m'.$$

We know that $d - 1$ and m' are both less than m, by the way m was defined, and since $m = dm'$, the integer $(d-1)m'$ is also less than m. Thus, there are exactly d solutions to the congruence $ax \equiv b \bmod m$. ∎

Example 6.0.6 Let $a = 48$, $b = 36$, and $m = 72$. Then $\gcd(48, 72) = 24$. We want to find solutions to $48x \equiv 36 \bmod 72$, if they exist. By the theorem, there will be exactly 24 solutions if and only if $24 \mid 36$. Since 24 clearly does not divide 36, the congruence has no solution. □

Theorem 6.0.7 *$x^2 \equiv 1 \bmod p$ has exactly two solutions, $x = 1$ and $x = p-1$.*

Proof: Assume p is prime.

$$\begin{aligned} & x^2 \equiv 1 \bmod p \\ \iff & x^2 - 1 \equiv 0 \bmod p && \text{(Subtraction Property of Equality)} \\ \iff & (x-1)(x+1) \equiv 0 \bmod p, && \text{(Factorization)} \end{aligned}$$

so 1 and -1 are solutions, and by Theorem 5.1.16, since $\mathbb{Z}_p$ is a field, these are the only two solutions. ∎

Example 6.0.8 Let p be prime. Then $\mathbb{Z}_p^*$ contains $\varphi(p) = p-1$ elements and $a^{p-1} \equiv 1 \bmod p$ for all $a \in \mathbb{Z}_n^*$. There are exactly $p-1$ such elements $a \in \mathbb{Z}_p^*$ to choose from, thus $x^{p-1} \equiv 1 \bmod p$ has exactly $p-1$ solutions. □

Example 6.0.9 The congruence $x^{\varphi(n)} \equiv 1 \bmod n$ has exactly $\varphi(n)$ solutions modulo n, since $a^{\varphi(n)} \equiv 1 \bmod n$ for all $a \in \mathbb{Z}_n^*$. Note that if $b \in \mathbb{Z}$ is such that $\gcd(b, n) > 1$, then $b^k \neq 1$ for any k, otherwise b would have a multiplicative inverse, and thus would be an element of $\mathbb{Z}_n^*$. □

Lemma 6.0.10 *If $d \mid (p-1)$ and $p \in \mathbb{Z}$ is prime, then $x^d \equiv 1 \bmod p$ has exactly d solutions.*

Proof: Assume p is prime and suppose $d \mid (p-1)$, for some $d \in \mathbb{Z}$. By Fermat's Little Theorem, we know that if $\gcd(a, p) = 1$, then $a^{p-1} \equiv 1 \bmod p$. Thus, for each of the $a \in \{1, \ldots, p-1\}$, $x = a$ is a solution to $x^{p-1} \equiv 1 \bmod p$.

Factorization of $x^{p-1} - 1$ yields

$$\begin{aligned} x^{p-1} - 1 &\equiv (x^d - 1)(x^{p-1-d} + x^{p-1-2d} + \cdots + 1) \bmod p \\ &\equiv (x^d - 1) \cdot g(x) \bmod p && \text{(Relabel second polynomial)} \\ &\equiv 0 \bmod p, && (x^d \equiv 1 \bmod p) \end{aligned}$$

where $g(x)$ is of degree $p-1-d$. By Theorem 5.1.16, $g(x) = 0$ has at most $p-1-d$ solutions. Since $x^{p-1} - 1 \equiv 0 \bmod p$ has $p-1$ solutions, it follows that

$x^d - 1 \equiv 0 \bmod p$ has at least d solutions. But if we consider $x^d - 1 \equiv 0 \bmod p$ on its own, we see that it has at most d solutions. In order for both outcomes to be true, it must be the case that it has exactly d solutions. ∎

Example 6.0.11 Let $p = 17$. Suppose $d = 4$ and consider $x^4 \equiv 1 \bmod 17$. Clearly $x = 1$ is a solution, so $x = 16$ is also a solution. Fairly simple computations reveal that $x = 4$ and $x = 13$ are also solutions, and it can easily be verified that the other twelve elements in $\{1, 2, \ldots, 16\}$ do not satisfy the congruence. □

Theorem 6.0.12 (Wilson's Theorem) *p is a prime if and only if*

$$(p-1)! \equiv -1 \bmod p.$$

Example 6.0.13 Let $p = 5$. Then we have $(5-1)! = 24 \equiv -1 \bmod 5$. Next let $p = 6$. Then $(6-1)! = 120 \equiv 0 \bmod 6$.

The main thing to note with these examples is that when p is not prime, $(p-1)!$ will contain factors of p, thus the result is a multiple of p. When p is prime, this does not happen, and our result is nonzero. □

Proof: $\boxed{\Rightarrow}$ Suppose first that $p = 2$. Then $(2-1)! = 1 \equiv -1 \bmod 2$. Now suppose that p is an odd prime.

$$(p-1)! = (p-1) \cdot (p-2) \ldots 2 \cdot 1$$

Set $p - 1$ and 1 aside for a moment and consider the rest of the product. For each $a \in \{2, \ldots, p-2\}$, there exists a^{-1}, since $\gcd(a, p) = 1$. There are an even

number of elements in the set when p is odd, so they pair up since no element is equal to 1 or -1. Thus $2 \cdot 3 \ldots (p-2) \equiv 1 \bmod p$, and it follows that

$$\begin{aligned}(p-1)! &= (p-1) \cdot (p-2) \ldots 3 \cdot 2 \cdot 1 \\ &\equiv (p-1) \bmod p \\ &\equiv -1 \bmod p\end{aligned}$$

$\boxed{\Leftarrow}$ Suppose that $p > 1$ is not prime. We must consider two cases.

Case 1: Let $p = ab$ for $a, b \in \mathbb{Z}$. Without loss of generality, assume $b > a$. Then

$$\begin{aligned}(p-1)! &= (p-1)(p-2) \ldots b \ldots a \ldots 2 \cdot 1 \\ &= abk, \text{ for some } k \in \mathbb{Z} \\ &\equiv 0 \bmod p.\end{aligned}$$

Case 2: Let $p = a^2$, so $a < p$. If $p = 4$, then $3! \equiv 6 \not\equiv -1 \bmod 4$. If $p \neq 4$, we have $(p-1)! = 2a^2k \equiv 0 \bmod p$, since a and $2a$ are both less than $p - 1$. Thus by contraposition, if p is not prime, then $(p-1)! \not\equiv 1 \bmod p$. ∎

Lemma 6.0.14 *If n is an odd integer, then*

$$n^2 - 1 \equiv 0 \bmod 8.$$

Proof: Recall that $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$. It is clear that $k^2 \equiv 1 \bmod 8$ for each $k \in \mathbb{Z}_8^*$. Furthermore, every odd integer n is congruent to one of the four elements of $\mathbb{Z}_8^*$ modulo 8. Thus $n^2 - 1 \equiv 0 \bmod 8$ for each odd $n \in \mathbb{Z}$. ∎

This is a very useful result in number theory and we will use it when we look at reciprocity.

Theorem 6.0.15 *Let* $\gcd(a, m) = 1$ *and suppose that* a *has order* t *modulo* m. *Then*

1. $a^n \equiv 1 \bmod m$ *if and only if* $t \mid n$.

2. $t \mid \varphi(m)$.

Proof: Assume $\gcd(a, m) = 1$ and $a^t \equiv 1 \bmod m$.

1. $\boxed{\Rightarrow}$ Suppose $a^n \equiv 1 \bmod m$. By the division algorithm, $n = qt + r$, where $0 \leqslant r < t$. Thus

$$\begin{aligned} & a^n \equiv 1 \bmod m \\ \iff & a^{qt+r} \equiv 1 \bmod m && \text{(Substitution)} \\ \iff & a^{qt} \cdot a^r \equiv 1 \bmod m && \text{(Properties of Exponents)} \\ \iff & (a^t)^q \cdot a^r \equiv 1 \bmod m && \text{(Properties of Exponents)} \\ \iff & a^r \equiv 1 \bmod m. && (a^t \equiv 1 \bmod m) \end{aligned}$$

But since $0 \leqslant r < t$, we will only have $a^r \equiv 1 \bmod m$ if $r = 0$. It follows that $a^n \equiv 1 \bmod m$ only if $t \mid n$.

$\boxed{\Leftarrow}$ Suppose now that $t \mid n$. Then $n = tk$, for some $k \in \mathbb{Z}$. So

$$\begin{aligned} & a^t \equiv 1 \bmod m \\ \Longrightarrow & (a^t)^k \equiv 1^k \bmod m && \text{(Power Rule)} \\ \Longleftrightarrow & a^{tk} \equiv 1 \bmod m && \text{(Properties of Exponents)} \\ \Longleftrightarrow & a^n \equiv 1 \bmod m, && \text{(Substitution)} \end{aligned}$$

as desired.

2. We know that the order of $\mathbb{Z}_m^*$ is $\varphi(m)$. Lagrange's Theorem states that the order of an element divides the order of the group, and since $a \in \mathbb{Z}_m^*$ has order t, it follows that $t \mid \varphi(m)$. ∎

Theorem 6.0.16 *Let the order of $a \in \mathbb{Z}_n^*$ be t. Then*

1. *$a^r \equiv a^s \bmod n$ if and only if $r \equiv s \bmod t$.*

2. *a^k has order t if and only if $\gcd(k, t) = 1$.*

Proof: Assume that $a \in \mathbb{Z}_n^*$ is order t modulo n.

1. $\boxed{\Rightarrow}$ Since a is an element of the group of units, a has a multiplicative inverse modulo n. Suppose that $a^r \equiv a^s \bmod n$, and without loss of generality, assume that $r \geqslant s$. Then

$$\begin{aligned} & a^r \equiv a^s \bmod n \\ \Longleftrightarrow & a^r \cdot a^{-s} \equiv a^s \cdot a^{-s} \bmod n && \text{(Multiplication Property of Equality)} \\ \Longleftrightarrow & a^{r-s} \equiv 1 \bmod n. && \text{(Properties of exponents)} \end{aligned}$$

But a has order t, which means that t is the smallest positive integer such that $a^t \equiv 1 \bmod n$. Thus, $t \mid r - s$, so $(r - s) = kt$ for some $k \in \mathbb{Z}$, and $(r - s) \equiv 0 \bmod t$. It follows that $r \equiv s \bmod t$, by definition of congruent.

$\boxed{\Leftarrow}$ Now assume that $r \equiv s \bmod t$. Then $r = s + kt$ for some $k \in \mathbb{Z}$, so $a^r \equiv a^{s+kt} \equiv a^s a^{kt} \equiv a^s (a^t)^k \equiv a^s \bmod n$.

2. $\boxed{\Rightarrow}$ Suppose that a and a^k both have order t modulo m. Assume that $\gcd(k, t) = d$, for some $d \in \mathbb{Z}^+$. Then $1 \equiv a^t \equiv (a^t)^{k/d} \equiv (a^k)^{t/d} \bmod m$. But a^k has order t, thus by Theorem 6.0.15, t/d is a multiple of t. So for some $l \in \mathbb{Z}$, we have

$$
\begin{aligned}
& t/d = tl \\
\iff & t = dtl && \text{(Multiplication Property of Equality)} \\
\iff & 1 = dl && \text{(Division Property of Equality)}
\end{aligned}
$$

But $d \in \mathbb{Z}^+$ and $l \in \mathbb{Z}$, so $d = 1$. Thus $\gcd(k, t) = 1$.

$\boxed{\Leftarrow}$ Suppose that $\gcd(k, t) = 1$, for some $k \in \mathbb{N}$. Let a^k have order s modulo m. Then since a has order t, $1 \equiv (a^t)^k \equiv (a^k)^t \bmod m$. But Theorem 6.0.15 states that t is a multiple of s, since a^k has order s. Thus, $t = js$ for some $j \in \mathbb{Z}$, and so $s \mid t$.

It is also true that $(a^k)^s \equiv a^{ks} \equiv 1 \bmod m$, so by Theorem 6.0.15, ks is a multiple of t, since a has order t. Thus $t \mid ks$. But by the hypothesis,

$\gcd(k,t) = 1$, thus by Theorem 4.3.12, $t \mid s$.

Now we have $s \mid t$ and $t \mid s$, which clearly implies that $s = t$, since both s and t are natural numbers. Thus a^k has order t modulo m as desired.

It follows that $a^r \equiv a^s \bmod n$ if and only if $r \equiv s \bmod t$ and a^k has order t if and only if $\gcd(k,t) = 1$. ∎

Recall that if $a \in \mathbb{Z}_n^*$ and $\langle a \rangle = \mathbb{Z}_n^*$, then a is said to be a primitive root of n. We will prove in Chapter 7 that every prime p has $\varphi(p)$ primitive roots, where φ is Euler's φ-function. For now we assume that any given prime p has at least one primitive root, and we use this assumption to prove the following Corollary.

Corollary 6.0.17 *If $\langle g \rangle = \mathbb{Z}_p^*$ for a prime p, then $\langle g^k \rangle = \mathbb{Z}_p^*$ if and only if $\gcd(k, p-1) = 1$.*

Proof: Assume that g is a primitive root of a prime p. Then g has order $\varphi(p) = p-1$. So $g^{p-1} \equiv 1 \bmod p$. By Theorem 6.0.16, g^k has order $p-1$ modulo p if and only if $\gcd(k, p-1) = 1$. In order for the least residue of g^k to be a primitive root of p, we must have $0 \leqslant g^k \bmod p < p$ and the order of g^k modulo p must be $\varphi(p)$. Both of those conditions are met if $\gcd(k, p-1) = 1$, in which case the least residue of g^k will be a primitive root of p. ∎

Definition 6.0.18 Let m, n be positive integers and let a be any integer, such that $\gcd(a, m) = 1$. Then we say that a is an n^{th} *power residue* modulo m if

$x^n \equiv a \bmod m$ has a solution. $\diamondsuit$

There are two specific cases of n^{th} power residues that we are concerned with in this thesis. We say that a is a quadratic residue if $x^2 \equiv a \bmod m$ has a solution. Similarly, if $x^3 \equiv a \bmod m$ has a solution, then a is a cubic residue.

Example 6.0.19 Let $m = 6$, $n = 2$, and $a = 2$ and consider $x^2 \equiv 2 \bmod 6$.

$$1^2 \equiv 1 \bmod 6$$

$$2^2 \equiv 4 \bmod 6$$

$$3^2 \equiv 3 \bmod 6$$

$$4^2 \equiv 4 \bmod 6$$

$$5^2 \equiv 1 \bmod 6$$

Thus 2 is not a quadratic residue modulo 6, since $x^2 \equiv 2 \bmod 6$ does not have a solution.

Now suppose that $m = 7$ and consider $x^2 \equiv 2 \bmod 7$.

$$1^2 \equiv 1 \bmod 7$$

$$2^2 \equiv 4 \bmod 7$$

$$3^2 \equiv 2 \bmod 7$$

$$4^2 \equiv 2 \bmod 7$$

$$5^2 \equiv 4 \bmod 7$$

$$6^2 \equiv 1 \bmod 7$$

We see that 3 and 4 are solutions, so 2 is a quadratic residue modulo 7. This idea of quadratic residues and nonresidues is going to play a key role in the quadratic reciprocity chapter. □

Recall that if $a \in \mathbb{Z}_n^*$ and $\langle a \rangle = \mathbb{Z}_n^*$, then a is a primitive root of n.

Theorem 6.0.20 *Let m be a positive integer that possesses primitive roots and let $\gcd(a, m) = 1$, for $a \in \mathbb{Z}$. Then a is an n^{th} power residue modulo m if and only if $a^{\varphi(m)/d} \equiv 1 \bmod m$, where $d = \gcd\big(n, \varphi(m)\big)$.*

Proof: Suppose m is a positive integer and $d = \gcd\big(n, \varphi(m)\big)$ for some $n \in \mathbb{N}$. Let g be a primitive root of m and let $a = g^j$ and $x = g^k$, for positive integers j and k. Then

$$\begin{aligned} & x^n \equiv a \bmod m \\ \iff & g^{nk} \equiv g^j \bmod m && \text{(Substitution)} \\ \iff & nk \equiv j \bmod \varphi(m). && \text{(Theorem 6.0.16)} \end{aligned}$$

Since $d \mid n$ and $d \mid \varphi(m)$, Theorem 6.0.5 tells us that $nk \equiv j \bmod \varphi(m)$ has a solution if and only if $d \mid j$. Furthermore, if a solution exists, there are exactly d of them. Suppose $d \mid j$. Then

$$\begin{aligned} a^{\varphi(m)/d} &\equiv (g^j)^{\varphi(m)/d} && \text{(Substitution)} \\ &\equiv \left(g^{\varphi(m)}\right)^{j/d} && \text{(Properties of exponents)} \\ &\equiv 1 \bmod m. && (g \text{ is a primitive root of } m) \end{aligned}$$

Thus if a is an n^{th} power residue, $a^{\varphi(m)/d} \equiv 1 \bmod m$.

Suppose now that $a^{\varphi(m)/d} \equiv 1 \bmod m$. Then

$$\begin{aligned}(g^j)^{\varphi(m)/d} &\equiv (g^{\varphi(m)})^{j/d} && \text{(Properties of exponents)}\\ &\equiv 1 \bmod m.\end{aligned}$$

This implies that $j\varphi(m)/d$ is a multiple of $\varphi(m)$, by Theorem 6.0.15. Thus, $j/d \in \mathbb{Z}$, so $d \mid j$. ∎

Note that this theorem really says that $x^n \equiv a \bmod m$ is solvable if and only if $a^{\varphi(m)/d} \equiv 1 \bmod m$. It also indicates that if a solution exists, then there are exactly $d = \gcd\big(n, \varphi(m)\big)$ of them. We are going to revisit this idea in Chapter 8.

6.1 Chinese Remainder Theorem

Theorem 6.1.1 *If* $a \equiv b \bmod m_1, a \equiv b \bmod m_2, \ldots, a \equiv b \bmod m_k$, *for* $a, b \in \mathbb{Z}$ *and* $m_1, m_2, \ldots, m_k \in \mathbb{Z}^+$, *then*

$$a \equiv b \bmod \big(\operatorname{lcm}(m_1, m_2, \ldots, m_k)\big).$$

Proof: Suppose $a \equiv b \bmod m_1, a \equiv b \bmod m_2, \ldots, a \equiv b \bmod m_k$. Then by the definition of congruent, $m_1 \mid (a-b), m_2 \mid (a-b), \ldots, m_k \mid (a-b)$. By Lemma 2.3.4,

$$\operatorname{lcm}(m_1, m_2, \ldots, m_k) \mid (a-b).$$

Thus, by the definition of congruent,

$$a \equiv b \bmod \big(\mathrm{lcm}(m_1, m_2, \ldots, m_k)\big). \qquad \blacksquare$$

Corollary 6.1.2 *Let a and b be integers and let $m_1, m_2, \ldots, m_k$ be positive integers such that for any $i, j \in \{1, \ldots, k\}$ and $i \neq j$, $\gcd(m_i, m_j) = 1$. Then*

$$a \equiv b \bmod m_1, a \equiv b \bmod m_2, \ldots, a \equiv b \bmod m_k$$

if and only if

$$a \equiv b \bmod (m_1 m_2 \ldots m_k).$$

Proof: Assume that a and b are integers and $m_1, m_2, \ldots, m_k$ are positive integers that are pairwise relatively prime.

$\boxed{\Rightarrow}$ Suppose $a \equiv b \bmod m_i$, for each $i \in \{1, \ldots, k\}$. By Lemma 2.3.3, $\mathrm{lcm}(m_1, m_2, \ldots, m_k) = m_1 m_2 \ldots m_k$, since the m_i are pairwise relatively prime. Thus, by Theorem 6.1.1,

$$a \equiv b \bmod (m_1 m_2 \ldots m_k).$$

$\boxed{\Leftarrow}$ Suppose that $a \equiv b \bmod (m_1 m_2 \ldots m_k)$. Then for each m_i, a is b more than a multiple of m_i. Thus $a \equiv b \bmod m_i$ for each m_i. $\blacksquare$

Note that the only restriction on a in this Corollary is that $a \in \mathbb{Z}$. Thus we can extend this result so that $x^n \equiv b \bmod (m_1 m_2 \ldots m_k)$ if and only if $x^n \equiv b \bmod m_i$ for each m_i and $n \in \mathbb{N}$. Thus we have a tool that allows us to break congruences up into a system of equations. We are going to use this result in our work with reciprocity in later chapters.

Lemma 6.1.3 *If $a_1, a_2, \ldots, a_k$ are all relatively prime to n, then $a_1 a_2 \ldots a_k$ is also relatively prime to n.*

Proof: Assume that $a_1 a_2 \ldots a_k$ is not relatively prime to n. Then there exists some prime p such that $p \mid n$ and $p \mid a_1 a_2 \ldots a_k$. Since p is prime, p must divide some a_i, which implies that $\gcd(a_i, n) \neq 1$. ∎

Lemma 6.1.4 *If a and b divide n and $\gcd(a, b) = 1$, then ab divides n.*

Proof: Assume that $\gcd(a, b) = 1$ for some $a, b \in \mathbb{Z}$. Then $ar + bs = 1$, for some $r, s \in \mathbb{Z}$, by Definition 4.3.10. This implies that $arn + bsn = n$. But $a \mid n$ means that $al = n$ for some $l \in \mathbb{Z}$. Likewise, since $b \mid n$, there is some $k \in \mathbb{Z}$, such that $bk = n$. Thus

$$
\begin{aligned}
& arn + bsn = n \\
\iff & arbk + bsal = n && \text{(Substitution)} \\
\iff & ab(rk + sl) = n. && \text{(Commutative, Distributive Properties)}
\end{aligned}
$$

Since $rk + sl \in \mathbb{Z}$, it follows that $ab \mid n$ by definition of divides. ∎

Lemma 6.1.5 *Suppose that each of $a_1, a_2, \ldots, a_k$ divide n and $\gcd(a_i, a_j) = 1$ for $i \neq j$. Then $a_1 a_2 \ldots a_k \mid n$.*

Proof: Assume that each of $a_1, a_2, \ldots, a_k$ divide some n and assume also that $\gcd(a_i, a_j) = 1$ for $i \neq j$. We use induction on k, where the base

case, $k = 2$, is handled by Lemma 6.1.4. Assume that the result holds for some $k - 1$, and consider k. Set $a = a_1 a_2 \dots a_{k-1}$ and $b = a_k$. Then $a \mid n$ by the induction hypothesis and $\gcd(a, b) = 1$, so by Lemma 6.1.4, $ab = a_1 a_2 \dots a_k$ divides n. ∎

Theorem 6.1.6 (Chinese Remainder Theorem) *Suppose* $m = m_1 m_2 \dots m_k$ *and* $\gcd(m_i, m_j) = 1$ *for* $i \neq j$. *Let* $b_1, b_2, \dots, b_k$ *be integers and consider the system of congruences:*

$$x \equiv b_1 \bmod m_1$$

$$x \equiv b_2 \bmod m_2$$

$$\vdots$$

$$x \equiv b_k \bmod m_k.$$

This system always has solutions, and any two solutions differ only by a multiple of m.

Proof: Let $n_i = \dfrac{m}{m_i}$. Then n_i is a product of integers that are all relatively prime to m_i, thus by Lemma 6.1.3, $\gcd(m_i, n_i) = 1$. By Theorem 4.3.11, there exist $x_i, y_i \in \mathbb{Z}$ such that $m_i x_i + n_i y_i = 1$. Let $e_i = n_i y_i$. Then $m_i x_i + e_i = 1$, which implies that $e_i = 1 - m_i x_i$, so $e_i \equiv 1 \bmod m_i$ by definition of congruent, and $e_i \equiv 0 \bmod m_j$, since $\gcd(m_i, m_j) = 1$ for all $j \neq i$.

Set $x_0 = \sum_{i=1}^{k} b_i e_i$. Then $x_0 \equiv b_i e_i \equiv b_i \bmod m_i$, and x_0 is a solution.

Suppose that x_1 is any other solution. Then $x_1 - x_0 \equiv 0 \bmod m_i$, for $i \in \{1, 2, \ldots, k\}$, or in other words, each of the m_i divides $(x_1 - x_0)$. Then by Lemma 6.1.5, we have $m \mid (x_1 - x_0)$, and it follows that the given system of congruences always has solutions, and any pair of solutions differs by some multiple of m. ∎

Chapter 7

Multiplicative Functions

We begin this chapter by defining multiplicative functions and relatively multiplicative functions. Each of the three sections of Chapter 7 is then devoted to a particular type of multiplicative, or relatively multiplicative, function. Section 1 explores two functions that pertain to the divisors of an integer and several results are established here as well. In Section 2, we examine Euler's φ-function and show that it is relatively multiplicative. We conclude the chapter by defining characters and then exploring their multiplicativity. Characters are going to show up again when we look at Gauss and Jacobi sums and cubic reciprocity.

Definition 7.0.7 Let R and R' be rings with Euclidean domains and consider $f : R \to R'$.

- f is a *multiplicative function* if $f(ab) = f(a)f(b)$.

- f is a *relatively multiplicative function* if whenever $\gcd(a, b) = 1$, then $f(ab) = f(a)f(b)$. $\diamondsuit$

Example 7.0.8 We've seen several examples of multiplicative functions already. In Example 5.3.2, we saw that $|ab| = |a| \cdot |b|$ for $a, b \in \mathbb{Z}$, so the absolute value function is multiplicative. We looked at norms in $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$ as well. By Example 5.3.5, the norm function on $\mathbb{Z}[i]$ is a multiplicative function. Similarly, by Theorem 5.4.3, the norm on $\mathbb{Z}[\omega]$ is multiplicative as well. $\square$

Example 7.0.9 Let $a = 3$ and $b = 4$. Recall that $\varphi(n)$ is Euler's φ-function, and it tells us how many positive integers are between 1 and n that are also relatively prime to n. So $\varphi(3) = 2$, since $1 \leqslant 1, 2 \leqslant 3$ and both 1 and 2 are relatively prime to 3. Similarly, $\varphi(4) = 2$ since 1 and 3 are the only positive integers less than and relatively prime to 4. If we look at $\varphi(12)$, we have $\varphi(12) = \varphi(3 \cdot 4) = 4$, since 1, 5, 7, and 11 are the only integers less than and relatively prime to 12. But this is exactly $\varphi(3)\varphi(4)$. We will shortly see that in general Euler's φ-function is a relatively multiplicative function. $\square$

Theorem 7.0.10 *Let $n \in \mathbb{Z}$ and let the prime-power decomposition of n be given by $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$. Then $f(n) = f\left(p_1^{e_1}\right) f\left(p_2^{e_2}\right) \dots f\left(p_k^{e_k}\right)$ if and only if f is a relatively multiplicative function.*

Proof: If $f(n) = f\left(p_1^{e_1}\right) f\left(p_2^{e_2}\right) \dots f\left(p_k^{e_k}\right)$, then it follows immediately that f is a relatively multiplicative function. On the other hand, simple in-

duction on k reveals that if f is a relatively multiplicative function, then $f(n) = f\left(p_1^{e_1}\right) f\left(p_2^{e_2}\right) \dots f\left(p_k^{e_k}\right)$. ∎

7.1 Divisors of an Integer

Definition 7.1.1 Let n be a positive integer. Then denote the *number of positive divisors of* n (including 1 and n) by $d(n)$. In other words,

$$d(n) = \sum_{d \mid n} 1.$$

Also, denote the *sum of the positive divisors of* n by $\sigma(n)$, where

$$\sigma(n) = \sum_{d \mid n} d.$$

The notation $\sum_{d \mid n}$ means to sum over all of the positive divisors of n. ♢

Example 7.1.2 Let $n = 48$. It is fairly straightforward to find that the divisors of 48 are $1, 2, 3, 4, 6, 8, 12, 16, 24$, and 48, so $d(48) = 10$. However, if we consider the factorizations $48 = 6 \cdot 8$ and $48 = 12 \cdot 4$, we see that $d(6) \cdot d(8) = 4 \cdot 4 = 16$ and $d(12) \cdot d(4) = 6 \cdot 3 = 18$. Since neither of these results agree with $d(48)$, we can see that $d(n)$ is not multiplicative. We shall see soon, however, that it is a relatively multiplicative function.

Similarly, we can see that $\sigma(48) = 124$, but $\sigma(6) \cdot \sigma(8) = 12 \cdot 15 = 180$ and $\sigma(12) \cdot \sigma(4) = 28 \cdot 7 = 196$. Thus $\sigma(n)$ is not multiplicative, but we will prove shortly that it is relatively multiplicative. □

Theorem 7.1.3 *If $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ is the prime-power decomposition of n, then*

1. $d(n) = d\big(p_1^{e_1}\big) d\big(p_2^{e_2}\big) \dots d\big(p_k^{e_k}\big)$

2. $\sigma(n) = \sigma\big(p_1^{e_1}\big) \sigma\big(p_2^{e_2}\big) \dots \sigma\big(p_k^{e_k}\big)$.

Proof: Let $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ be the prime-power decomposition of n. We use induction on k to prove parts 1 and 2 simultaneously.

Consider the base case $k = 1$. This yields $n = p_1^{e_1}$, so $d(n) = d\big(p_1^{e_1}\big)$ and $\sigma(n) = \sigma\big(p_1^{e_1}\big)$. Hence the two results hold. Assume that both results hold for some k.

Now consider $N = p_1^{e_1} p_2^{e_2} \dots p_{k+1}^{e_{k+1}} = n p_{k+1}^{e_{k+1}}$. Let $\{1, d_1, d_2, \dots, d_t\}$ be the set of divisors of n. Since $\gcd(n, p_{k+1}) = 1$, the divisors of N are as follows.

$$\begin{array}{ccccc} 1 & d_1 & d_2 & \dots & d_t \\ p_{k+1} & d_1 p_{k+1} & d_2 p_{k+1} & \dots & d_t p_{k+1} \\ & & \vdots & & \\ p_{k+1}^{e_{k+1}} & d_1 p_{k+1}^{e_{k+1}} & d_2 p_{k+1}^{e_{k+1}} & \dots & d_t p_{k+1}^{e_{k+1}} \end{array}$$

First note that the number of columns represents the number of divisors of n, and the number of rows gives us the number of divisors of $p_{k+1}^{e_{k+1}}$. Thus there are $d(n)$ columns and $d\big(p_{k+1}^{e_{k+1}}\big)$ rows, for a total of $d(n) d\big(p_{k+1}^{e_{k+1}}\big)$ divisors of N. But by the inductive assumption, $d(n) = d\big(p_1^{e_1}\big) d\big(p_2^{e_2}\big) \dots d\big(p_k^{e_k}\big)$, so $d(N) = d\big(p_1^{e_1}\big) d\big(p_2^{e_2}\big) \dots d\big(p_k^{e_k}\big) d\big(p_{k+1}^{e_{k+1}}\big)$.

Now observe that $(1 + d_1 + d_2 + \cdots + d_t)\big(1 + p_{k+1} + \cdots + p_{k+1}^{e_{k+1}}\big)$ yields the sum of all of the divisors of N. Thus

$$\begin{aligned}\sigma(N) &= (1 + d_1 + d_2 + \cdots + d_t)\big(1 + p_{k+1} + \cdots + p_{k+1}^{e_{k+1}}\big) && \text{(Definition of } \sigma\text{)}\\ &= \sigma(n)\sigma(p_{k+1}^{e_{k+1}}). && \text{(Definition of } \sigma\text{)}\end{aligned}$$

But $\sigma(n) = \sigma\big(p_1^{e_1}\big)\sigma\big(p_2^{e_2}\big)\ldots\sigma\big(p_k^{e_k}\big)$ by the inductive assumption, so it follows that $\sigma(N) = \sigma\big(p_1^{e_1}\big)\sigma\big(p_2^{e_2}\big)\ldots\sigma\big(p_{k+1}^{e_{k+1}}\big)$. ∎

7.2 Euler's φ-function

Theorem 7.2.1 *φ is relatively multiplicative.*

Proof: Assume that a and b are positive integers and $\gcd a, b = 1$. Without loss of generality, assume that $b > a$. Consider the integers from 1 to ab, laid out as follows.

$$\begin{array}{ccccc} 1 & 2 & 3 & \ldots & a \\ a+1 & a+2 & a+3 & \ldots & 2a \\ 2a+1 & 2a+2 & 2a+3 & \ldots & 3a \\ & \vdots & & & \\ (b-1)a+1 & (b-1)a+2 & (b-1)a+3 & \ldots & ba \end{array}$$

Note that in the first row, there are a total of $\varphi(a)$ elements that are relatively prime to a.

Consider the r^{th} column of the array.

$$r$$

$$a + r$$

$$2a + r$$

$$\vdots$$

$$(b-1)a + r$$

If $\gcd(a, r) = d$ and $d > 1$, then $d \mid r$ and $d \mid a$. But this implies that $d \mid ka + r$ for each $0 \leqslant k \leqslant b-1$. Thus, none of the elements in such a column is relatively prime to ab. Hence, the elements relatively prime to ab can only be found in columns whose first element is relatively prime to a. Since there are $\varphi(a)$ such columns, it remains only to show that there are exactly $\varphi(b)$ elements that are relatively prime to ab in each of those columns.

Consider the b elements in the r^{th} column modulo b. Choose two arbitrary elements from the column, say $ka + r$ and $ja + r$ and suppose that $ka + r \equiv ja + r \bmod b$. Then the congruence reduces to $ka \equiv ja \bmod b$. But since $\gcd(a, b) = 1$, this can be further simplified to $k \equiv j \bmod b$, by Corollary 4.3.20. However, $0 \leqslant j, k \leqslant b - 1$, so this can only be the case if $k = j$. Thus if k and j are distinct, then $ka + r \not\equiv ja + r \bmod b$. Since they were chosen arbitrarily, no pair of distinct elements in the r^{th} column is congruent modulo b, so their least residues modulo b must be a permutation of the b elements $0, 1, \ldots, b-1$. Since exactly $\varphi(b)$ of these least residues are relatively

prime to b, there are $\varphi(b)$ such elements in each of the $\varphi(a)$ columns of the array.

Thus, there are exactly $\varphi(a)\varphi(b)$ elements from 1 to ab that are relatively prime to ab, so $\varphi(ab) = \varphi(a)\varphi(b)$ when $\gcd(a, b) = 1$. ∎

Example 7.2.2 We know that 8 and 9 are relatively prime, and by the theorem above, $\varphi(72)$ should be the same as $\varphi(8)\varphi(9)$. It is easy to see that $\varphi(8) = 4$ and $\varphi(9) = 6$, so $\varphi(8)\varphi(9) = 24$. It can be verified by listing the numbers 1 to 72 and checking each of them, that there are exactly 24 that are relatively prime to 72. □

Theorem 7.2.3 *If p is prime, then $\varphi(p^n) = p^{n-1}(p-1)$ for all $n \in \mathbb{N}$.*

Proof: Assume p is prime and n is a positive integer. By definition of Euler's φ-function, $\varphi(p^n)$ is the number of integers a, such that $1 \leqslant a \leqslant p^n$ and $\gcd(a, p^n) = 1$. Since p is prime, the only integers in $\{1, \ldots, p^n\}$ that are not relatively prime to p^n are the multiples of p, namely $\{p, 2p, \ldots, (p^{n-1})p\}$. Since there are p^{n-1} such integers and a total of p^n integers in $\{1, \ldots, p^n\}$, $\varphi(n) = p^n - p^{n-1} = p^{n-1}(p-1)$. ∎

Example 7.2.4 We have already seen that $\varphi(9) = 6$, but if we apply the theorem, then we have $\varphi(3^2) = 3^{2-1}(3-1) = 3 \cdot 2 = 6$ as well. □

It is a tedious exercise to list the numbers from 1 to n when n starts to get big, so it's easy to see how these theorems can save a lot of time when

trying to find $\varphi(n)$ of something like 1361^5. Certainly 1361 is a relatively small prime when compared to some of the known primes, but 1361^5 is a 16 digit number, and it would take a huge amount of time to determine this result by hand.

Corollary 7.2.5 *If n has a prime decomposition given by $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, then $\varphi(n) = p_1^{e_1-1}(p_1-1)p_2^{e_2-1}(p_2-1)\dots p_k^{e_k-1}(p_k-1)$.*

Proof: Since $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, $\gcd\left(p_i^{e_i}, p_j^{e_j}\right) = 1$ for any pair $i \neq j$, and φ is relatively multiplicative, then $\varphi(n) = \varphi\left(p_1^{e_1}\right)\varphi\left(p_2^{e_2}\right)\dots\varphi\left(p_k^{e_k}\right)$. But we can apply Theorem 7.2.3 to the terms in the right hand side of the equation, which yields $\varphi(n) = p_1^{e_1}(p_1-1)p_2^{e_2-1}(p_2-1)\dots p_k^{e_k-1}(p_k-1)$, as desired. ∎

Example 7.2.6 Let $n = 830,297$. Then

$$\varphi(830,297) = \varphi(17^3 \cdot 13^2) = 17^2 \cdot 16 \cdot 13 \cdot 12 = 721,344,$$

by Corollary 7.2.5 □

Corollary 7.2.7 *If $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ is the prime decomposition of n, then*

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_k}\right).$$

Proof: Let $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, where each p_i for $i \in \{1, \dots, k\}$ is prime. From Corollary 7.2.5, we have

$$\begin{aligned}
\varphi(n) &= p_1^{e_1-1}(p_1 - 1) \cdot p_2^{e_2-1}(p_2 - 1) \dots p_k^{e_k-1}(p_k - 1) \\
&= \frac{p_1^{e_1}(p_1 - 1)}{p_1} \cdot \frac{p_2^{e_2}(p_2 - 1)}{p_2} \cdots \frac{p_k^{e_k}(p_k - 1)}{p_k} \\
&= p_1^{e_1}\left(1 - \frac{1}{p_1}\right) \cdot p_2^{e_2}\left(1 - \frac{1}{p_2}\right) \dots p_k^{e_k}\left(1 - \frac{1}{p_k}\right) \\
&= p_1^{e_1} \cdot p_2^{e_2} \cdot p_k^{e_k}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right) \\
&= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right),
\end{aligned}$$

as desired. ∎

Example 7.2.8 Suppose $n = 830,297$, as in the previous example. Then we have seen that $\varphi(830,297) = 721,344$. Applying Corollary 7.2.7 yields

$$\varphi(830,297) = 830,297 \cdot \frac{16}{17} \cdot \frac{12}{13} = 721,344,$$

which agrees with our previous result. □

Theorem 7.2.9 *If $n \geqslant 1$, then*

$$\sum_{d \mid n} \varphi(d) = n.$$

Example 7.2.10 Let $n = 6$. The divisors of 6 are 1, 2, 3, and 6, and $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, and $\varphi(6) = 2$. So $\sum_{d \mid 6} \varphi(d) = 1 + 1 + 2 + 2 = 6$. □

Proof: Assume $n \geqslant 1$. Consider the integers $\alpha \in \{1, 2, \dots, n\}$. Recall that we defined partitions in Definition 2.4.3. We want to use a similar

notion in this proof, and for each $\alpha \in \{1, \ldots, n\}$, place α in C_d if and only if $\gcd(\alpha, n) = d$. In other words, each of the C_i is going to be a cell containing one or more divisors d of n, and together they will form a partition of the set of divisors.

To illustrate this idea, consider $n = 8$. Then $\alpha \in \{1, 2, \ldots, 8\}$ and the divisors of n are $d \in \{1, 2, 4, 8\}$. Thus, we will have four subsets, where $C_1 = \{1, 3, 5, 7\}$, $C_2 = \{2, 6\}$, $C_4 = \{4\}$, and $C_8 = \{8\}$.

So $\alpha \in C_d$ if and only if $\gcd(\alpha, n) = d$. But $\gcd(\alpha, n) = d$ if and only if $\gcd(\alpha/d, n/d) = 1$. Thus, $\alpha \in C_d$ if and only if α/d is relatively prime to n/d. But by definition, the number of elements β such that $1 \leqslant \beta \leqslant n/d$ and $\gcd(\beta, n/d) = 1$ is $\varphi(n/d)$. Thus, there are $\varphi(n/d)$ elements in C_d, for each d. Also, there is exactly one cell C_d for each divisor d of n, so the total number of elements in all of the C_d is given by $\sum_{d|n} \varphi(n/d) = n$. But $\sum_{d|n} \varphi(n/d) = \sum_{d|n} \varphi(d)$, since the set of all n/d is a permutation of the set of all d. Hence, we have $\sum_{d|n} \varphi(d) = n$, as desired. ∎

Recall that if $a \in \mathbb{Z}_n^*$ and $\langle a \rangle = \mathbb{Z}_n^*$, then a is a primitive root of n.

Theorem 7.2.11 *Every prime p has $\varphi(p-1)$ primitive roots.*

Example 7.2.12 Let $p = 3$. Then we have $\varphi(p-1) = \varphi(2) = 1$, so we should expect 3 to have one primitive root, with order $\varphi(p) = \varphi(3) = 2$. $1^1 \equiv 1 \bmod 3$, but $2^1 \equiv 2 \bmod 3$ and $2^2 \equiv 1 \bmod 3$, thus the only primitive root of 3 is 2.

Now suppose that $p = 7$. Then $\varphi(p-1) = \varphi(6) = 2$. So we are

expecting two primitive roots, whose orders are $\varphi(7) = 6$. It can quickly be seen that 1, 2, 4, and 6 will not work, because they do not have the correct orders. But checking 3 and 5 gives

3^1	3^2	3^3	3^4	3^5	3^6	5^1	5^2	5^3	5^4	5^5	5^6
3	2	6	4	5	1	5	4	6	2	3	1

where the bottom row is the least residue of each of the entries in the top row, modulo 7. Both 3 and 5 have order 6, and thus both are primitive roots of 7. This together with the previous work tells us that in fact, 3 and 5 are the only two primitive roots of 7. □

Proof: Assume p is prime. By Theorem 7.2.11, we know that p has at least one primitive root, so suppose that g is a primitive root of p. By Corollary 6.0.17, we know that an element g^k is a generator of $\mathbb{Z}_p^*$ if and only if $\gcd(k, p-1) = 1$. Since there are $\varphi(p-1)$ such k, there are $\varphi(p-1)$ primitive roots of p. ∎

7.3 Multiplicative Characters

We are going to be working in the field $\mathbb{Z}/p\mathbb{Z}$, which is isomorphic to $\mathbb{Z}_p$. Recall that both $\mathbb{Z}_p^*$ and $\mathbb{C}^*$ are cyclic groups under multiplication. More specifically, $\mathbb{Z}_p^*$ is the group of units, and the elements are $\{1, 2, \ldots, p-1\}$.

Definition 7.3.1 Assume $p \in \mathbb{Z}$ is prime. A *multiplicative character* on $\mathbb{Z}_p^*$ is

a group homomorphism $\chi : \mathbb{Z}_p^* \to \mathbb{C}^*$, where $\chi(ab) = \chi(a)\chi(b)$ for all $a, b \in \mathbb{Z}_p^*$. The *trivial multiplicative character* is ε, where $\varepsilon(a) = 1$ for all $a \in \mathbb{Z}_p^*$. We can extend the domain of our characters to all of $\mathbb{Z}_p$ if for $\chi \neq \varepsilon$ we have $\chi(0) = 0$ and $\varepsilon(0) = 1$. $\diamondsuit$

Theorem 7.3.2 (Properties of multiplicative characters) *Let χ be a multiplicative character and let $a \in \mathbb{Z}_p^*$. Then*

1. $\chi(1) = 1$.
2. $\chi(a)$ *is a* $(p-1)^{st}$ *root of unity.*
3. $\chi(a^{-1}) = \big(\chi(a)\big)^{-1} = \overline{\chi(a)}$.

Before we prove this theorem, note that in Property 1, the 1 on the left hand side is the unity element of $\mathbb{Z}_p^*$, and the 1 on the right hand side is the complex number 1. Also, in Property 3, the bar is used to denote the complex conjugate of $\chi(a)$.

Proof: Assume p is prime. Suppose χ is a multiplicative character and let $a \in \mathbb{Z}_p^*$.

1. This is a direct consequence of the fact that χ is a homomorphism, since homomorphisms preserve identity.
2. Since p is prime and $a \in \{1, 2, \ldots, p-1\}$, $p \nmid a$, so by Fermat's Little

Theorem, we have $a^{p-1} \equiv 1 \bmod p$. So

$$\begin{aligned} 1 &= \chi(1) && \text{(Property 1 of multiplicative characters)} \\ &\equiv \chi(a^{p-1}) \bmod p && (a^{p-1} \equiv 1 \bmod p) \\ &= \big(\chi(a)\big)^{p-1} \bmod p, && \text{(Homomorphism Property)} \end{aligned}$$

and $\chi(a)$ is a $(p-1)^{st}$ root of unity by definition.

3. Since homomorphisms preserve inverses, $\chi(a^{-1}) = \big(\chi(a)\big)^{-1}$, thus we have $\chi(a)\big(\chi(a)\big)^{-1} = 1$. Recall that $\chi(a)$ and $\chi(a)^{-1}$ are elements of $\mathbb{C}^*$. From our work with norms in $\mathbb{Z}[i]$ in Example 5.3.5, we know that for $\alpha \in \mathbb{C}$, $N(\alpha) = \alpha\overline{\alpha}$. Also, each $\chi(a)$ is a root of unity, so $N\big(\chi(a)\big) = 1$. Putting these two things together gives us

$$N\big(\chi(a)\big) = 1 = \chi(a)\overline{\chi(a)}.$$

But $\chi(a)\big(\chi(a)\big)^{-1} = 1$ as well, which implies that $\big(\chi(a)\big)^{-1} = \overline{\chi(a)}$, which is the desired result. ∎

Theorem 7.3.3 *Let χ be a multiplicative character and extend the domain to include all of $\mathbb{Z}_p$ as discussed in Definition 7.3.1. Then*

$$\sum_{t=0}^{p-1} \chi(t) = \begin{cases} 0, & \chi \neq \varepsilon \\ \\ p, & \chi = \varepsilon. \end{cases}$$

Proof: Suppose $\chi = \varepsilon$. Then $\chi(a) = 1$ for all $a \in \mathbb{Z}_p$ and $\displaystyle\sum_{t=0}^{p-1} \chi(t) = p$. Suppose $\chi \neq \varepsilon$. Then there exists at least one element $a \in \mathbb{Z}_p$ such that

$\chi(a) \neq 1$. Let $\sum_{t=0}^{p-1} \chi(t) = T$. Then

$$\begin{aligned} \chi(a) \cdot T &= \sum_{t=0}^{p-1} \chi(a)\chi(t) \\ &= \sum_{t=0}^{p-1} \chi(at). \end{aligned}$$

Since $a, t \in \{0, 1, \ldots, p-1\}$, the set of all at as t ranges from 0 to $p-1$ is a permutation of $\{0, 1, \ldots, p-1\}$, thus $\sum_{t=0}^{p-1} \chi(at) = T$. So we have $\chi(a) \cdot T = T$ and $\chi(a) \neq 1$, and it follows that $T = 0$ as desired. ∎

Recall that if we have two multiplicative characters χ and γ, then their function multiplication is given by $\big(\chi\gamma\big)(a) = \chi(a)\gamma(a)$. In addition,

$$\chi(b^n) = \big(\chi(b)\big)^n = \chi^n(b).$$

Theorem 7.3.4 *The set of characters on $\mathbb{Z}_p$ is a cyclic group of order $p-1$ under the usual function multiplication. If $a \in \mathbb{Z}_p^*$ and $a \neq 1$, then there is a character χ such that $\chi(a) \neq 1$.*

Proof: Let χ and λ be characters on $\mathbb{Z}_p$ and let $a, b \in \mathbb{Z}_p^*$. Then

$$\big(\chi\lambda\big)(a) = \chi(a)\lambda(a),$$

by function multiplication. Also, since $\chi(a), \lambda(a) \in \mathbb{C}^*$ and $\mathbb{C}^*$ is a group, $\chi(a)\lambda(a) \in \mathbb{C}^*$. Now,

$$\begin{aligned}
\big(\chi\lambda\big)(ab) &= \chi(ab)\lambda(ab) && \text{(Function multiplication)} \\
&= \chi(a)\chi(b)\lambda(a)\lambda(b) && \text{(Multiplicative Characters)} \\
&= \chi(a)\lambda(a)\chi(b)\lambda(b) && \text{(Commutative Property in } \mathbb{C}^*) \\
&= \big(\chi\lambda\big)(a)\big(\chi\lambda\big)(b), && \text{(Multiplicative Characters)}
\end{aligned}$$

thus $\chi\lambda$ is a multiplicative character.

To show that there is an identity in this set, note that

$$\begin{aligned}
\big(\chi\varepsilon\big)(a) &= \chi(a)\varepsilon(a) && \text{(Function multiplication)} \\
&= \chi(a) \cdot 1 && \text{(Definition of } \varepsilon) \\
&= \chi(a) && \text{(1 is the unity element in } \mathbb{C}) \\
&= 1 \cdot \chi(a) \\
&= \varepsilon(a)\chi(a) && \text{(Definition of } \varepsilon) \\
&= \big(\varepsilon\chi\big)(a). && \text{(Function multiplication)}
\end{aligned}$$

To show that each element has a unique inverse, first define

$$\chi^{-1}(a) = \frac{1}{\chi(a)}.$$

Then

$$\begin{aligned}
\chi^{-1}(ab) &= \frac{1}{\chi(ab)} && \text{(Definition of } \chi^{-1}\text{)} \\
&= \frac{1}{\chi(a)\chi(b)} && (\chi \text{ is multiplicative}) \\
&= \frac{1}{\chi(a)}\frac{1}{\chi(b)} && \text{(Fraction multiplication)} \\
&= \chi^{-1}(a)\chi^{-1}(b), && \text{(Definition of } \chi^{-1}\text{)}
\end{aligned}$$

so χ^{-1} is multiplicative. Also, since $\chi^{-1}(a), \chi^{-1}(b) \in \mathbb{C}^*$, their product is clearly in $\mathbb{C}^*$ as well, so χ^{-1} is a character. Finally,

$$\begin{aligned}
\left(\chi\chi^{-1}\right)(a) &= \chi(a)\chi^{-1}(a) && \text{(Function multiplication)} \\
&= \frac{\chi(a)}{\chi(a)} && \text{(Definition of } \chi^{-1}(a)\text{)} \\
&= 1 && \text{(Arithmetic in } \mathbb{C}\text{)} \\
&= \varepsilon(a). && \text{(Definition of } \varepsilon\text{)}
\end{aligned}$$

Thus $\chi^{-1}(a)$ is the inverse of $\chi(a)$.

We know that function multiplication is associative, so that comes along for free. Thus the set of characters forms a multiplicative group.

It remains to show that this is a cyclic group. First recall that $\mathbb{Z}_p^*$ is a cyclic group, thus $h : \mathbb{Z}_p^* \to \mathbb{C}^*$ is completely determined by what it does to a generator g of $\mathbb{Z}_p^*$. Let $h(g) = e^{2\pi i/(p-1)}$. Then for $g^l \in \mathbb{Z}_p^*$, $h(g^l) = e^{2l\pi i/(p-1)}$, which is a $(p-1)^{st}$ root of unity, thus h is a character.

Now suppose that χ is a character. Then $\chi(g)$ is something of the form $e^{2k\pi i/(p-1)}$ for some k, so

$$\begin{aligned}
\chi(g) &= e^{2k\pi i/(p-1)} \\
&= \left(e^{2\pi i/(p-1)}\right)^k && \text{(Properties of exponents)} \\
&= \big(h(g)\big)^k.
\end{aligned}$$

But by the definition of the group operation on characters, $\big(h(g)\big)^k = h^k(g)$, thus $\chi = h^k$, and it follows that the group of characters is cyclic.

The fact that the group has order $p-1$ comes directly from Theorem 7.3.2, since there are $p-1$ roots of unity.

Now suppose $a \neq 1$, where $a \in \mathbb{Z}_p^*$. Then $a = g^j$ for some j, where $(p-1) \nmid j$. This yields

$$\begin{aligned}
h(a) &= \big(h(g)\big)^j && \text{(Substitution)} \\
&= e^{2j\pi i/(p-1)} && \text{(Definition of } h'(g)\text{)} \\
&\neq 1,
\end{aligned}$$

since j is not a multiple of $p-1$. ∎

Corollary 7.3.5 *Let $a \in \mathbb{Z}_p^*$, where $a \neq 1$. Then $\sum_{\chi} \chi(a) = 0$, where the sum is over all characters.*

Proof: Assume $a \in \mathbb{Z}_p^*$ and $a \neq 1$. Let $\sum_{\chi} \chi(a) = S$. By Theorem 7.3.4, there exists a character λ such that $\lambda(a) \neq 1$. So

$$\begin{aligned} \lambda(a) \cdot S &= \sum_{\chi} \lambda(a)\chi(a) && \text{(Multiply both sides by } \lambda(a)) \\ &= \sum_{\chi} \big(\lambda\chi\big)(a) && \text{(Function multiplication)} \\ &= S, \end{aligned}$$

since as we sum over all of the characters, the $\lambda\chi$ are just a permutation of the elements in the group of characters. Thus, we have $\lambda(a) \cdot S = S$ and $\lambda(a) \neq 1$, so it follows that $S = 0$. ∎

Theorem 7.3.6 *Let $a \in \mathbb{Z}_p^*$ and choose $n \in \mathbb{N}$ such that $n \mid p-1$. Then if $x^n = a$ is not solvable, there is a character χ such that*

1. $\chi^n = \varepsilon$.
2. $\chi(a) \neq 1$.

Proof: Let g be a generator of $\mathbb{Z}_p^*$. Define a function λ as in Theorem 7.3.4 by $\lambda(g^k) = e^{2\pi ik/(p-1)}$, and set $\chi = \lambda^{(p-1)/n}$. Then

$$\begin{aligned} \chi^n &= \big(\lambda^{(p-1)/n}\big)^n && \text{(Definition of } \chi) \\ &= \lambda^{p-1} && \text{(Properties of exponents)} \\ &= \varepsilon, && \text{(Lagrange's Theorem)} \end{aligned}$$

which satisfies Part 1.

To prove Part 2, observe that

$$\begin{aligned}
\chi(g) &= \big(\lambda(g)\big)^{(p-1)/n} && \text{(Definition of } \chi\text{)} \\
&= \lambda\big(g^{(p-1)/n}\big) && \text{(Homomorphism Property)} \\
&= e^{2\pi i(p-1)/n(p-1)} && \text{(Definition of } \lambda\text{)} \\
&= e^{2\pi i/n}, && \text{(Properties of exponents)}
\end{aligned}$$

and $e^{2\pi i/n}$ has order n in $\mathbb{C}^*$. Since g generates $\mathbb{Z}_p^*$ and $a \in \mathbb{Z}_p^*$, there is some j, such that $a = g^j$. But $x^n = a$ is not solvable, so $n \nmid j$. Thus

$$\begin{aligned}
\chi(a) &= \chi(g^j) && \text{(Substitution)} \\
&= \big(\lambda(g^j)\big)^{(p-1)/n} && \text{(Definition of } \chi\text{)} \\
&= \big(e^{2\pi ij/(p-1)}\big)^{(p-1)/n} && \text{(Definition of } \lambda\text{)} \\
&\neq 1,
\end{aligned}$$

since j is not a multiple of n. ∎

The use of characters plays a key role in regard to determining whether or not solutions to equations exist. Suppose $a \in \mathbb{Z}_p^*$ and consider $x^n = a$. Recall from Theorem 6.0.20 that solutions to this equation exist if and only if $a^{(p-1)/d} = 1$, where $d = \gcd(n, p-1)$. Furthermore, there are exactly d solutions. For now, the assumption will be made that $n \mid p-1$, so $d = n$.

We need to define a new notation before we look at the next theorem. If $a \in \mathbb{Z}_p$, then denote the number of solutions to the equation $x^n = a$ by $\mathcal{N}(x^n = a)$. When $n \mid p-1$, then we have the following result.

Theorem 7.3.7 *Let $a \in \mathbb{Z}_p^*$ and $n \in \mathbb{N}$ such that $n \mid p-1$. Then*

$$\mathcal{N}(x^n = a) = \sum_{\chi^n = \varepsilon} \chi(a),$$

where the sum is over all characters whose order divides n.

Proof: Suppose g generates $\mathbb{Z}_p^*$. Then if $\big(\chi(g)\big)^n = \varepsilon$, the value of $\chi(g)$ must be an n^{th} root of unity, so there are exactly n such characters.

Recall from the proof of Theorem 7.3.6 that there is a character λ with $\lambda(g) = e^{2\pi i/n}$. Because of the uniqueness of roots of unity, $\lambda, \lambda^2, \ldots, \lambda^n = \varepsilon$ are n distinct characters whose order divides n.

Now, if $a = 0$, then $x^n = 0$ has exactly one solution, $x = 0$. Also,

$$\begin{aligned}
\sum_{\chi^n = \varepsilon} \chi(0) &= \chi(0) + \chi^2(0) + \cdots + \chi^{n-1}(0) + \varepsilon(0) && \text{(Expansion of the sum)} \\
&= 0 + 0 + \cdots + 0 + 1 && \text{(Definition 7.3.1)} \\
&= 1.
\end{aligned}$$

So $\mathcal{N}(x^n = a) = 1 = \sum_{\chi^n = \varepsilon} \chi(0)$.

Suppose now that $a \neq 0$ and assume that $x^n = a$ is solvable. Then there is some $b \in \mathbb{Z}_p^*$ such that $b^n = a$. If $\chi^n = \varepsilon$, then

$$\begin{aligned}
\chi(a) &= \chi(b^n) && \text{(Substitution)} \\
&= \big(\chi(b)\big)^n && (\chi \text{ is multiplicative}) \\
&= \chi^n(b) && \text{(Definition of function multiplication)} \\
&= \varepsilon(b) && (\chi^n = \varepsilon) \\
&= 1. && \text{(Definition of } \varepsilon)
\end{aligned}$$

Since there are n such χ, $\sum_{\chi^n=\varepsilon} \chi(a) = n$. By Theorem 6.0.20, there are exactly $d = \gcd(n, p-1)$ solutions, but since $n \mid p-1$, we have $d = n$, so there are exactly n solutions, which agrees with the value of the sum.

Finally, suppose that $a \neq 0$ and assume that $x^n = a$ is not solvable. Set $T = \sum_{\chi^n=\varepsilon} \chi(a)$. By Theorem 7.3.6, there is a character λ, such that $\lambda^n = \varepsilon$ and $\lambda(a) \neq 1$. So $T = \sum_{\chi^n=\varepsilon} \chi(a)$ implies that

$$\begin{aligned}
\lambda(a) \cdot T &= \lambda(a) \cdot \sum_{\chi^n=\varepsilon} \chi(a) && \text{(Multiply both sides by } \lambda(a)) \\
&= \sum_{\chi^n=\varepsilon} \lambda(a) \cdot \chi(a) \\
&= \sum_{\chi^n=\varepsilon} \lambda\chi(a). && \text{(Function multiplication)}
\end{aligned}$$

But observe that the characters that satisfy $\chi^n = \varepsilon$ forms a subgroup of the group of characters. The identity element is present, since $\varepsilon^n = \varepsilon$, and certainly if $\chi^n = \varepsilon$ and $\lambda^n = \varepsilon$, then $\varepsilon = \chi^n\lambda^n = (\chi\lambda)^n$, so there is closure

under multiplication of characters. Also, $\left(\chi^{-1}\right)^n = \left(\chi^n\right)^{-1} = \varepsilon$, so each such character has an inverse element that is also contained in the set. Associativity comes for free from the group of characters, thus we have a subgroup. Hence it follows that as we sum $\lambda\chi(a)$ over all characters that satisfy $\chi^n = \varepsilon$, the result is one row of the group table for the subgroup, so $\lambda(a) \cdot T = T$. But this implies that $T = 0$, since $\lambda(a) \neq 1$. Therefore, $\mathcal{N}(x^n = a) = 0 = \sum_{\chi^n = \varepsilon} \chi(a)$. ∎

Chapter 8

Quadratic Reciprocity

We begin our exploration of quadratic reciprocity by defining quadratic residues and establishing results about solvability of quadratic congruences. We define Euler's Criterion as it pertains to solvability, and then establish a couple of results about the solvability of n^{th} power congruences.

In Section 2, we define the Legendre symbol and then prove several properties about it. We conclude the section by examining two examples that allow us to use the properties of the Legendre symbol to evaluate it.

The third section is devoted to the Law of Quadratic Reciprocity. We begin by stating the three parts of the theorem and then establish results to prove the first two parts. We offer up two different versions of the second part of the Law of Quadratic Reciprocity. Finally we prove the third part and then prove that several different forms of the theorem are in fact equivalent.

In section four, we define another symbol, the Jacobi symbol, and then prove several useful properties about it. We also compare and contrast the Jacobi symbol to the Legendre symbol, and conclude the section by proving the Reciprocity Law for the Jacobi symbol.

We wrap up Chapter 8 by looking at some of the more common applications of quadratic residues and the Law of Quadratic Reciprocity. These applications are in areas such as acoustics, cryptography, and graph theory.

8.1 Quadratic Residues

Definition 8.1.1 If $\gcd(a, m) = 1$, a is called a *quadratic residue* modulo m if the congruence $x^2 \equiv a \bmod m$ has a solution. Otherwise a is called a *quadratic nonresidue* modulo m. $\diamondsuit$

For the sake of simplicity in this chapter, quadratic residues may sometimes be referred to as residues, and quadratic nonresidues may be referred to as nonresidues.

Example 8.1.2 Consider the congruence $x^2 \equiv a \bmod 7$.

$$1^2 \equiv 1 \bmod 7$$

$$2^2 \equiv 4 \bmod 7$$

$$3^2 \equiv 2 \bmod 7$$

$$4^2 \equiv 2 \bmod 7$$

$$5^2 \equiv 4 \bmod 7$$

$$6^2 \equiv 1 \bmod 7$$

Since 7 is prime, 1, 2, and 4 are all relatively prime to 7, and thus each of the three is a residue modulo 7. On the other hand, 3, 5, and 6 are nonresidues modulo 7, since $x^2 \equiv 3 \bmod 7$, $x^2 \equiv 5 \bmod 7$, and $x^2 \equiv 6 \bmod 7$ do not have solutions.

Observe that this partitions $\mathbb{Z}_7^*$ into two equal sets of residues and nonresidues. Furthermore, each of the residues has exactly two solutions. □

Theorem 8.1.3 *Suppose p is an odd prime. If $p \nmid a$, then $x^2 \equiv a \bmod p$ either has exactly two solutions or it has no solution.*

Proof: Assume that $p \nmid a$ for some $a \in \mathbb{Z}$ and some odd prime p. Suppose that r is a solution to $x^2 \equiv a \bmod p$. Then $p - r$ is also a solution, since

$$(p - r)^2 \equiv p^2 - 2pr + r^2 \equiv r^2 \bmod p.$$

Furthermore, we claim that the two solutions are distinct. Assume that this is not the case. Then $r \equiv (p - r) \bmod p$.

$$
\begin{aligned}
& r \equiv (p - r) \bmod p \\
\iff & 2r \equiv p \bmod p && \text{(Arithmetic)} \\
\iff & 2r \equiv 0 \bmod p. && (p \equiv 0 \bmod p)
\end{aligned}
$$

But p is odd, so $\gcd(2, p) = 1$. This implies that $r \equiv 0 \bmod p$. However, $p \nmid r$, so this is impossible. Thus, if r is a solution, $p - r$ is a different solution.

Since $\mathbb{Z}_p$ is a field when p is prime, there can be at most two solutions to this congruence. Thus, if $x^2 \equiv a \bmod p$ has a solution, it has exactly two of them, and they are $x = r$ and $x = p - r$. ∎

Recall from the Group Theory chapter that $a \in \mathbb{Z}_n^*$ is called a primitive root of n if a is a generator of $\mathbb{Z}_n^*$.

Lemma 8.1.4 *If g is a primitive root of p, then $g^{(p-1)/2} \equiv -1 \bmod p$.*

Proof: Assume that g is a primitive root of some prime p. Since there are $\varphi(p) = p - 1$ elements in $\mathbb{Z}_p^*$, we know that the order of g is $\varphi(p)$, thus $g^{p-1} \equiv 1 \bmod p$. Hence

$$
\begin{aligned}
& g^{p-1} \equiv 1 \bmod p \\
\iff & \left(g^{(p-1)/2}\right)^2 \equiv 1 \bmod p && \text{(Properties of exponents)} \\
\iff & g^{(p-1)/2} \cdot g^{(p-1)/2} \equiv 1 \bmod p. && \text{(Properties of exponents)}
\end{aligned}
$$

This implies that either $g^{(p-1)/2} \equiv 1 \bmod p$ or $g^{(p-1)/2} \equiv -1 \bmod p$. But g has order $p-1$ since g is a primitive root of p, so $g^{(p-1)/2} \equiv -1 \bmod p$. ∎

Example 8.1.5 Recall that we examined $\mathbb{Z}_{19}^*$ in Example 4.3.29. We saw that 2, 3, 10, 13, 14, and 15 are the generators and primitive roots of 19. Applying the lemma to 2 yields

$$2^{(19-1)/2} \equiv 2^9 \equiv -1 \bmod 19.$$

Similar calculations hold for each of the other primitive roots as well.

Note that the converse of the lemma is not true. We can easily see that

$$8^9 \equiv \left(2^3\right)^9 \equiv \left(2^9\right)^3 \equiv -1 \bmod 19.$$

However,

$$8^1 \equiv 8 \bmod 19$$

$$8^2 \equiv 7 \bmod 19$$

$$8^3 \equiv 18 \bmod 19$$

$$8^4 \equiv 11 \bmod 19$$

$$8^5 \equiv 12 \bmod 19$$

$$8^6 \equiv 1 \bmod 19,$$

so 8 is not a primitive root of 19, since it is not a generator of $\mathbb{Z}_{19}^*$. □

Lemma 8.1.6 *Let p be prime with primitive root g and let $a = g^k$. Then $x^2 \equiv a \bmod p$ has a solution if and only if k is even.*

Proof: $\boxed{\Rightarrow}$ Assume that $x^2 \equiv a \bmod p$ has a solution, say g^l, for some l. Then $\left(g^l\right)^2 \equiv a \bmod p$, which implies that $g^{2l} \equiv a \bmod p$. Thus $k = 2l$, so k is even.

$\boxed{\Leftarrow}$ Assume that k is even. Then

$$x^2 \equiv g^k \bmod p \iff x^2 \equiv \left(g^{k/2}\right)^2 \bmod p,$$

but since k is even, $\dfrac{k}{2}$ is an integer, thus $x^2 \equiv g^k \bmod p$ has a solution, namely $g^{k/2}$. ∎

Theorem 8.1.7 (Euler's Criterion) *If p is an odd prime and $p \nmid a$, then*

$$a^{(p-1)/2} \equiv \begin{cases} 1 \bmod p, & \text{if } x^2 \equiv a \bmod p \text{ has a solution} \\ -1 \bmod p, & \text{if } x^2 \equiv a \bmod p \text{ has no solution.} \end{cases}$$

Proof: Let p be an odd prime with primitive root g. Then $g \in \mathbb{Z}_p^*$ and the order of g modulo p is $\varphi(p)$, so $g^{p-1} \equiv 1 \bmod p$.

Consider the congruence $x^2 \equiv a \bmod p$. Since $a \in \mathbb{Z}_p^*$, $a \equiv g^k \bmod p$, for some $1 \leqslant k \leqslant p-1$. If a solution to the congruence exists, then k is even, by Lemma 8.1.6. Thus

$$\begin{aligned} a^{(p-1)/2} &\equiv \left(g^k\right)^{(p-1)/2} \bmod p && \text{(Substitution)} \\ &\equiv \left(g^{p-1}\right)^{k/2} \bmod p && \text{(Properties of exponents)} \\ &\equiv 1 \bmod p. && \text{(Fermat's Little Theorem)} \end{aligned}$$

So $a^{(p-1)/2} \equiv 1 \bmod p$ if a solution exists.

Now, one direction of Lemma 8.1.6 says that if there is a solution to $x^2 \equiv a \bmod p$, then k is even. Thus the contrapositive says that if k is odd, then there is no solution. Assume that k is odd. Then since $a \equiv g^k \bmod p$,

$$\begin{aligned} a^{(p-1)/2} &\equiv \left(g^k\right)^{(p-1)/2} \bmod p && \text{(Substitution)} \\ &\equiv \left(g^{(p-1)/2}\right)^k \bmod p && \text{(Properties of exponents)} \\ &\equiv (-1)^k \bmod p && \text{(Lemma 8.1.4)} \\ &\equiv -1 \bmod p. && (k \text{ is odd}) \end{aligned}$$

Combining these results yields $a^{(p-1)/2} \equiv 1 \bmod p$ if $x^2 \equiv a \bmod p$ has a solution, and $a^{(p-1)/2} \equiv -1 \bmod p$ if $x^2 \equiv a \bmod p$ has no solution. ∎

Example 8.1.8 By Example 8.1.2, $x^2 \equiv 3 \bmod 7$ has no solution, and Euler's Criterion yields $3^{(7-1)/2} \equiv -1 \bmod 7$. There are two solutions to $x^2 \equiv 4 \bmod 7$, and Euler's Criterion yields $4^{(7-1)/2} \equiv 1 \bmod 7$.

If we examine $x^2 \equiv 1 \bmod 7$, we know that there are also two solutions and Euler's Criterion yields $1^{(7-1)/2} \equiv 1 \bmod 7$. In fact, since $1^k = 1$ for any $k \in \mathbb{N}$, 1 will always be a quadratic residue for any prime p. This follows from the fact that $x^2 - 1 \equiv 0 \bmod p$ always has exactly two solutions, since $\mathbb{Z}_p$ is a field. □

Corollary 8.1.9 *There are as many quadratic residues as quadratic non-residues modulo p.*

Proof: Assume that $x^2 \equiv a \bmod p$ has a solution for some prime p. Then by Euler's Criterion, $a^{(p-1)/2} \equiv 1 \bmod p$. Clearly $\frac{p-1}{2} \mid p-1$, so by Lemma 6.0.10, we know that $a^{(p-1)/2} \equiv 1 \bmod p$ has exactly $\frac{p-1}{2}$ solutions. Thus there are exactly $\frac{p-1}{2}$ values of a for which Euler's Criterion indicates that $x^2 \equiv a \bmod p$ has a solution, so there are exactly $\frac{p-1}{2}$ quadratic residues. But there are $p-1$ elements in $\mathbb{Z}_p^*$, so there are $p-1-\left(\frac{p-1}{2}\right) = \frac{p-1}{2}$ nonresidues as well. ∎

Theorem 8.1.10 *Suppose p is an odd prime. Let $a \in \mathbb{Z}$ and $n \in \mathbb{N}$ such that $p \nmid a$ and $p \nmid n$. Then if $x^n \equiv a \bmod p$ is solvable, so is $x^n \equiv a \bmod p^e$ for all $e \geqslant 1$. Furthermore, for any given n, these congruences have the same number of solutions.*

Example 8.1.11 Consider the congruence $x^2 \equiv 2 \bmod 5$.

x	1	2	3	4
$x^2 \bmod 5$	1	4	4	1

Note that none of the least residues is equivalent to 2 modulo 5, thus our congruence has no solution. If $e = 2$, the congruence becomes $x^2 \equiv 2 \bmod 25$.

x	1	2	3	4	5	6	7	8	9	10	11	12
$x^2 \bmod 25$	1	4	9	16	0	11	24	14	6	0	21	19
x	13	14	15	16	17	18	19	20	21	22	23	24
$x^2 \bmod 25$	19	21	0	6	14	24	11	0	16	9	4	1

Again we do not have a least residue that is equivalent to 2 modulo 25, so this congruence also has no solution.

Consider $x^2 \equiv 4 \bmod 5$. From the first table, we can see that $x = 2$ and $x = 3$ are both solutions. Thus the congruence is solvable for $e = 1$. If $e = 2$, we can see from the second table that $x = 2$ and $x = 23$ are both solutions to $x^2 \equiv 4 \bmod 25$. □

Proof: Assume that p is an odd prime and let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ be such that $p \nmid n$ and $p \nmid a$. Consider $x^n \equiv a \bmod p$.

Suppose $n = 1$. Then $x \equiv a \bmod p$, which is trivially solvable, and the solution is simply the least residue of a modulo p. Likewise, $x \equiv a \bmod p^e$ is also trivially solvable, and both congruences have the same solution.

Assume that $n \geqslant 2$. We use induction on e. For $e = 1$, we can see that $x^n \equiv a \bmod p$ and $x^n \equiv a \bmod p^e$ are the same congruence, so the theorem holds regardless of whether or not a solution exists. Assume that the result holds for some e.

Now examine $e + 1$. Assume that $x^n \equiv a \bmod p^e$ has a solution, say x_0. Set $x_1 = x_0 + bp^e$, where b is yet to be determined. Then by the binomial expansion theorem,

$$\begin{aligned} x_1^n &= (x_o + bp^e)^n \\ &= \binom{n}{0} x_0^n + \binom{n}{1} x_0^{n-1} bp^e + \binom{n}{2} x_0^{n-2} (bp^e)^2 + \cdots + \binom{n}{n} (bp^e)^n. \end{aligned}$$

We are working modulo p^{e+1}, and it is clear that the terms that contain $(p^e)^j$ for $2 \leqslant j \leqslant n$ will be congruent to 0 modulo p^{e+1}.

Collecting the leftover terms leaves us with $x_1^n \equiv x_0^n + nx_0^{n-1}bp^e \bmod p^{e+1}$. We want this congruence to be of the form $x_1^n \equiv a \bmod p^{e+1}$, for two reasons. First, it will indicate that x_1 is a solution to $x^n \equiv a \bmod p^{e+1}$, which is the result we are trying to achieve via induction. The second reason is that if x_1 is a solution, then both $x^n \equiv a \bmod p^e$ and $x^n \equiv a \bmod p^{e+1}$ have the same number of solutions, since x_1 was constructed from an arbitrary solution of $x^n \equiv a \bmod p^e$. To achieve this goal, we need to take a step back and examine some things.

By assumption, $x_0^n \equiv a \bmod p^e$. By the definition of congruent, there exists $k \in \mathbb{Z}$ such that $p^e k = a - x_0^n$. Solving this equation for k yields $k = \dfrac{a - x_0^n}{p^e}$, so we know that $\dfrac{a - x_0^n}{p^e} \in \mathbb{Z}$. Recall that $x_1 = x_0 + bp^e$ and consider

$$
\begin{aligned}
& nx_0^{n-1}b \equiv \frac{a - x_0^n}{p^e} \bmod p \\
\iff & nx_0^{n-1}b = \frac{a - x_0^n}{p^e} + jp, \text{ for some } j && \text{(Definition of congruent)} \\
\iff & nx_0^{n-1}bp^e = a - x_0^n + jp^{e+1}, \text{ for some } j && \text{(Arithmetic)} \\
\iff & x_0^n + nx_0^{n-1}bp^e = a + jp^{e+1}, \text{ for some } j && \text{(Arithmetic)} \\
\iff & x_0^n + nx_0^{n-1}bp^e \equiv a \bmod p^{e+1} && \text{(Definition of congruent)} \\
\iff & x_1^n \equiv a \bmod p^{e+1}. && \text{(Substitution)}
\end{aligned}
$$

Note that $nx_0^{n-1}b \equiv \dfrac{a - x_0^n}{p^e} \bmod p$ is a linear congruence in b. We want to find a solution, if one exists. Recall that Theorem 6.0.5 states that if $\gcd(nx_0^{n-1}, p) = 1$, then there is a solution. Since $p \nmid n$ and $x_0 \not\equiv 0 \bmod p$ by hypothesis, $p \nmid nx_0^{n-1}$. Thus there is exactly one $b \in \mathbb{Z}$ that will satisfy the congruence.

With this value of b and the work done above, we have established that $x_1^n \equiv x_0^n + nx_0^{n-1}bp^e \equiv a \bmod p^{e+1}$, as required.

Suppose now that $x^n \equiv a \bmod p$ has no solution. It is clear that $x^n \equiv a \bmod p^e$ will also have no solution. So by induction on e, the first part of the theorem holds.

It remains to show that for any given n, the congruences have the same number of solutions. Recall that by Theorem 6.0.20, $x^n \equiv a \bmod m$ has a solution if and only if $a^{\varphi(m)/d} \equiv 1 \bmod m$, where $d = \gcd\big(n, \varphi(m)\big)$. In terms of our situation, this means that $x^n \equiv a \bmod p$ has a solution if and only if $a^{\varphi(p)/d_1} \equiv 1 \bmod p$, where $d_1 = \gcd\big(n, \varphi(p)\big)$, and $x^n \equiv a \bmod p^e$ has a solution if and only if $a^{\varphi(p^e)/d_2} \equiv 1 \bmod p^e$, where $d_2 = \gcd\big(n, \varphi(p^e)\big)$. So, in order to show that the congruences have the same number of solutions, we need to show that $\gcd\big(n, \varphi(p)\big) = \gcd\big(n, \varphi(p^e)\big)$.

Let $d = \gcd\big(n, \varphi(p)\big)$. We know that since p is prime, $\varphi(p) = p - 1$, so $d = \gcd(n, p-1)$. By definition of greatest common divisor, we have $d \mid n$ and $d \mid (p-1)$, which imply that $ds = n$ and $dt = p - 1$, for some $s, t \in \mathbb{Z}$.

Now we want to show that $\gcd\big(n, \varphi(p^e)\big) = d$ as well. To do this, we first refer back to Theorem 7.2.3 to find that $\varphi(p^e) = p^{e-1}(p-1)$. Thus, we are actually trying to find $\gcd\big(n, p^{e-1}(p-1)\big)$. We already have $d \mid n$ and $d \mid (p-1)$. The final step is to note that since p is prime, $d \nmid p^{e-1}$, thus $\gcd\big(n, \varphi(p^e)\big) = d$ as desired, and both congruences have the same number of solutions, regardless of the value of n. ∎

Recall that in Theorem 6.0.20, we saw that if m is a positive integer that has primitive roots and a and m are relatively prime, then a is an n^{th} power residue modulo m if and only if $a^{\varphi(m)/d} \equiv 1 \bmod m$, where $d = \gcd\big(n, \varphi(m)\big)$. Recall also that m having primitive roots means that there is some element $g \in \mathbb{Z}_m^*$, such that $\langle g \rangle = \mathbb{Z}_m^*$.

Consider the congruence $x^n \equiv a \bmod m$, where $m \in \mathbb{Z}^+$. We can express m by its prime-power decomposition, so that $m = 2^e p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, where each p_i is distinct and e and each e_i are natural numbers. Then by Corollary 6.1.2, $x^n \equiv a \bmod 2^e p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ can be written as the system of congruences

$$\begin{aligned} x^n &\equiv a \bmod 2^e \\ x^n &\equiv a \bmod p_1^{e_1} \\ &\vdots \\ x^n &\equiv a \bmod p_k^{e_k}, \end{aligned}$$

so $x^n \equiv a \bmod 2^e p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ is solvable if and only if the system of congruences is solvable.

We proved in Theorem 7.2.11 that every prime has $\varphi(p-1)$ primitive roots, which means that every prime possesses at least one primitive root. If we first consider the odd prime powers of m, then Theorem 6.0.20 applies and provides the criteria under which the last k congruences of the system have solutions. If $e = 0$, then m is odd, so our system does not contain the congruence $x^n \equiv a \bmod 2^e$. Thus we can assume that $e \neq 0$, and we are left with the question of whether or not the congruence $x^n \equiv a \bmod 2^e$ has solutions.

Since 1 is a primitive root of 2 and 3 is a primitive root of 4, we can also apply Theorem 6.0.20 to $x^n \equiv a \bmod 2^e$ in the cases $e = 1$ and $e = 2$. This reduces our problem to determining whether or not we can solve the congruence $x^n \equiv a \bmod 2^e$ if $e \geqslant 3$.

Proposition 8.1.12 *Suppose that a is odd and $e \geqslant 3$. Consider the congruence $x^n \equiv a \bmod 2^e$.*

1. *If n is odd, a unique solution always exists.*

2. *If n is even, a solution exists if and only if $a \equiv 1 \bmod 4$ and $a^{(2^{e-2})/d} \equiv 1 \bmod 2^e$, where $d = \gcd\left(n, 2^{e-2}\right)$. When a solution exists, there are exactly $2d$ of them.*

The proof of this proposition can be found in [8].

Theorem 8.1.13 *Let 2^l be the highest power of 2 dividing n. Suppose that a is odd and $x^n \equiv a \bmod 2^{2l+1}$ is solvable. Then $x^n \equiv a \bmod 2^e$ is solvable for all $e \geqslant 2l+1$. Moreover, all of these congruences have the same number of solutions.*

Example 8.1.14 Let $n = 6$. Then since $2^1 \mid 6$, we have $l = 1$. Suppose that $x^6 \equiv a \bmod 2^3$ is solvable.

$$1^6 \equiv 1 \bmod 8$$

$$2^6 \equiv 0 \bmod 8$$

$$3^6 \equiv 1 \bmod 8$$

$$4^6 \equiv 0 \bmod 8$$

$$5^6 \equiv 1 \bmod 8$$

$$6^6 \equiv 0 \bmod 8$$

$$7^7 \equiv 1 \bmod 8$$

The theorem states that a needs to be odd, so if $a = 1$, we have the possible solutions $x = 1$, $x = 3$, $x = 5$, or $x = 7$. Also, if $x^6 \equiv a \mod 2^3$ is solvable, then so is $x^6 \equiv a \bmod 2^e$, for all $e \geqslant 3$.

If we examine the congruence for $e = 4$, we have $x^6 \equiv 1 \bmod 16$. Clearly $x = 1$ is also a solution here, so this congruence is solvable. In fact, 1 will be a solution for any positive choice of e, so the result holds. □

This proof is going to be very similar to the proof of Theorem 8.1.10.

Proof: Assume that $x^n \equiv a \bmod 2^m$ has a solution for some $m \geqslant 2l+1$. Let this solution be x_0 and let $x_1 = x_0 + 2^{m-l}b$. Then by the binomial expansion theorem,

$$\begin{aligned} x_1^n &= \left(x_o + 2^{m-l}b\right)^n \\ &= \binom{n}{0}x_0^n + \binom{n}{1}x_0^{n-1}2^{m-l}b + \binom{n}{2}x_0^{n-2}\left(2^{m-l}b\right)^2 + \cdots + \binom{n}{n}\left(2^{m-l}b\right)^n \\ &= x_0^n + nx_0^{n-1}2^{m-l}b + \binom{n}{2}x_0^{n-2}2^{2m-2l}b^2 + \cdots + \binom{n}{n}2^{mn-ln}b^n. \end{aligned}$$

Now we want to examine the right hand side modulo 2^{m+1}. Notice that if $m = 2l + 1$, then

$$\begin{aligned} 2m - 2l &= 2(2l+1) - 2l && \text{(Substitution)} \\ &= 4l + 2 - 2l && \text{(Distributive Property)} \\ &= 2l + 2 && \text{(Arithmetic)} \\ &= m + 1. && \text{(Substitution)} \end{aligned}$$

Thus $\binom{n}{2}x_0^{n-2}2^{2m-2l}b^2 \equiv 0 \bmod 2^{m+1}$ regardless of m, since $m \geqslant 2l+1$. The terms that follow this one will also be equivalent to 0 modulo 2^{m+1}, since their powers of 2 will be even higher, so $x_1^n \equiv x_0^n + nx_0^{n-1}2^{m-l}b \bmod 2^{m+1}$.

We need this congruence to be of the form $x_1^n \equiv a \bmod 2^{m+1}$. To that end, recall that $x_0^n \equiv a \bmod 2^m$. This implies that there exists $k \in \mathbb{Z}$ such that $a - x_0^n = 2^m k$, so $k = \dfrac{a - x_0^n}{2^m} \in \mathbb{Z}$. We need to find $b \in \mathbb{Z}$ such that $nx_0^{n-1}b \equiv \dfrac{a - x_0^n}{2^{m-l}} \bmod 2^{l+1}$. This is a linear congruence in b, so we can apply Theorem 6.0.5. Then if $\gcd\left(nx_0^{n-1}, 2^{l+1}\right) = d = 1$, a unique solution exists.

Since $2^{l+1} \nmid nx_0^{n-1}$ by hypothesis, $d = 1$. Thus there exists exactly one b that satisfies the congruence.

Since $nx_0^{n-1}b \equiv \dfrac{a - x_0^n}{2^{m-l}} \bmod 2^{l+1}$, there exists some $j \in \mathbb{Z}$ such that $s^{l+1}j = 2^{m-l}nx_0^{n-1}b - \dfrac{a - x_0^n}{2^{m-l}}$, by definition of congruent. Clearing fractions and simplifying this equation yields $2^{m+1}j + a = 2^{m-l}nx_0^{n-1}b + x_0^n$. But this implies that $2^{m-l}nx_0^{n-1}b + x_0^n \equiv a \bmod 2^{m+1}$. With this value of b, we have $x_1^n \equiv x_0^n + 2^{m-l}nx_0^{n-1}b \equiv a \bmod 2^{m+1}$, which is exactly the result we needed.

Finally, we need to show that for any n, the congruences have the same number of solutions. We saw in Theorem 6.0.20 that if one solution exists, then there are exactly $\gcd\big(n, \varphi(p^e)\big)$ solutions. Thus we need to show that $\gcd\big(n, \varphi(p)\big) = \gcd\big(n, \varphi(p^e)\big)$.

Let $d = \gcd\big(n, \varphi(p)\big) = \gcd(n, p-1)$. Then $d \mid n$ and $d \mid p-1$. We need to establish that $d = \gcd\big(n, \varphi(p^e)\big)$. Recall from Theorem 7.2.3 that $\varphi(p^e) = p^{e-1}(p-1)$. Thus we need $d = \gcd\big(n, p^{e-1}(p-1)\big)$. Since p is prime, $d \nmid p^{e-1}$, but $d \mid n$ and $d \mid p-1$, so $\gcd\big(n, p^{e-1}(p-1)\big) = d$ as required. Thus both congruences have exactly the same number of solutions, regardless of the value of n. ∎

Theorem 8.1.15 *Let $m = 2^e p_1^{e_1} \dots p_k^{e_k}$ be the prime decomposition of m, and suppose that $\gcd(a, m) = 1$. Then $x^2 \equiv a \bmod m$ is solvable if and only if the following conditions are satisfied:*

1. *If $e = 2$, then $a \equiv 1 \bmod 4$.*

If $e \geqslant 3$, *then* $a \equiv 1 \bmod 8$.

2. *For each* $1 \leqslant i \leqslant k$, *we have* $a^{(p_i-1)/2} \equiv 1 \bmod p_i$.

Before we prove this theorem, recall that we begin looking at this congruence in the preamble to Theorem 8.1.12. We said that $x^n \equiv a \bmod m$ could be broken down into a system of congruences, and that a solution exists if and only if the system is solvable. Then in Theorem 8.1.12, it was stated that if n is even, then if a solution exists, there are certain conditions on a that must be satisfied. This theorem takes that idea one step further and considers the conditions for specific values of e. The case $e = 1$ is not addressed by this theorem, because if $e = 1$, then $m = 2p_1^{e_1} \dots p_k^{e_k}$. Since 2 and each odd prime power possess primitive roots, then solvability of each of the congruences in this system is covered by Theorem 6.0.20.

Proof: Let $m = 2^e p_1^{e_1} \dots p_k^{e_k} \in \mathbb{Z}$ and suppose $\gcd(a, m) = 1$ for some $a \in \mathbb{Z}$. Consider the congruence $x^2 \equiv a \bmod (2^e p_1^{e_1} \dots p_k^{e_k})$. By Corollary 6.1.2, $x^2 \equiv a \bmod (2^e p_1^{e_1} \dots p_k^{e_k})$ is equivalent to the system of congruences

$$x^2 \equiv a \bmod 2^e$$

$$x^2 \equiv a \bmod p_1^{e_1}$$

$$\vdots$$

$$x^2 \equiv a \bmod p_k^{e_k}.$$

Consider $x^2 \equiv a \bmod 2^e$. If $e = 2$, then $x^2 \equiv a \bmod 4$, and

$$1^2 \equiv 1 \bmod 4$$

$$2^2 \equiv 0 \bmod 4$$

$$3^2 \equiv 1 \bmod 4.$$

Note that since $\gcd(a, m) = 1$, a must necessarily be odd, since m is even, so $a \equiv 1 \bmod 4$ implies that $x^2 \equiv a \bmod 2^e$ has a solution. To satisfy the if and only if requirement of the theorem, suppose that $x^2 \equiv a \bmod 4$ is solvable and $\gcd(a, 4) = 1$. Then from the work above, a is necessarily congruent to 1 modulo 4. It follows that if $e = 2$, then $x^2 \equiv a \bmod 4$ is solvable if and only if $a \equiv 1 \bmod 4$.

Now suppose $e = 3$. Then for $x^2 \equiv a \bmod 8$, we have

$$1^2 \equiv 1 \bmod 8$$

$$2^2 \equiv 4 \bmod 8$$

$$3^2 \equiv 1 \bmod 8$$

$$4^2 \equiv 0 \bmod 8$$

$$5^2 \equiv 1 \bmod 8$$

$$6^2 \equiv 4 \bmod 8$$

$$7^2 \equiv 1 \bmod 8.$$

Again we know that a is odd, so $a \equiv 1 \bmod 8$ implies that $x^2 \equiv a \bmod 8$ has a

solution. By Theorem 8.1.13, if $x^2 \equiv a \bmod 8$ is solvable, then $x^2 \equiv a \bmod 2^e$ is also solvable for all $e \geqslant 3$.

Now consider $x^2 \equiv a \bmod p_i^{e_i}$. Since each of the p_i is an odd prime, $\gcd(2, p_i) = 1$. Then we know from Theorem 8.1.10 that if $x^2 \equiv a \bmod p_i$ is solvable, then $x^2 \equiv a \bmod p_i^{e_i}$ is also solvable. Suppose that $x^2 \equiv a \bmod p_i^{e_i}$ has a solution, say r. Then $r^2 \equiv a \bmod p_i^{e_i}$, which implies that $r^2 = a + \alpha p_i^{e_i}$, and thus $r^2 = a + \beta p_i$, where $\beta = \alpha p_i^{e_i - 1}$. But this implies that $r^2 \equiv a \bmod p_i$, so r is also a solution to the congruence $x^2 \equiv a \bmod p_i$. It follows that $x^2 \equiv a \bmod p_i^{e_i}$ is solvable if and only if $x^2 \equiv a \bmod p_i$ is solvable.

Now we are in a position to apply Theorem 6.0.20 with $n = 2$, $m = p_i$, and $d = \gcd\big(n, \varphi(m)\big) = \gcd(2, p_i - 1) = 2$. The theorem indicates that $x^2 \equiv a \bmod p_i$ is solvable if and only if $a^{(p_i - 1)/2} \equiv 1 \bmod p_i$. ∎

Example 8.1.16 Let $m = 72$. Then the prime-power decomposition of 72 is $72 = 2^3 3^3$. Consider the congruence $x^2 \equiv a \bmod 72$. By Theorem 8.1.15, $e = 3$ and this congruence has a solution if and only if $a \equiv 1 \bmod 8$.

Suppose $a = 35$. Since $35 \equiv 3 \bmod 8$, $x^2 \equiv 35 \bmod 72$ has no solution.

If $a = 41$ instead, then $41 \equiv 1 \bmod 8$, but if we consider the second requirement of the theorem, for $p = 3$, we have $41^{(3-1)/2} = 41 \equiv 2 \bmod 3$. Thus condition 2 is not satisfied, and there is no solution to $x^2 \equiv 41 \bmod 72$.

Let $a = 49$. Then $49 \equiv 1 \bmod 8$ and $49^{(3-1)/2} = 49 \equiv 1 \bmod 3$, so the congruence $x^2 \equiv 49 \bmod 72$ has a solution by Theorem 8.1.15. This should

feel somewhat intuitive, since $x = 7$ clearly satisfies the congruence. □

8.2 Legendre Symbol

The remainder of this chapter will be spent exploring congruences of the form $x^2 \equiv a \bmod p$, and determining whether or not they have solutions. A. M. Legendre came up with a notation called the Legendre symbol that represents the phrase "$x^2 \equiv a \bmod p$ has a solution". The use of this symbol, as defined and explored in the pages to come, will greatly simplify the rest of the work done in this chapter.

Definition 8.2.1 Let (a/p) be called the *Legendre symbol*. Then for odd primes p,

$$(a/p) = \begin{cases} 0, & \text{if } p \mid a \\ 1, & \text{if } a \text{ is a quadratic residue modulo } p \\ -1, & \text{if } a \text{ is a quadratic nonresidue modulo } p. \end{cases}$$

As far as notation goes, the Legendre symbol can either be written as (a/p) or as $\left(\frac{a}{p}\right)$. We don't have a preferred notation, and will just use whichever notation is more convenient. ♢

Note that the special case of $(a/2)$ is not addressed in this definition. If we examine the congruence $x^2 \equiv a \bmod 2$, our only choices are $a = 0$ and

$a = 1$. If $a = 1$, then $x = 1$ is clearly a solution. In fact, any odd integer is a solution when we are working modulo 2.

Most of the work we do from here on out will involve odd primes as our p values, and we will address the special cases of $a = 2$ separately.

Theorem 8.2.2 (Properties of the Legendre Symbol)

1. $a^{(p-1)/2} \equiv (a/p) \bmod p$.
2. *If* $p \nmid a$ *and* $p \nmid b$, *then* $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.
3. *If* $a \equiv b \bmod p$, *then* $(a/p) = (b/p)$.
4. *If* $p \nmid a$, *then* $\left(\frac{a^2}{p}\right) = 1$.
5. $\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \bmod 4 \\ -1, & \text{if } p \equiv 3 \bmod 4. \end{cases}$

Example 8.2.3 This example is designed to illustrate the properties of the Legendre symbol. We do not have the *Law of Quadratic Reciprocity* available to use yet, but once we have established it, we will give other examples that show how powerful it is in evaluating Legendre symbols.

Consider the Legendre symbol $\left(\frac{87}{101}\right)$. By Property 2, this becomes

$$\left(\frac{87}{101}\right) = \left(\frac{3}{101}\right)\left(\frac{29}{101}\right).$$

Now if we apply Property 1 to each of the Legendre symbols on the right hand side, we have

$$\begin{aligned}
\left(\frac{3}{101}\right) &\equiv 3^{(101-1)/2} \bmod 101 && \text{(Property 1 of Legendre symbols)} \\
&\equiv 3^{50} \bmod 101 && \text{(Arithmetic)} \\
&\equiv -1 \bmod 101 && \text{(Reduce modulo 101)}
\end{aligned}$$

and

$$\begin{aligned}
\left(\frac{29}{101}\right) &\equiv 29^{(101-1)/2} \bmod 101 && \text{(Property 1 of Legendre symbol)} \\
&\equiv 29^{50} \bmod 101 && \text{(Arithmetic)} \\
&\equiv -1 \bmod 101. && \text{(Reduce modulo 101)}
\end{aligned}$$

Thus $\left(\frac{87}{101}\right) \equiv (-1)(-1) \equiv 1 \bmod 101$, so $x^2 \equiv 87 \bmod 101$ has a solution by the definition of Legendre symbol.

It is fairly straightforward (using a computer for the computations) to discover that $x = 17$ and $x = 84$ are the two solutions. □

Proof: Assume that p is an odd prime and consider the congruence $x^2 \equiv a \bmod p$.

1. Property 1 follows immediately from Euler's Criterion.

2. Suppose that $p \nmid a$ and $p \nmid b$. Then

$$\begin{aligned}\left(\frac{ab}{p}\right) &\equiv (ab)^{(p-1)/2} \bmod p && \text{(Property 1 of Legendre symbols)}\\ &\equiv a^{(p-1)/2} \cdot b^{(p-1)/2} \bmod p && \text{(Properties of exponents)}\\ &\equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \bmod p. && \text{(Property 1 of Legendre symbols)}\end{aligned}$$

3. Suppose $a \equiv b \bmod p$. Then $x^2 \equiv a \bmod p$ and $x^2 \equiv b \bmod p$ are the same congruence, so they either both have solutions, or they both do not.

4. Assume that $p \nmid a$. Then $x^2 \equiv a^2 \bmod p$ clearly has a solution, specifically the least residue of a modulo p. Thus $\left(\frac{a^2}{p}\right) = 1$.

5. Suppose that $p \equiv 1 \bmod 4$. Then $p = 4k + 1$ for some $k \in \mathbb{Z}$. Consider $x^2 \equiv -1 \bmod p$. By Property 1 of the Legendre symbol, we have

$$\begin{aligned}(-1)^{(p-1)/2} &\equiv (-1)^{(4k+1-1)/2} \bmod p && (p = 4k+1)\\ &\equiv (-1)^{2k} \bmod p && \text{(Arithmetic)}\\ &\equiv 1 \bmod p.\end{aligned}$$

Suppose that $p \equiv 3 \bmod 4$. Then $p = 4j + 3$, for some $j \in \mathbb{Z}$. Consider $x^2 \equiv -1 \bmod p$. By Property 1 of the Legendre symbol, we have

$$\begin{aligned}(-1)^{(p-1)/2} &\equiv (-1)^{(4j+3-1)/2} \bmod p && (p = 4j+3)\\ &\equiv (-1)^{2j+1} \bmod p && \text{(Arithmetic)}\\ &\equiv -1 \bmod p.\end{aligned}$$

Thus $\left(\frac{-1}{p}\right) = 1$ if $p \equiv 1 \bmod 4$ and $\left(\frac{-1}{p}\right) = -1$ if $p \equiv 3 \bmod 4$.

It follows that all five properties hold as desired. ∎

Observe that the properties of the Legendre symbol indicate that the product of two quadratic residues is again a residue. If a and b are residues modulo p, then $\left(\frac{a}{p}\right) = 1 = \left(\frac{b}{p}\right)$ and certainly multiplying those results together yields 1 as well, so ab is also a residue. On the other hand, if a is a residue and b is a nonresidue, then $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = (1)(-1) = -1$, and ab is a nonresidue. Thus the product of a residue and a nonresidue is a nonresidue. This means that the Legendre symbol can be interpreted as a multiplicative character.

Example 8.2.4 Consider the congruence $x^2 \equiv 3870 \bmod 431$. Since $3870 \equiv 422 \bmod 431$, by Property 3 of the Legendre symbol, $\left(\frac{3870}{431}\right) = \left(\frac{422}{431}\right)$. Thus, if we evaluate both symbols, they should give us the same result. The first yields

$$\begin{aligned}
\left(\frac{3870}{431}\right) &= \left(\frac{430 \cdot 3^2}{431}\right) && \text{(Factorization of 3870)} \\
&= \left(\frac{-1 \cdot 3^2}{431}\right) && (430 \equiv -1 \bmod 431) \\
&= \left(\frac{-1}{431}\right)\left(\frac{3}{431}\right)^2 && \text{(Property 2 of Legendre symbols)} \\
&\equiv (-1)(1) \bmod 431, && \text{(Properties 3 and 5 of Legendre symbols)}
\end{aligned}$$

and the second yields

$$\begin{aligned}
\left(\frac{422}{431}\right) &= \left(\frac{2}{431}\right)\left(\frac{211}{431}\right) && \text{(Property 2 of Legendre symbols)} \\
&\equiv 2^{(431-1)/2} \cdot 211^{(431-1)/2} \bmod 431 && \text{(Property 1 of Legendre symbols)} \\
&\equiv 2^{215} \cdot 211^{215} \bmod 431 && \text{(Arithmetic)} \\
&\equiv (1)(-1) \bmod 431 && \text{(Reduce modulo 431)} \\
&\equiv -1 \bmod 431. && \text{(Arithmetic)}
\end{aligned}$$

The two results agree, which is what Property 3 states, and since the result is -1, there is no solution to the congruence $x^2 \equiv 3870 \bmod 431$. □

8.3 Law of Quadratic Reciprocity

The Law of Quadratic Reciprocity has three parts. The first two parts deal with the cases $a = -1$ and $a = 2$ in the congruence $x^2 \equiv a \bmod p$. The third part is a powerful tool that allows us to determine the relationship between (p/q) and (q/p) when p and q are both prime. In other words, it addresses the question "if $x^2 \equiv p \bmod q$ has a solution, under what circumstances does $x^2 \equiv q \bmod p$ also have a solution"?

We introduce the theorem here, and our goal is to prove it in its entirety. We need some additional results first though, so the proof will be given shortly.

Theorem 8.3.1 (The Law of Quadratic Reciprocity) *Let p and q be distinct odd primes. Then*

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

2. $(2/p) = (-1)^{(p^2-1)/8}$

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

Recall that we looked at the properties of the Legendre symbol in the previous section. Part 1 of the Law of Quadratic Reciprocity follows immediately from Property 1 of the Legendre symbol. We need to establish additional results before we can prove the remaining two parts of the Law of Quadratic Reciprocity.

Lemma 8.3.2 (Gauss' Lemma) *Let p be an odd prime and let $a \in \mathbb{Z}$ be such that $\gcd(a, p) = 1$. Define μ to be the number of least residues of the integers $\left\{a, 2a, 3a, \ldots, \left(\frac{p-1}{2}\right)a\right\}$ that are greater than $\frac{p-1}{2}$. Then $(a/p) = (-1)^{\mu}$.*

Example 8.3.3 Let $p = 11$ and $a = 4$. Then $\gcd(4, 11) = 1$ and $\frac{11-1}{2} = 5$. The table below shows the least residues modulo 11 of the integers $a, 2a, \ldots, 5a$.

	4	8	12	16	20
mod 11	4	8	1	5	9

Note that there are three least residues less than or equal to 5 and two that are greater than 5, so $\mu = 2$. By Gauss' Lemma, $(4/11) = (-1)^2 = 1$. Notice that Property 4 of Legendre symbols gives us this result as well, since 4 is a perfect square. □

Proof: Assume that p is an odd prime. Let $a \in \mathbb{Z}$ be such that $\gcd(a, p) = 1$. Consider the integers

$$\left\{a, 2a, \ldots, \left(\frac{p-1}{2}\right) a\right\}. \tag{8.1}$$

Let $u_1, u_2, \ldots, u_s$ denote the least residues modulo p of the integers in (8.1) that are less than or equal to $\dfrac{p-1}{2}$, and let $v_1, v_2, \ldots, v_t$ denote the least residues modulo p of the integers in (8.1) that are greater than $\dfrac{p-1}{2}$.

Suppose that two of the u_i are congruent modulo p. Then for some s_1 and s_2, we have $s_1 a \equiv s_2 a \bmod p$. But $\gcd(a, p) = 1$, so by Corollary 4.3.20, we have $s_1 \equiv s_2 \bmod p$. Since $s_1, s_2 \in \left\{1, \ldots, \dfrac{p-1}{2}\right\}$, we have $s_1 = s_2$, and it follows that the u_i are unique. By a similar argument, we get that the v_j are also unique.

Now consider the set of numbers

$$R = \{u_1, u_2, \ldots, u_s, p - v_1, p - v_2, \ldots, p - v_t\}.$$

Recall that $0 \leqslant u_i \leqslant \dfrac{p-1}{2}$ and $\dfrac{p-1}{2} < v_j < p$. Thus, $1 \leqslant r \leqslant \dfrac{p-1}{2}$ for each $r \in R$. There are at most $\dfrac{p-1}{2}$ such elements r, since $s + t = \dfrac{p-1}{2}$.

We claim that $u_i \not\equiv p - v_j \bmod p$ for any $1 \leqslant i \leqslant s$, $1 \leqslant j \leqslant t$. Note that $u_i \equiv s'a \bmod p$ for some $1 \leqslant s' \leqslant \dfrac{p-1}{2}$ and $p - v_j \equiv t'a \bmod p$ for some $1 \leqslant t' \leqslant \dfrac{p-1}{2}$. Suppose $u_i \equiv p - v_j \bmod p$, for some i, j. Then by substitution, we have $s'a \equiv t'a \bmod p$. But $\gcd(a, p) = 1$, so by Theorem 4.3.20, we have $s' \equiv t' \bmod p$. However, $1 \leqslant s', t' \leqslant \dfrac{p-1}{2}$, so $s' = t'$, and it follows that each

$r \in R$ is unique.

Since $1 \leqslant r \leqslant \dfrac{p-1}{2}$ for each unique $r \in R$, it must be the case that R is a permutation of $\left\{1, 2, \ldots, \dfrac{p-1}{2}\right\}$. Multiplying all of the elements of R together yields

$$u_1 u_2 \ldots u_s (p - v_1)(p - v_2) \ldots (p - v_t) = 1 \cdot 2 \ldots \frac{p-1}{2}. \tag{8.2}$$

Now, $p - v_j \equiv -v_j \bmod p$ for all $1 \leqslant j \leqslant t$, and there are μ such terms, so Equation (8.2) becomes

$$u_1 u_2 \ldots u_s v_1 v_2 \ldots v_\mu (-1)^\mu \equiv \left(\frac{p-1}{2}\right)! \bmod p. \tag{8.3}$$

But $u_1, \ldots, u_2, v_1, \ldots, v_\mu$ are a permutation of the least residues modulo p of the integers in (8.1), so

$$\begin{aligned} u_1 \ldots u_s v_1 \ldots v_\mu &\equiv (a)(2a) \ldots \left(\frac{p-1}{2}\right) a \bmod p \\ \iff u_1 \ldots u_s v_1 \ldots v_\mu &\equiv a^{(p-1)/2} \left(\frac{p-1}{2}\right)! \bmod p. \end{aligned}$$

This last congruence implies that Congruence (8.3) can be rewritten as

$$(-1)^\mu a^{(p-1)/2} \left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)! \bmod p. \tag{8.4}$$

Since p is prime, $\left(\dfrac{p-1}{2}\right)!$ is relatively prime to p, so by Theorem 4.3.20, we have $a^{(p-1)/2}(-1)^\mu \equiv 1 \bmod p$.

Multiplying both sides of Congruence (8.4) by $(-1)^\mu$, yields

$$a^{(p-1)/2} \equiv (-1)^\mu \bmod p. \tag{8.5}$$

By Property 1 of Legendre symbols, $a^{(p-1)/2} \equiv (a/p) \bmod p$, so $(a/p) \equiv (-1)^{\mu} \bmod p$. Note that each side of Congruence (8.5) will only take the values of 1 or -1, so the two sides must be equivalent modulo p. It follows that $(a/p) = (-1)^{\mu}$. ∎

Theorem 8.3.4 *2 is a quadratic residue of primes of the form $8k+1$ and $8k+7$. 2 is a quadratic nonresidue of primes of the form $8k+3$ and $8k+5$. This information is summarized in the formula*

$$(2/p) = (-1)^{(p^2-1)/8}.$$

Example 8.3.5 To illustrate this theorem, we consider the primes 11, 13, 17, and 23. Since $11 \equiv 3 \bmod 8$, it is of the form $8k+3$. By Euler's Criterion,

$$2^{(p-1)/2} = 2^{(11-1)/2} \equiv -1 \bmod 11,$$

thus $x^2 \equiv 2 \bmod 11$ does not have a solution and $(2/p) = -1$. The formula from Theorem 8.3.4 yields

$$\begin{aligned} (-1)^{(p^2-1)/8} &= (-1)^{(11^2-1)/8} && (p = 11) \\ &= (-1)^{15} && \text{(Arithmetic)} \\ &= -1. \end{aligned}$$

Similarly, since $13 \equiv 5 \bmod 8$, 13 is of the form $8k+5$, and

$$2^{(p-1)/2} = 2^6 \equiv -1 \bmod 13.$$

Thus $(2/p) = -1$ and $(-1)^{(13^2-1)/8} = (-1)^{21} = -1$. Therefore 2 is a quadratic nonresidue of both 11 and 13, which were primes of the form $8k+3$ and $8k+5$ respectively.

Since $17 \equiv 1 \bmod 8$, it is of the form $8k + 1$, and

$$2^{(17-1)/2} = 2^8 = 256 \equiv 1 \bmod 17.$$

Thus $x^2 \equiv 2 \bmod 17$ has a solution, and $(2/p) = 1 = (-1)^{(17^2-1)/8}$.

Finally, $23 \equiv 7 \bmod 8$, so 23 is of the form $8k + 7$ and

$$2^{(23-1)/2} = 2^{11} = 2048 \equiv 1 \bmod 23,$$

thus $(2/p) = 1 = (-1)^{(23^2-1)/8}$. Hence 2 is a quadratic residue of the primes 17 and 23, which are of the form $8k + 1$ and $8k + 7$ respectively. □

We present two very different proofs of Theorem 8.3.4. The first is a variation of the proof that is generally credited to Gauss, which relies heavily on the use of Gauss' Lemma. While it does give the desired result, the method is a bit unwieldy. We have changed the second half of the proof slightly to make it more straightforward.

Before we work through the first proof of this theorem, we need to recall that the greatest integer of a real number x, denoted by $[x]$, is the largest integer less than or equal to x. Symbolically, this is $[x] \leqslant x \leqslant [x] + 1$. For example, $[1/4] = 0$ and $[5] = 5$. This idea will be used in Gauss' version of the proof.

Proof: Assume that p is an odd prime. Recall that Gauss' Lemma takes the set of integers $\left\{a, 2a, \ldots, \frac{p-1}{2}a\right\}$ and divides them into two groups. For $1 \leqslant m \leqslant \frac{p-1}{2}$, the first group is the set of ma for which $ma \leqslant \frac{p-1}{2}$, and the second group is the set of ma such that $ma > \frac{p-1}{2}$. The number of elements in this second group is the value of μ in Gauss' Lemma.

So for $a = 2$, μ is the number of $2m \in S = \left\{1 \cdot 2, 2 \cdot 2, \ldots, \left(\frac{p-1}{2}\right) \cdot 2\right\}$ such that $2m > \frac{p-1}{2}$. We want to find the value of m that is the cutoff point between the two groups. In other words, we are looking for the m, such that $2m \leqslant \frac{p-1}{2}$, but $2(m+1) > \frac{p-1}{2}$. Solving each of these inequalities for m and then combining inequalities yields

$$\frac{p-1}{4} - 1 < m \leqslant \frac{p-1}{4}.$$

Since each of the integers in $\{1 \cdot 2, 2 \cdot 2, \ldots, m \cdot 2\}$ is less than or equal to $\frac{p-1}{2}$, we see that m is the number of least residues that are less than or equal to $\frac{p-1}{2}$. Thus, since there are a total of $\frac{p-1}{2}$ least residues, $\mu = \frac{p-1}{2} - m$.

There are four possibilities for least residues modulo 8, and they are 1, 3, 5, and 7. We examine each of these individually, and determine m and μ in each case.

- Suppose $p \equiv 1 \bmod 8$. Then $p = 8k + 1$, for some $k \in \mathbb{Z}$, so $\frac{p-1}{2} = 4k$.

Since $\frac{p-1}{4} - 1 < m \leqslant \frac{p-1}{4}$, we have

$$\frac{8k+1-1}{4} - 1 < m \leqslant \frac{8k+1-1}{4} \qquad \text{(Substitution)}$$

$$\iff 2k - 1 < m \leqslant 2k, \qquad \text{(Arithmetic)}$$

which implies that $m = 2k$. Thus, $\mu = 4k - 2k = 2k$, so

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

It follows that 2 is a quadratic residue of primes of the form $8k + 1$.

- Suppose $p \equiv 7 \bmod 8$. Then $p = 8k + 7$, for some $k \in \mathbb{Z}$, which gives us $\frac{p-1}{2} = 4k + 3$. Thus,

$$\frac{8k+7-1}{4} - 1 < m \leqslant \frac{8k+7-1}{4} \iff 2k + \frac{1}{2} < m \leqslant 2k + \frac{3}{2}.$$

But m is an integer, so $m = 2k + 1$ by the greatest integer function, and $\mu = 4k + 3 - (2k + 1) = 2(k + 1)$. Thus $(2/p) = (-1)^{2(k+1)} = 1$, and it follows that 2 is a quadratic residue of primes of the form $8k + 7$, which is equivalent to saying that $p \equiv -1 \bmod 8$.

- Suppose $p \equiv 3 \bmod 8$. Then $p = 8k + 3$, for some $k \in \mathbb{Z}$, which yields $\frac{p-1}{2} = 4k + 1$. Thus

$$\frac{8k+3-1}{4} - 1 < m \leqslant \frac{8k+3-1}{4} \iff 2k - \frac{1}{2} < m \leqslant 2k + \frac{1}{2}.$$

But since m is an integer, $m = 2k$ by the greatest integer function, so $\mu = 4k + 1 - 2k = 2k + 1$, which is odd. Hence $(2/p) = (-1)^{2k+1} = -1$,

and it follows that 2 is a quadratic nonresidue of primes of the form $8k + 3$.

- Suppose $p \equiv 5 \bmod 8$. Then there is some $k \in \mathbb{Z}$, such that $p = 8k + 5$. Thus $\dfrac{p-1}{2} = 4k + 2$, so

$$\frac{8k+5-1}{4} - 1 < m \leqslant \frac{8k+5-1}{4} \iff 2k < m \leqslant 2k+1,$$

which implies that $m = 2k+1$. Thus $\mu = 4k+2-(2k+1) = 2k+1$, which is odd, so $(2/p) = (-1)^{2k+1} = -1$, and it follows that 2 is a quadratic nonresidue of primes of the form $8k + 5$.

At this point we have established that

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{if } p \equiv \pm 1 \bmod 8 \\ -1, & \text{if } p \not\equiv \pm 1 \bmod 8. \end{cases}$$

It remains to show that the formula $(2/p) = (-1)^{(p^2-1)/8}$ holds. We have already seen that we can write each of the odd primes as $8k + r$, where $k \in \mathbb{Z}$ and $r \in \{1, 3, 5, 7\}$. Examination of $\dfrac{p^2-1}{8}$ yields

$$\begin{aligned} \frac{(8k+r)^2-1}{8} &= \frac{64k^2+16rk+r^2-1}{8} && \text{(Substitution; Arithmetic)} \\ &= 8k^2 + 2rk + \frac{r^2-1}{8}. && \text{(Arithmetic)} \end{aligned}$$

But $8k^2 + 2rk \equiv 0 \bmod 2$, so we only need to be concerned with the term $\dfrac{r^2-1}{8}$ for $r \in \{1, 3, 5, 7\}$. Examining this term for each of the possible values of r yields the following table of results.

r	r^2-1	$\frac{r^2-1}{8}$	mod 2
1	0	0	0
3	8	1	1
5	24	3	1
7	48	6	0

Note that the values in the modulo 2 column match our previous results for each value of r. Thus

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

as desired. ∎

The second version of this proof that we present is a version by Euler. He used complex numbers and primitive roots of unity to derive the formula for $(2/p)$. The math is more complicated in Euler's version, but it is presented here as a contrast to the fairly straightforward proof by Gauss.

Proof: Let ζ be a primitive eighth root of unity. Then $\zeta = e^{2\pi i/8}$. By definition of primitive roots of unity, we have $\zeta^8 - 1 = (\zeta^4 - 1)(\zeta^4 + 1) = 0$.

Since ζ is an eighth root of unity, $\zeta^4 \neq 1$, so $\zeta^4 + 1 = 0$. Thus we have

$$\begin{aligned}
& \zeta^4 = -1 \\
\iff & \zeta^{-2} \cdot \zeta^4 = \zeta^{-2} \cdot (-1) && \text{(Left multiplication by } \zeta^{-2}\text{)} \\
\iff & \zeta^2 = -\zeta^{-2} && \text{(Arithmetic)} \\
\iff & \zeta^2 + \zeta^{-2} = 0 && \text{(Addition Property of Equality)} \\
\iff & \zeta^2 + 2 + \zeta^{-2} = 2 && \text{(Add 2 to both sides)} \\
\iff & (\zeta + \zeta^{-1})^2 = 2. && \text{(Factorization)}
\end{aligned}$$

Set $\tau = \zeta + \zeta^{-1}$. Then $\tau^2 = 2$. Now, since $\zeta^8 - 1 = 0$, ζ is an algebraic integer, because it is the root of a polynomial with integer coefficients. Recall that we stated earlier that the algebraic integers form a ring. This implies that τ is also an algebraic integer, since rings are closed under addition and multiplication.

We need to work temporarily in the setting $\mathbb{Z}_p(\zeta)$, where ζ is a primitive 8^{th} root of unity. $\mathbb{Z}_p(\zeta)$ is an extension field of $\mathbb{Z}_p$ containing ζ. We did not prove results in this thesis about extension fields, but they can be found in [6]. For the remainder of this proof, whenever τ comes into play, we will be working in this extension field.

For the odd prime p in $\mathbb{Z}_p(\zeta)$,

$$\begin{aligned}
\tau^{p-1} &= (\tau^2)^{(p-1)/2} && \text{(Properties of exponents)} \\
&= 2^{(p-1)/2} && (\tau^2 = 2) \\
&= (2/p). && \text{(Property 1 of Legendre Symbols)}
\end{aligned}$$

To justify the third step, note that $\tau^2 = 2$, since p is an odd prime, and $2 < p$ for any p. Thus $2^{(p-1)/2} = (2/p)$ by Property 1 of Legendre symbols.

So now we have $\tau^{p-1} = (2/p)$ if and only if τ is in the extension field. But this is equivalent to $\tau^p = \tau \cdot (2/p)$. By Theorem 5.5.3, we also have $\tau^p = (\zeta + \zeta^{-1})^p = \zeta^p + \zeta^{-p}$. Recall that $\zeta^8 = 1$. We can now see that if $p \equiv \pm 1 \bmod 8$, $\zeta^p + \zeta^{-p} = \zeta + \zeta^{-1}$, and if $p \equiv \pm 3 \bmod 8$, $\zeta^p + \zeta^{-p} = \zeta^3 + \zeta^{-3}$. Recall that we saw previously that $\zeta^4 = -1$, so

$$\begin{aligned}
&\zeta^4 = -1 \\
\iff &\zeta^{-1} \cdot \zeta^4 = \zeta^{-1} \cdot (-1) && \text{(Multiplication Property of Equality)} \\
\iff &\zeta^3 = -\zeta^{-1}. && \text{(Arithmetic)}
\end{aligned}$$

A similar calculation yields $\zeta^{-3} = -\zeta$. Thus, when $p \equiv \pm 3 \bmod 8$, we have $\zeta^p + \zeta^{-p} = -(\zeta + \zeta^{-1})$. Combining these results yields

$$\zeta^p + \zeta^{-p} = \begin{cases} \tau, & \text{if } p \equiv \pm 1 \bmod 8 \\ -\tau, & \text{if } p \equiv \pm 3 \bmod 8. \end{cases} \tag{8.6}$$

Putting all of the pieces together reveals that

$$\begin{aligned}
&\tau^p = \tau \cdot (2/p) \\
\iff &\zeta^p + \zeta^{-p} = \tau \cdot (2/p) && (\tau^p = \zeta^p + \zeta^{-p}) \\
\iff &(-1)^\alpha(\zeta + \zeta^{-1}) = \tau \cdot (2/p), && (\text{Equation (8.6)})
\end{aligned}$$

where α is yet to be determined. Based on our previous work in this proof, we see that $(-1)^\alpha = 1$ when $p \equiv \pm 1 \bmod 8$ and $(-1)^\alpha = -1$ when $p \equiv \pm 3 \bmod 8$. Thus

$$\alpha = \begin{cases} 0, & \text{if } p \equiv \pm 1 \bmod 8 \\ 1, & \text{if } p \equiv \pm 3 \bmod 8. \end{cases}$$

Now suppose that $p \equiv 1 \bmod 8$. Then $p = 8k + 1$ for some $k \in \mathbb{Z}$. Observe that

$$\begin{aligned}
\frac{p^2 - 1}{8} &= \frac{64k^2 + 16k + 1 - 1}{8} && (\text{Substitution; Arithmetic}) \\
&= 8k^2 + 2k && (\text{Arithmetic}) \\
&\equiv 0 \bmod 2.
\end{aligned}$$

Similar calculations reveal that $\dfrac{p^2 - 1}{8} \equiv 0 \bmod 2$ when $p \equiv -1 \bmod 8$ and $\dfrac{p^2 - 1}{8} \equiv 1 \bmod 8$ when $p \equiv \pm 3 \bmod 8$.

Returning to our previous work, $\tau^p = \tau \cdot (2/p)$ yields

$$\begin{aligned}
&\tau^p = \tau \cdot (2/p) \\
\iff &(-1)^{\alpha}(\zeta + \zeta^{-1}) = \tau \cdot (2/p) \\
\iff &(-1)^{(p^2-1)/8}(\zeta + \zeta^{-1}) = \tau \cdot (2/p) && (\alpha = (p^2-1)/8) \\
\iff &(-1)^{(p^2-1)/8} \cdot \tau = \tau \cdot (2/p) && (\tau = \zeta + \zeta^{-1}) \\
\iff &(-1)^{(p^2-1)/8} = (2/p), && \text{(Corollary 4.3.20)}
\end{aligned}$$

which is the desired result. ∎

Now we have proved parts 1 and 2 of the Law of Quadratic Reciprocity, and it remains only to prove part 3. However, we need to establish a few more results before we prove that portion of the theorem. Once we have proved the third part, we will demonstrate its usefulness with some examples.

Recall that $[x]$ is the greatest integer function, and $[x] \leqslant x \leqslant [x] + 1$. We will use this function in the proofs to come.

Lemma 8.3.6 *Let p and q be odd primes. Then $(q/p) = (-1)^k$, where*

$$k = \sum_{i=1}^{(p-1)/2} \left[\frac{qi}{p} \right].$$

Example 8.3.7 Let $p = 11$ and $q = 7$. Then

$$\begin{aligned}
\sum_{i=1}^{(11-1)/2} \left[\frac{7i}{11} \right] &= \left[\frac{7}{11} \right] + \left[\frac{14}{11} \right] + \left[\frac{21}{11} \right] + \left[\frac{28}{11} \right] + \left[\frac{35}{11} \right] \\
&= 0 + 1 + 1 + 2 + 3 && \text{(Definition of } [x]) \\
&= 7. && \text{(Arithmetic)}
\end{aligned}$$

We know from previous work that

$$\begin{aligned}(7/11) &\equiv 7^{(11-1)/2} \bmod 11 \\ &\equiv 16807 \bmod 11 \\ &\equiv -1 \bmod 11,\end{aligned}$$

and if we apply the lemma, we have $(7/11) = (-1)^7 = -1$, which agrees.

Note that

$$14 = \left[\frac{14}{11}\right] \cdot 11 + 3 \text{ and } 0 < 3 < \frac{11}{2},$$

but

$$28 = \left[\frac{28}{11}\right] \cdot 11 + 6 = \left[\frac{28}{11}\right] \cdot 11 + (11 - 5), \text{ where } 0 < 5 < \frac{11}{2}.$$

In other words, some of the qi can be expressed as $qi = \left[\frac{qi}{p}\right] \cdot p + u$, where $0 < u < \frac{p}{2}$. However, if $qj = \left[\frac{qj}{p}\right] \cdot p + v$, where $\frac{p}{2} < v < p$, then we can express qj as $qj = \left[\frac{qj}{p}\right] \cdot p + (p - u')$, where $u' = p - v$ and $0 < u' < \frac{p}{2}$.

This idea that each qi can be expressed as either $qi = \left[\frac{qi}{p}\right] \cdot p + r$, for some $0 < r < \frac{p}{2}$, or $qi = \left[\frac{qi}{p}\right] \cdot p + (p - r')$, where $r' = p - r$ and $0 < r' < \frac{p}{2}$ is going to play a part in the proof of Lemma 8.3.6.

We can use a similar process to calculate (11/7).

$$\begin{aligned}\sum_{i=1}^{(7-1)/2} \left[\frac{11i}{7}\right] &= \left[\frac{11}{7}\right] + \left[\frac{22}{7}\right] + \left[\frac{33}{7}\right] \\ &= 1 + 3 + 4 && \text{(Definition of } [x]) \\ &= 8 && \text{(Arithmetic)}\end{aligned}$$

By the definition of the Legendre Symbol, $(11/7) \equiv 11^{(7-1)/2} \bmod 7 \equiv 1 \bmod 7$, and $(11/7) = (-1)^8 = 1$ by the lemma, so the results agree. □

Proof: Consider the integers $q, 2q, \ldots, \left(\frac{p-1}{2}\right) q$. By the division algorithm for integers, we can divide these into two types, as modeled by Example 8.3.7. So either

$$qi = \left[\frac{qi}{p}\right] \cdot p + u_i, \text{ where } 0 < u_i < \frac{p}{2}, \tag{8.7}$$

or

$$qi = \left[\frac{qi}{p}\right] \cdot p + (p - v_i), \text{ where } 0 < p - v_i < \frac{p}{2}. \tag{8.8}$$

Now recall that by Gauss' Lemma, μ is defined to be the number of least residues of $q, 2q, \ldots, \left(\frac{p-1}{2}\right) q$ that are greater than $\frac{p-1}{2}$. By definition, the number of v_i is exactly μ. In the proof of Gauss' Lemma, we showed that $\{u_1, \ldots, u_s, p-v_1, \ldots, p-v_\mu\}$ is a permutation of the integers $\left\{1, 2, \ldots, \frac{p-1}{2}\right\}$.

Adding Equations (8.7) and (8.8) together yields

$$\begin{aligned}
\sum_{i=1}^{(p-1)/2} qi &= \sum_{i=1}^{(p-1)/2} \left\lfloor \frac{qi}{p} \right\rfloor \cdot p + \sum_{i=1}^{s} u_i + \sum_{i=1}^{\mu} (p - v_i) \\
&= p \cdot \sum_{i=1}^{(p-1)/2} \left\lfloor \frac{qi}{p} \right\rfloor + \sum_{i=1}^{s} u_i + \sum_{i=1}^{\mu} p - \sum_{i=1}^{\mu} v_i \qquad \text{(Properties of sums)} \\
&= p \cdot \sum_{i=1}^{(p-1)/2} \left\lfloor \frac{qi}{p} \right\rfloor + \sum_{i=1}^{s} u_i + p\mu - \sum_{i=1}^{\mu} v_i \\
&= p \cdot \sum_{i=1}^{(p-1)/2} \left\lfloor \frac{qi}{p} \right\rfloor + p\mu + \sum_{i=1}^{s} u_i - \sum_{i=1}^{\mu} v_i + \sum_{i=1}^{\mu} v_i - \sum_{i=1}^{\mu} v_i \\
&\qquad \text{(Addition of zero)} \\
&= p \cdot \sum_{i=1}^{(p-1)/2} \left\lfloor \frac{qi}{p} \right\rfloor + p\mu + \sum_{i=1}^{s} u_i + \sum_{i=1}^{\mu} v_i - 2\sum_{i=1}^{\mu} v_i \\
&\qquad \text{(Rearrange summand)} \\
&= p \cdot \sum_{i=1}^{(p-1)/2} \left\lfloor \frac{qi}{p} \right\rfloor + p\mu + \sum_{i=1}^{(p-1)/2} i - 2\sum_{i=1}^{\mu} v_i. \qquad (s + \mu = (p-1)/2)
\end{aligned}$$

In the final step, note that $s + \mu = \dfrac{p-1}{2}$ and since the u_i and v_i are distinct, $\displaystyle\sum_{i=1}^{s} u_i + \sum_{i=1}^{\mu} v_i$ gives us the sum of the integers $1, 2, \ldots, \dfrac{p-1}{2}$.

Thus continuing our work from above and using properties of sums to manipulate the equation, we have

$$\begin{aligned}
&\sum_{i=1}^{(p-1)/2} qi = p \cdot \sum_{i=1}^{(p-1)/2} \left\lfloor \frac{qi}{p} \right\rfloor + p\mu + \sum_{i=1}^{(p-1)/2} i - 2\sum_{i=1}^{\mu} v_i \\
\iff &\sum_{i=1}^{(p-1)/2} qi - \sum_{i=1}^{(p-1)/2} i = p \cdot \sum_{i=1}^{(p-1)/2} \left\lfloor \frac{qi}{p} \right\rfloor + p\mu - 2\sum_{i=1}^{\mu} v_i \\
\iff &\sum_{i=1}^{(p-1)/2} i(q-1) = p \cdot \sum_{i=1}^{(p-1)/2} \left\lfloor \frac{qi}{p} \right\rfloor + p\mu - 2\sum_{i=1}^{\mu} v_i \\
\iff &(q-1) \sum_{i=1}^{(p-1)/2} i = p \cdot \sum_{i=1}^{(p-1)/2} \left\lfloor \frac{qi}{p} \right\rfloor + p\mu - 2\sum_{i=1}^{\mu} v_i.
\end{aligned}$$

But p and q are both odd, so taking

$$(q-1)\sum_{i=1}^{(p-1)/2} i = p\cdot\sum_{i=1}^{(p-1)/2}\left[\frac{qi}{p}\right] + p\mu - 2\sum_{i=1}^{\mu} v_i$$

modulo 2 yields

$$1\cdot\sum_{i=1}^{(p-1)/2}\left[\frac{qi}{p}\right] + 1\cdot\mu \equiv 0 \bmod 2,$$

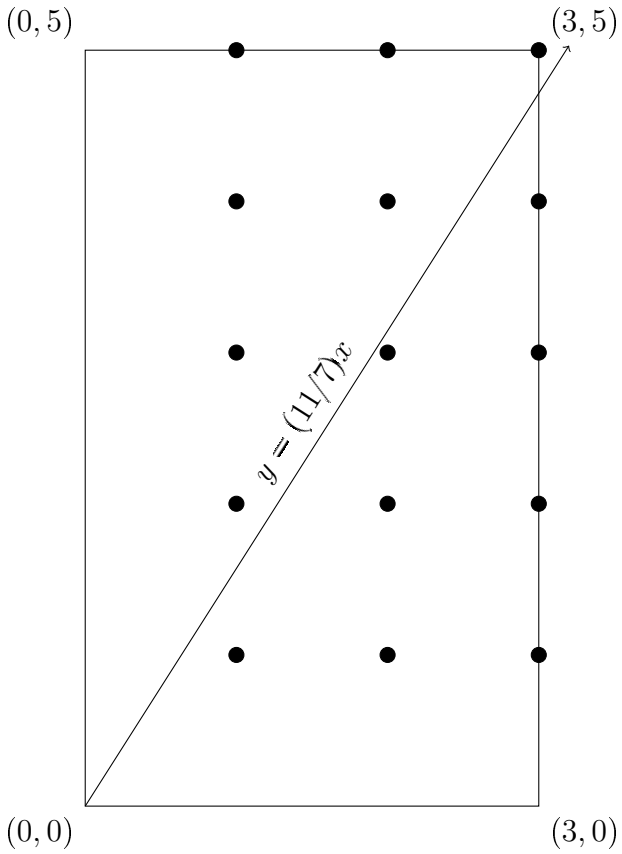
which implies that

$$\mu \equiv -\sum_{i=1}^{(p-1)/2}\left[\frac{qi}{p}\right] \bmod 2.$$

Now recall that by hypothesis, $k = \sum_{i=1}^{(p-1)/2}\left[\frac{qi}{p}\right]$, so $\mu \equiv -k \bmod 2$. This means that μ and k differ only by sign, and thus they are either both even or both odd. So by Gauss' Lemma, $(q/p) = (-1)^{\mu} = (-1)^{k}$. ∎

Before we prove part 3 of the Law of Quadratic Reciprocity, we want to look at an example that illustrates geometrically how Lemma 8.3.6 works, because we will use a similar approach in our proof.

Example 8.3.8 From Example 8.3.7, consider the ordered pairs (x, y), such that $1 \leqslant x \leqslant \left(\frac{7-1}{2}\right) = 3$ and $1 \leqslant y \leqslant \left(\frac{11-1}{2}\right) = 5$, where $x, y \in \mathbb{Z}$. There are $3 \cdot 5 = 15$ such pairs, and we can arrange them in the rectangle shown below.



Now consider the line $7y = 11x$. This equation implies that $11 \mid 7y$, so either $11 \mid 7$ or $11 \mid y$. Clearly $11 \nmid 7$, and since $1 \leqslant y \leqslant 5$, we can see easily that $11 \nmid y$ as well. Thus, none of the 15 ordered pairs (x, y) lie on the line $y = \dfrac{11}{7}x$.

This line effectively splits the pairs into two groups. The group in the top portion of the rectangle are those pairs that satisfy $11x < 7y$, or the values $1 \leqslant y \leqslant 5$ and $1 \leqslant x \leqslant \dfrac{7}{11}y$. Since x is an integer, this last inequality is $1 \leqslant x \leqslant \left[\dfrac{7y}{11}\right]$, for each $1 \leqslant y \leqslant 5$. The group in the bottom portion of the rectangle are the pairs satisfying $7y < 11x$, or the values $1 \leqslant x \leqslant 3$ and

$1 \leqslant y < \left[\frac{11x}{7}\right]$.

From our work above, we can see that there are

$$\sum_{i=1}^{5} \left[\frac{7i}{11}\right] = 7$$

points that lie above the line $y = \frac{11}{7}x$. Similarly, there are

$$\sum_{i=1}^{3} \left[\frac{11i}{7}\right] = 8$$

points below the line, and since none of the points lie exactly on the line, this accounts for all 15 of the ordered pairs.

Examining the product $\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$ for our values $p = 11$ and $q = 7$ yields

$$\begin{aligned}
\left(\frac{11-1}{2}\right)\left(\frac{7-1}{2}\right) &= 5 \cdot 3 && \text{(Arithmetic)} \\
&= 15 && \text{(Arithmetic)} \\
&= 8 + 7 && \text{(Arithmetic)} \\
&= \sum_{i=1}^{3} \left[\frac{11i}{7}\right] + \sum_{i=1}^{5} \left[\frac{7i}{11}\right].
\end{aligned}$$

Now recall that in part 3 of the Law of Quadratic Reciprocity, the right hand side of the equation is $(-1)^{((p-1)/2)((q-1)/2)}$. Our work here means that when we prove the Law of Quadratic Reciprocity, we can replace the exponent on the right side of the equation in part 3 with the sums that we constructed. □

We are now in a position to prove part 3 of the Law of Quadratic Reciprocity. There are to date over two hundred versions of this proof [18].

The proof that we present here is credited to Eisenstein and makes use of the greatest integer function.

Theorem 8.3.9 (The Law of Quadratic Reciprocity) *Let p and q be distinct odd primes. Then*

1. $(-1/p) = (-1)^{(p-1)/2}$
2. $(2/p) = (-1)^{(p^2-1)/8}$
3. $(p/q)(q/p) = (-1)^{((p-1)/2)((q-1)/2)}$.

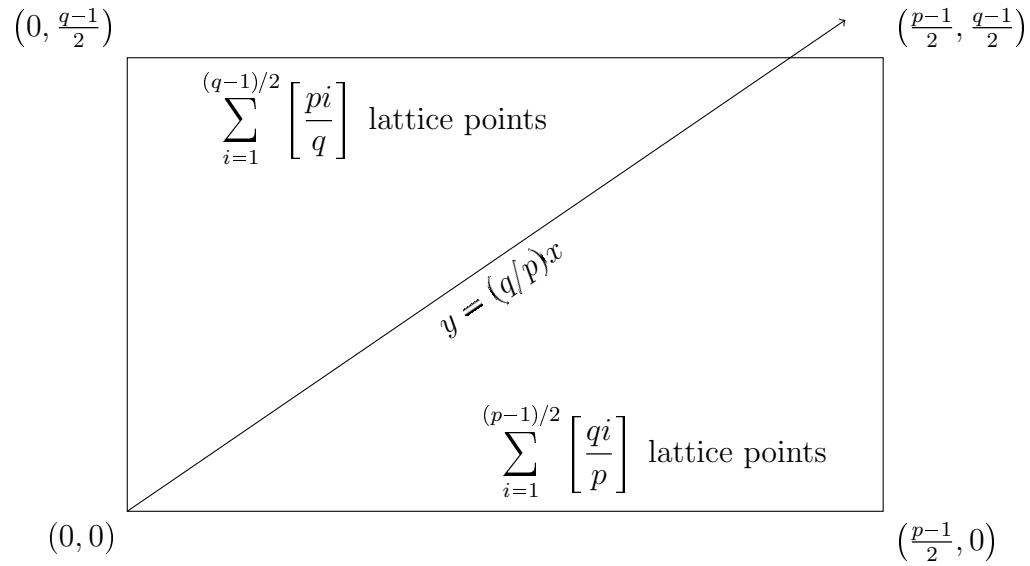
Proof: Assume that p and q are distinct odd primes.

1. This follows immediately from Property 1 of Legendre symbols.
2. This result was proved in Theorem 8.3.4.
3. Let $k = \sum_{i=1}^{(q-1)/2} \left[\frac{pi}{q}\right]$ and $k' = \sum_{i=1}^{(p-1)/2} \left[\frac{qi}{p}\right]$. Then by Lemma 8.3.6, we know that $(p/q) = (-1)^k$ and $(q/p) = (-1)^{k'}$. Thus

$$(p/q)(q/p) = (-1)^k \cdot (-1)^{k'} = (-1)^{k+k'}.$$

Our goal is to show that $k + k' = \frac{p-1}{2} \cdot \frac{q-1}{2}$.

Consider a rectangle similar to the one from Example 8.3.8, as shown below.



Now consider the ordered pairs (x, y) in the rectangle, where $x, y \in \mathbb{Z}$ and $1 \leqslant x \leqslant \dfrac{p-1}{2}$, $1 \leqslant y \leqslant \dfrac{q-1}{2}$, and note that there are $\dfrac{p-1}{2} \cdot \dfrac{q-1}{2}$ such pairs.

If we graph the line $qx = py$, notice that none of the integer pairs (x, y) is on the line, since if $qx = py$, then $q \mid py$, which implies that either $q \mid p$ or $q \mid y$. But p and q are distinct primes, so $q \mid p$ is not possible. Also, $1 \leqslant y \leqslant \dfrac{q-1}{2}$, so y cannot be a multiple of q either. Thus $qx \neq py$ for any pair (x, y).

Suppose $py > qx$. We want to count the number of (x, y) pairs that lie above the line $py = qx$. These pairs satisfy $1 \leqslant y \leqslant \dfrac{q-1}{2}$ and $1 \leqslant x \leqslant \dfrac{py}{q}$. As we run through each y value, we can see that there are $\left[\dfrac{py}{q}\right]$ integers that satisfy $1 \leqslant x \leqslant \dfrac{py}{q}$. Since there are $\dfrac{q-1}{2}$ such

values of y, there are exactly $\sum_{i=1}^{(q-1)/2} \left[\frac{pi}{q}\right]$ pairs (x, y) such that x and y are both integers and $1 \leqslant y \leqslant \frac{q-1}{2}$ and $1 \leqslant x \leqslant \frac{py}{q}$ are both satisfied.

In a similar fashion, if we consider the inequality $qx > py$, we can determine how many (x, y) pairs lie below the line $py = qx$. The pairs below the line must satisfy $1 \leqslant x \leqslant \frac{p-1}{2}$ and $1 \leqslant y \leqslant \frac{qx}{p}$. Running through each x value gives us $\left[\frac{qx}{p}\right]$ integers that satisfy $1 \leqslant y \leqslant \frac{qx}{p}$. There are $\frac{p-1}{2}$ such x values, so there are exactly $\sum_{i=1}^{(p-1)/2} \left[\frac{qi}{p}\right]$ pairs (x, y) such that $x, y \in \mathbb{Z}$ and $1 \leqslant x \leqslant \frac{p-1}{2}$ and $1 \leqslant y \leqslant \frac{qx}{p}$ are both satisfied.

Now, since there are $\frac{p-1}{2} \cdot \frac{q-1}{2}$ total pairs in the rectangle and none of the pairs lie on the line $py = qx$,

$$\frac{p-1}{2} \cdot \frac{q-1}{2} = \sum_{i=1}^{(q-1)/2} \left[\frac{pi}{q}\right] + \sum_{i=1}^{(p-1)/2} \left[\frac{qi}{p}\right] = k + k'.$$

Thus $(p/q)(q/p) = (-1)^{((p-1)/2)((q-1)/2)}$ as desired.

It follows that the Law of Quadratic Reciprocity holds. ∎

There are of course several different ways to state the third part of the Law of Quadratic Reciprocity, so we will state three versions and then prove that they are equivalent. We require a lemma for the proof.

Lemma 8.3.10 *Suppose q is an odd prime and $a \geqslant 1 \in \mathbb{Z}$. If $x^2 \equiv a \bmod q$, then $(2x)^2 \equiv 4a \bmod q$ and $(4a/q) = (a/q)$.*

Proof: Suppose $x^2 \equiv a \bmod q$. Then

$$x^2 \equiv a \bmod q$$

$$\iff 4x^2 \equiv 4a \bmod q$$

$$\iff (2x)^2 \equiv 4a \bmod q.$$

Thus

$$\begin{aligned}(4a/q) &= (4/q)(a/q) && \text{(Properties of Legendre Symbol)}\\ &= (a/q), && \text{((4/q) = 1 by Properties of Legendre Symbol)}\end{aligned}$$

as desired. ∎

Theorem 8.3.11 *Let p and q be odd primes and $a \geqslant 1$ an integer. Then the following assertions are equivalent.*

1. *If $p \equiv q \equiv 3 \bmod 4$, then $(p/q) = -(q/p)$. Otherwise, $(p/q) = (q/p)$.*
2. $(p/q)(q/p) = (-1)^{(p-1)(q-1)/4}$.
3. *If $p \equiv \pm q \bmod 4a$ and $p \nmid a$, then $(a/p) = (a/q)$.*

In the statement of the theorem, a is restricted to the natural numbers. This restriction prevents strange occurrences such as working modulo negative numbers, since in the third part of the theorem, we work modulo $4a$.

Proof: Throughout this proof, assume that p and q are odd primes and let $a \in \mathbb{N}$.

$\boxed{1 \Rightarrow 2}$ Assume $p \equiv q \equiv 3 \bmod 4$. Then $(p/q) = -(q/p)$, which implies that exactly one of (p/q) or (q/p) is equal to 1 and the other is equal to -1, and thus the product $(p/q)(q/p) = -1$. Let $p = 4t + 3$ and $q = 4s + 3$, for some $s, t \in \mathbb{Z}$. Then

$$\begin{aligned} \frac{p-1}{2} \cdot \frac{q-1}{2} &= \frac{4t+3-1}{2} \cdot \frac{4s+3-1}{2} && \text{(Substitution)} \\ &= (2t+1)(2s+1) && \text{(Arithmetic)} \\ &= 2(2st+t+s)+1, && \text{(Distributive Property)} \end{aligned}$$

which is odd. So $(-1)^{(p-1)(q-1)/4} = -1$, hence $(p/q)(q/p) = (-1)^{(p-1)(q-1)/4}$.

Suppose now that $p \equiv q \equiv 1 \bmod 4$. Then $(p/q) = (q/p)$, which implies that $(p/q)(q/p) = 1$. Let $p = 4t + 1$ and $q = 4s + 1$, for some $s, t \in \mathbb{Z}$. Then

$$\begin{aligned} \frac{p-1}{2} \cdot \frac{q-1}{2} &= \frac{4t+1-1}{2} \cdot \frac{4s+1-1}{2} && \text{(Substitution)} \\ &= 2t \cdot 2s, && \text{(Arithmetic)} \end{aligned}$$

which is even. Thus $(-1)^{(p-1)(q-1)/4} = 1$, so $(p/q)(q/p) = (-1)^{(p-1)(q-1)/4}$.

Finally, suppose that $p \not\equiv q \bmod 4$. Without loss of generality, assume that $p \equiv 3 \bmod 4$ and $q \equiv 1 \bmod 4$. Then $(p/q) = (q/p)$, so $(p/q)(q/p) = 1$. Let $p = 4t + 3$ and $q = 4s + 1$, for some $s, t \in \mathbb{Z}$. Then

$$\begin{aligned} \frac{p-1}{2} \cdot \frac{q-1}{2} &= \frac{4t+3-1}{2} \cdot \frac{4s+1-1}{2} && \text{(Substitution)} \\ &= (2t+1)(2s) && \text{(Arithmetic)} \\ &= 2(2st+s), && \text{(Distributive Property)} \end{aligned}$$

which is even, so $(-1)^{(p-1)(q-1)/4} = 1$. Thus $(p/q)(q/p) = (-1)^{(p-1)(q-1)/4} = 1$.

$\boxed{2 \Rightarrow 3}$ Assume that $(p/q)(q/p) = (-1)^{(p-1)(q-1)/4}$ and $p \nmid a$. Recall that the properties of the Legendre symbol tell us that if a is composite, then $(a/p) = (m/p)(n/p)$, where $a = mn$. Thus it is sufficient to show that the result holds when a is prime.

Suppose $a = 2$ and $p \equiv q \mod 4a$. Then $p \equiv q \mod 8$. So by Theorem 8.3.4, $(a/p) = (a/q)$. Suppose that $p \equiv -q \mod 8$. Then $p \equiv 1 \mod 8$ implies that $q \equiv 7 \mod 8$. Likewise, if $p \equiv 3 \mod 8$, then $q \equiv 5 \mod 8$, etcetera. Thus $(a/p) = (a/q)$ by Theorem 8.3.4.

Suppose now that a is an odd prime. Then $(p/a)(a/p) = (-1)^{(p-1)(a-1)/4}$ and $(q/a)(a/q) = (-1)^{(q-1)(a-1)/4}$. Suppose $p \equiv q \mod 4a$. Then

$$
\begin{aligned}
& p \equiv q \mod 4a \\
\iff & p = q + (4a)k, \text{ for some } k \in \mathbb{Z} && \text{(Definition of congruent)} \\
\iff & p = q + a(4k) && \text{(Associativity in } \mathbb{Z}) \\
\implies & p \equiv q \mod a, && \text{(Definition of congruent)}
\end{aligned}
$$

which implies that $(p/a) = (q/a)$. So now we have

$$\begin{aligned}
(a/p) &= (-1)^{(p-1)(a-1)/4}(p/a) \\
&= (-1)^{(p-1)(a-1)/4}(q/a) && ((p/a) = (q/a)) \\
&= (-1)^{(p-1)(a-1)/4} \cdot (-1)^{(q-1)(a-1)/4}(a/q) && \text{(Substitution)} \\
&= (-1)^{((p-1)(a-1)+(q-1)(a-1))/4}(a/q) && \text{(Arithmetic)} \\
&= (-1)^{(a-1)(p-1+q-1)/4}(a/q) && \text{(Arithmetic)} \\
&= (-1)^{(a-1)(p+q-2)/4}(a/q). && \text{(Arithmetic)}
\end{aligned}$$

Note that $p \equiv q \bmod 4a$ implies that $p \equiv q \bmod 4$, by a similar argument to the one used previously. We examine the exponent on -1. Since a is odd, $a - 1$ is even. Recall that previously we let $p = q + 4ak$, for some $k \in \mathbb{Z}$. So

$$\begin{aligned}
\frac{p+q-2}{4} &= \frac{q+4ak+q-2}{4}, \text{ for some } k \in \mathbb{Z} && (p \equiv q \bmod 4a) \\
&= \frac{4ak + 2(q-1)}{4} \\
&= ak + \frac{q-1}{2}.
\end{aligned}$$

But q is an odd prime, so $q - 1$ is even, and it follows that $ak + \dfrac{q-1}{2}$ is an integer. Thus the exponent is an even integer, so $(a/p) = (a/q)$.

Suppose now that $p \equiv -q \bmod 4a$. Then $p \equiv -q \bmod a$, which implies

that $(p/a) = (-q/a) = (-1/a)(q/a)$. Thus

$$\begin{aligned}
(a/p) &= (-1)^{(p-1)(a-1)/4}(p/a) \\
&= (-1)^{(p-1)(a-1)/4}(-1/a)(q/a) && ((p/a) = (-1/a)(q/a)) \\
&= (-1)^{(p-1)(a-1)/4}(-1)^{(a-1)/2}(-1)^{(q-1)(a-1)/4}(a/q) && \text{(Substitution)} \\
&= (-1)^{((a-1)/2)((p-1+2+q-1)/2)}(a/q) && \text{(Properties of exponents)} \\
&= (-1)^{(a-1)(p+q)/4}(a/q). && \text{(Arithmetic)}
\end{aligned}$$

Without loss of generality, suppose that $p \equiv 1 \bmod 4$ and $q \equiv -1 \equiv 3 \bmod 4$. Let $p = 4t + 1$ and $q = 4s + 3$, for $s, t \in \mathbb{Z}$. Then

$$\begin{aligned}
\frac{p+q}{4} &= \frac{4t + 1 + 4s + 3}{4} \\
&= \frac{4(t + s + 1)}{4} && \text{(Arithmetic)} \\
&= t + s + 1,
\end{aligned}$$

so $(a/p) = (-1)^{(a-1)(t+s+1)}(a/q)$. But $a - 1$ is even, so $(a/p) = (a/q)$.

$\boxed{3 \Rightarrow 1}$ Assume that whenever $p \equiv \pm q \bmod 4a$ and $p \nmid a$, for some $a \in \mathbb{N}$, then $(a/p) = (a/q)$ is true. We want to show that if $p \equiv q \equiv 3 \bmod 4$, then $(p/q) = -(q/p)$, and otherwise $(p/q) = (q/p)$.

So

$$\begin{aligned}
(p/q) &= (q + 4a/q) && (p = q + 4a) \\
&= (4a/q) && (q + 4a \equiv 4a \bmod q) \\
&= (a/q) && \text{(Lemma 8.3.10)} \\
&= (a/p) && ((a/p) = (a/q)) \\
&= (4a/p) && \text{(Lemma 8.3.10)} \\
&= (p - q/p) && (p - q = 4a) \\
&= (-q/p) && (p - q \equiv -q \bmod p) \\
&= (-1/p)(q/p) && \text{(Properties of Legendre Symbol)} \\
&= (-1)^{(p-1)/2}(q/p). && \text{(Law of Quadratic Reciprocity)}
\end{aligned}$$

Suppose that $p \equiv 1 \bmod 4$, and let $p = 4t + 1$ for some $t \in \mathbb{Z}$. Then

$$\begin{aligned}
(p/q) &= (-1)^{(4t+1-1)/2}(q/p) && \text{(Substitution)} \\
&= (-1)^{2t}(q/p) && \text{(Arithmetic)} \\
&= (q/p).
\end{aligned}$$

By a symmetric argument, if we suppose that $q \equiv 1 \bmod 4$ and interchange p and q, we have $(q/p) = (p/q)$.

Suppose instead that $p \equiv q \equiv 3 \bmod 4$ and let $p = 4t + 3$ for some

$t \in \mathbb{Z}$. Then

$$\begin{aligned}
(p/q) &= (-1)^{(4t+3-1)/2}(q/p) && \text{(Substitution)} \\
&= (-1)^{2t+1}(q/p) && \text{(Arithmetic)} \\
&= -(q/p).
\end{aligned}$$

It follows that the three statements are equivalent. ∎

We are now in a position to look at some examples that pull together the various forms of the Law of Quadratic Reciprocity together with the properties of the Legendre symbol to determine whether or not selected quadratic congruences have solutions.

Example 8.3.12 Consider the congruence $x^2 \equiv 800 \bmod 431$.

$$\begin{aligned}
\left(\frac{800}{431}\right) &\equiv \left(\frac{369}{431}\right) \bmod 431 && \text{(Property 3 of Legendre symbols)} \\
&\equiv \left(\frac{3^2}{431}\right)\left(\frac{41}{431}\right) \bmod 431 && \text{(Property 2 of Legendre symbols)} \\
&\equiv (1)\cdot\left(\frac{41}{431}\right) \bmod 431 && \text{(Property 4 of Legendre symbols)} \\
&\equiv \left(\frac{431}{41}\right) \bmod 431 && \text{(Law of Quadratic Reciprocity)} \\
&\equiv \left(\frac{21}{41}\right) \bmod 431 && \text{(Property 3 of Legendre symbols)} \\
&\equiv \left(\frac{7}{41}\right)\left(\frac{3}{41}\right) \bmod 431 && \text{(Property 2 of Legendre symbols)} \\
&\equiv -\left(\frac{41}{7}\right)\cdot -\left(\frac{41}{3}\right) \bmod 431 && \text{(Law of Quadratic Reciprocity)} \\
&\equiv (-1)^2\left(-\frac{1}{7}\right)\left(\frac{2}{3}\right) \bmod 431 && \text{(Property 3 of Legendre symbols)} \\
&\equiv (-1)^{(7-1)/2}\cdot(-1)^{(3^2-1)/8} \bmod 431 && \text{(Law of Quadratic Reciprocity)} \\
&\equiv (-1)^3\cdot(-1)^1 \bmod 431 && \text{(Arithmetic)} \\
&\equiv 1 \bmod 431. && \text{(Arithmetic)}
\end{aligned}$$

It follows that $x^2 \equiv 800 \bmod 431$ has a solution. Sadly, these tools that we have developed do not help us to actually find the solution, but we do know that it exists in this example. □

Example 8.3.13 Now consider the congruence $x^2 \equiv 17471 \bmod 1697$. If we use a similar strategy as that used in the previous example, it yields the

following.

$$\begin{aligned}
\left(\frac{17471}{1697}\right) &\equiv \left(\frac{501}{1697}\right) \bmod 1697 && \text{(Property 3 of Legendre symbols)}\\
&\equiv \left(\frac{3}{1697}\right)\left(\frac{167}{1697}\right) \bmod 1697 && \text{(Property 2 of Legendre symbols)}\\
&\equiv \left(\frac{1697}{3}\right)\left(\frac{1697}{167}\right) \bmod 1697 && \text{(Law of Quadratic Reciprocity)}\\
&\equiv \left(\frac{2}{3}\right)\left(\frac{27}{167}\right) \bmod 1697 && \text{(Property 3 of Legendre symbols)}\\
&\equiv \left(\frac{2}{3}\right)\left(\frac{3^2}{167}\right)\left(\frac{3}{167}\right) \bmod 1697 && \\
& && \text{(Property 2 of Legendre symbols)}\\
&\equiv (-1)^{(3^2-1)/8}\cdot(1)\cdot -\left(\frac{167}{3}\right) \bmod 1697 && \\
& && \text{(Law of Quadratic Reciprocity)}\\
&\equiv (-1)(-1)\left(\frac{2}{3}\right) && \text{(Property 3 of Legendre symbols)}\\
&\equiv (-1)^{(3^2-1)/8} \bmod 1697 && \text{(Law of Quadratic Reciprocity)}\\
&\equiv -1 \bmod 1697. && \text{(Arithmetic)}
\end{aligned}$$

Suppose that now we want to examine $x^2 \equiv 1697 \bmod 17471$ to see if it has a solution. We could certainly repeat the above process to figure it out directly, but this method is a fair bit of work, and there are a lot of places where arithmetic errors could occur. This is where the Law of Quadratic Reciprocity

comes in handy. We know that

$$\left(\frac{17471}{1697}\right)\left(\frac{1697}{17471}\right) = (-1)^{(17471-1)(1697-1)/4} \quad \text{(Law of Quadratic Reciprocity)}$$
$$= (-1)^{7407280} \qquad \text{(Arithmetic)}$$
$$= 1,$$

so either both $\left(\frac{17471}{1697}\right)$ and $\left(\frac{1697}{17471}\right)$ are equal to 1 or they are both equal to -1. Since $\left(\frac{17471}{1697}\right) = -1$, it must be the case that $\left(\frac{1697}{17471}\right) = -1$ as well. Thus, neither congruence has a solution, and we haven't wasted a lot of time looking for solutions that don't exist. □

Example 8.3.14 Consider the congruence $x^2 + 5x \equiv 0 \bmod 37$. It seems only natural to wonder whether or not this congruence has a solution, but we have not discussed how to make that determination. However, we can use ideas from algebra to manipulate it into something that looks more familiar to us.

First just consider the equation $x^2 + 5x = 0$. If we complete the square, then we have

$$\left(x + \frac{5}{2}\right)^2 = \frac{25}{4}.$$

This is the basic idea we want to use on our congruence, but we need to make some minor changes. First, fractions are essentially meaningless when working modulo 37, so we need to write them in a different form. If we think about $\mathbb{Z}_37$, we can see easily that $4^{-1} = -9$, since $-9 \cdot 4 = 36 \equiv 1 \bmod 37$. Similarly,

$2^{-1} = -18$. So if we use these results on our congruence, we can rewrite it as

$$\begin{aligned} & x^2 + 5x \equiv 0 \bmod 37 \\ \implies & \left(x + 5 \cdot 2^{-1}\right)^2 \equiv 25 \cdot 4^{-1} \bmod 37 \\ \implies & (x - 90)^2 \equiv -225 \bmod 37 \\ \implies & (x - 90)^2 \equiv 34 \bmod 37. \end{aligned}$$

Now let $y = (x - 90)^2$, so our congruence becomes $y^2 \equiv 34 \bmod 37$, which is something we know how to evaluate for solvability.

$$\begin{aligned} \left(\frac{34}{37}\right) &= \left(\frac{2}{37}\right)\left(\frac{17}{37}\right) \\ &= (-1)\left(\frac{37}{17}\right) && \text{(Law of Quadratic Reciprocity)} \\ &= (-1)\left(\frac{3}{17}\right) && \text{(Property 3 of Legendre symbols)} \\ &= (-1)\left(\frac{17}{3}\right) && \text{(Law of Quadratic Reciprocity)} \\ &= (-1)\left(\frac{2}{3}\right) && \text{(Property 3 of Legendre symbols)} \\ &= (-1)(-1) && \text{(Law of Quadratic Reciprocity)} \\ &= 1. \end{aligned}$$

Thus $y^2 \equiv 34 \bmod 37$ has a solution, so $(x - 90)^2 \equiv 34 \bmod 37$ must also have a solution. But we got this congruence by completing the square on $x^2 + 5x \equiv 0 \bmod 37$, so it is necessarily solvable. □

Example 8.3.15 Suppose we have the congruence $2x^2 + 29x + 15 \equiv 0 \bmod 73$. We will use a similar method as that used in the previous example to determine

whether or not this has a solution. Note that when working modulo 73, the inverse of 2 is 36.

$$
\begin{aligned}
& 2x^2 + 29x + 15 \equiv 0 \bmod 73 \\
\implies & 2x^2 + 29x \equiv -15 \bmod 73 \\
\implies & 2x^2 + 29x \equiv 58 \bmod 73 \\
\implies & 2^{-1} \cdot 2x^2 + 2^{-1} \cdot 29x \equiv 2^{-1} \cdot 58 \bmod 73 \\
\implies & x^2 + (36)(29)x \equiv (36)(58) \bmod 73 \\
\implies & x^2 + 1044x \equiv 2088 \bmod 73 \\
\implies & x^2 + 1044x + (36 \cdot 1044)^2 \equiv 2088 + (36 \cdot 1044)^2 \bmod 73 \\
\implies & x^2 + 22x + 37584^2 \equiv 2088 + 37584^2 \bmod 73 \\
\implies & x^2 + 22x + 62^2 \equiv 19 \bmod 73 \\
\implies & (x + 62)^2 \equiv 19 \bmod 73
\end{aligned}
$$

So if we again make a substitution, then $y^2 \equiv 19 \bmod 73$ and

$$
\begin{aligned}
\left(\frac{19}{73}\right) &= \left(\frac{73}{19}\right) && \text{(Law of Quadratic Reciprocity)} \\
&= \left(\frac{16}{19}\right) && \text{(Property 3 of Legendre symbols)} \\
&= 1. && \text{(Property 4 of Legendre symbols)}
\end{aligned}
$$

Thus $y^2 \equiv 19 \bmod 73$ is solvable, which implies that $(2 + 62)^2 \equiv 19 \bmod 73$ is solvable, and thus $2x^2 + 29x + 15 \equiv 0 \bmod 73$ is solvable. □

Recall that assertion 1 of Theorem 8.3.11 states that for odd primes

p and q, if $p \equiv q \equiv 3 \bmod 4$, then $(p/q) = -(q/p)$ and otherwise we have $(p/q) = (q/p)$. The following proposition states this in a slightly different form. Because it does not give us any new results, we offer it without proof, but the proof can be found in [8].

Proposition 8.3.16 *Let q be an odd prime.*

1. *If $q \equiv 1 \bmod 4$, then q is a quadratic residue modulo p if and only if $p \equiv r \bmod q$, where r is a quadratic residue mod q.*

2. *If $q \equiv 3 \bmod 4$, then q is a quadratic residue modulo p if and only if $p \equiv \pm b^2 \bmod 4q$, where b is an odd integer relatively prime to q.*

8.4 Jacobi Symbol

We are going to introduce a new symbol, called the *Jacobi symbol*. It is somewhat similar to the Legendre symbol, in that it relates to the congruence $x^2 \equiv a \bmod b$, where b is not necessarily prime. However, we shall see momentarily that the output of the Jacobi symbol is not always completely helpful.

Definition 8.4.1 Let b be an odd, positive integer and a any integer such that $\gcd(a, b) = 1$. Let $b = p_1 p_2 \dots p_k$, where the p_i are not necessarily distinct primes. The symbol $[a/b]$ defined by

$$[a/b] = (a/p_1)(a/p_2)\dots(a/p_k)$$

is called the *Jacobi symbol*. $\diamondsuit$

The Jacobi symbol is a generalization of the Legendre symbol, but they are not the same. The right hand side of the definition is composed of Legendre symbols. Thus the Jacobi symbol is the product of a finite number of Legendre symbols. In other words, it is the product of a finite number of values of 1 and -1.

We must be cautious when we interpret the output of the Jacobi symbol. Recall that if we have $x^2 \equiv a \bmod b$ and $b = p_1 p_2 \dots p_k$, then by Corollary 6.1.2, we can write this congruence as the system of congruences

$$x^2 \equiv a \bmod p_1, x^2 \equiv a \bmod p_2, \dots, x^2 \equiv a \bmod p_k.$$

So the Jacobi symbol is really trying to tell us whether or not there is a solution to this system of congruences.

If $[a/b] = -1$, then at least one of the Legendre symbols is necessarily equal to -1, which means that at least one of the congruences in the system does not have a solution, so the system is not solvable. Thus $x^2 \equiv a \bmod b$ does not have a solution, so in this case, the output is helpful.

On the other hand, suppose that $[a/b] = 1$. There are two possibilities here. Either each of the Legendre symbols is equal to 1, which means that each congruence in the system has a solution, or there are an even number of Legendre symbols that are equal to -1. In the first case, $x^2 \equiv a \bmod b$ has a solution, since every congruence in the system is solvable, but in the second

case, it does not. Thus just having a Jacobi symbol output of 1 is not enough on its own to tell us anything useful about the solvability of $x^2 \equiv a \bmod b$.

For example, consider $[2/63]$. If we evaluate this using the definition of the Jacobi symbol and properties of the Legendre symbol, then

$$\begin{aligned}
[2/63] &= (2/3)(2/3)(2/7) \\
&\equiv (-1)^{(3^2-1)/8} \bmod 3 \cdot (-1)^{(3^2-1)/8} \bmod 3 \cdot (-1)^{(7^2-1)/8} \bmod 7 \\
&= (-1)(-1)(1) \\
&= 1.
\end{aligned}$$

If we just saw that $[2/63] = 1$, without the benefit of seeing the intermediate work, we might be tempted to assume that $x^2 \equiv 2 \bmod 63$ has a solution, but in fact it does not. This can be verified by checking each $x \in \{1, 2, \ldots, 62\}$, but is omitted here.

Generally speaking, the Jacobi symbol is denoted as (a/b) rather than as $[a/b]$, but to avoid confusion with the Legendre symbol, we will use $[a/b]$ to denote the Jacobi symbol in this thesis. As with the Legendre symbol, sometimes it will be more convenient to use $\left[\frac{a}{b}\right]$ rather than $[a/b]$. The two versions of the symbol are interchangeable, and we will endeavor to make the usage clear if this same notation is used for anything else, such as the greatest integer function.

We will state and prove some properties about the Jacobi symbol, but first we need to establish some results that will help us in part of the proof.

Lemma 8.4.2 *Suppose $j, k \in \mathbb{Z}$ and $n \in \mathbb{N}$. Then $(1 + jk)^n \equiv njk \bmod j^2$.*

Proof: By the Binomial Expansion Theorem, $(1+jk)^n = \sum_{i=0}^{n} \binom{n}{i} (jk)^i$. For each $i \geqslant 2$, $\binom{n}{i}(jk)^i \equiv 0 \bmod j^2$, since each of these terms contains a factor of j^2. Thus we are left with only the first two terms, and it follows that $(1 + jk)^n \equiv 1 + njk \bmod j^2$. ∎

Suppose that instead of $(1 + jk)^n$, we have $\prod_{i=1}^{n}(1 + jk_i)$, where each $k_i \in \mathbb{Z}$. Then $\prod_{i=1}^{n}(1 + jk_i) = \sum_{i=0}^{n} j^i C$, where C is the sum of all of the products of subsets of size i of $\{k_1 k_2 \ldots k_n\}$. But for each $i \geqslant 2$, $\sum_{i=0}^{n} j^i C \equiv 0 \bmod j^2$, for the same reasons as given in the proof of the lemma above. It follows that

$$\prod_{i=1}^{n}(1 + jk_i) \equiv 1 + j \sum_{i=1}^{n} k_i \bmod j^2.$$

Theorem 8.4.3 (Properties of the Jacobi Symbol) *Assume that b is an odd positive integer and a is any integer. Then for all such a and b, the following properties hold.*

1. *If $a_1 \equiv a_2 \bmod b$, then $[a_1/b] = [a_2/b]$.*
2. $[a_1 a_2/b] = [a_1/b][a_2/b]$.
3. $[a/b_1 b_2] = [a/b_1][a/b_2]$.

4. $[-1/b] = (-1)^{(b-1)/2}$.

5. $[2/b] = (-1)^{(b^2-1)/8}$.

Proof: Unless specified otherwise, for each piece of this proof, assume that b is an odd, positive integer and assume that $a_1, a_2 \in \mathbb{Z}$. We will represent b by its prime factorization, so $b = p_1 p_2 \dots p_m$, where the p_i are not necessarily distinct.

1. Suppose that $a_1 \equiv a_2 \bmod b$. Then

$$\begin{aligned}
[a_1/b] &= (a_1/p_1)(a_1/p_2)\dots(a_1/p_m) && \text{(Definition of Jacobi symbol)} \\
&= (a_2/p_1)(a_2/p_2)\dots(a_2/p_m) && \text{(Property 3 of Legendre symbol)} \\
&= [a_2/b]. && \text{(Definition of Jacobi symbol)}
\end{aligned}$$

2.

$$\begin{aligned}
\left[\frac{a_1 a_2}{b}\right] &= \left(\frac{a_1 a_2}{p_1}\right)\left(\frac{a_1 a_2}{p_2}\right)\dots\left(\frac{a_1 a_2}{p_m}\right) && \text{(Definition of Jacobi symbol)} \\
&= \left(\frac{a_1}{p_1}\right)\left(\frac{a_2}{p_1}\right)\left(\frac{a_1}{p_2}\right)\left(\frac{a_2}{p_2}\right)\dots\left(\frac{a_1}{p_m}\right)\left(\frac{a_2}{p_m}\right) \\
& && \text{(Property 2 of Legendre Symbol)} \\
&= \left(\frac{a_1}{p_1}\right)\left(\frac{a_1}{p_2}\right)\dots\left(\frac{a_1}{p_m}\right)\left(\frac{a_2}{p_1}\right)\left(\frac{a_2}{p_2}\right)\dots\left(\frac{a_2}{p_m}\right) \\
& && \text{(Commutative Property)} \\
&= \left[\frac{a_1}{b}\right]\left[\frac{a_2}{b}\right] && \text{(Definition of Jacobi symbol)}
\end{aligned}$$

3. Assume b_1 and b_2 are odd, positive integers and $a \in \mathbb{Z}$. Let the prime factorizations of $b_1 = p_1 p_2 \dots p_m$ and $b_2 = q_1 q_2 \dots q_n$, where the p_i and q_j are not necessarily distinct. Then $b_1 b_2 = p_1 p_2 \dots p_m q_1 q_2 \dots q_n$, and

$$\left[\frac{a}{b_1 b_2}\right] = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\dots\left(\frac{a}{p_m}\right)\left(\frac{a}{q_1}\right)\left(\frac{a}{q_2}\right)\dots\left(\frac{a}{q_n}\right)$$

(Definition of Jacobi symbol)

$$= \left[\frac{a}{b_1}\right]\left[\frac{a}{b_2}\right].$$

(Definition of Jacobi symbol)

4. Let $b = p_1^{e_1} p_2^{e_2} \dots p_m^{e_m}$ be the prime power decomposition of b. Note that since b is an odd integer, each p_i is also odd. By the Law of Quadratic Reciprocity, we know that if p is prime, then $(-1/p) = (-1)^{(p-1)/2}$. Thus

$$[-1/b] = (-1/p_1)^{e_1}(-1/p_2)^{e_2}\dots(-1/p_m)^{e_m}$$

(Definition of Jacobi Symbol)

$$= (-1)^{e_1(p_1-1)/2 + e_2(p_2-1)/2 + \dots + e_m(p_m-1)/2}.$$

(Law of Quadratic Reciprocity)

Now, since $b = p_1^{e_1} p_2^{e_2} \dots p_m^{e_m}$, we can cleverly write b as

$$b = \big(1 + (p_1 - 1)\big)^{e_1}\big(1 + (p_2 - 1)\big)^{e_2}\dots\big(1 + (p_m - 1)\big)^{e_m}.$$

Now apply Lemma 8.4.2, with $j = 2$ and $k = \dfrac{p_i - 1}{2}$. Then

$$\begin{aligned} b &= \big(1 + (p_1 - 1)\big)^{e_1}\big(1 + (p_2 - 1)\big)^{e_2} \dots \big(1 + (p_m - 1)\big)^{e_m} \\ &= \left(1 + 2\left(\frac{p_1 - 1}{2}\right)\right)^{e_1} \dots \left(1 + 2\left(\frac{p_m - 1}{2}\right)\right)^{e_m} \\ &\equiv \left(1 + 2e_1\left(\frac{p_1 - 1}{2}\right)\right) \dots \left(1 + 2e_m\left(\frac{p_m - 1}{2}\right)\right) \bmod 4 \end{aligned}$$

(Lemma 8.4.2)

$$\equiv 1 + 2\sum_{i=1}^{m} e_i\left(\frac{p_i - 1}{2}\right) \bmod 4$$

(By the comment following Lemma 8.4.2)

$$\equiv 1 + e_1(p_1 - 1) + e_2(p_2 - 1) + \cdots + e_m(p_m - 1) \bmod 4,$$

which implies that $b - 1 \equiv e_1(p_1 - 1) + \cdots + e_m(p_m - 1) \bmod 4$.

Since b is odd, $b-1$ is even, and we know that each $p_i - 1$ is also even. In Theorem 4.3.19, it was stated that if $ac \equiv bc \bmod m$ and $\gcd(c, m) = d$, then $a \equiv b \bmod (m/d)$. Thus we have

$$\frac{b-1}{2} \equiv \frac{e_1(p_1 - 1)}{2} + \cdots + \frac{e_m(p_m - 1)}{2} \bmod 2.$$

Recall that initially we came up with

$$[-1/b] = (-1)^{e_1(p_1-1)/2 + e_2(p_2-1)/2 + \cdots + e_m(p_m-1)/2}.$$

Combining these two results yields $[-1/b] = (-1)^{(b-1)/2}$. But the only least residues modulo p are 0 and 1, so since $\dfrac{b-1}{2}$ can only take values of 0 or 1 modulo 2, the result is either 1 or -1, as required.

5. Recall that if p is prime, then by the Law of Quadratic Reciprocity, $(2/p) = (-1)^{(p^2-1)/8}$. Thus

$$\begin{aligned}[2/b] &= (2/p_1)^{e_1}(2/p_2)^{e_2}\dots(2/p_m)^{e_m} \qquad \text{(Definition of Jacobi Symbol)}\\ &= (-1)^{e_1(p_1^2-1)/8+e_2(p_2^2-1)/8+\cdots+e_m(p_m^2-1)/8}.\end{aligned}$$

(Law of Quadratic Reciprocity)

If we square b, we have $b^2 = p_1^{2e_1}p_2^{2e_2}\dots p_m^{2e_m}$, which can be expressed as

$$b^2 = \big(1+(p_1^2-1)\big)^{e_1}\big(1+(p_2^2-1)\big)^{e_2}\dots\big(1+(p_m^2-1)\big)^{e_m}.$$

Now since each p_i is odd, we know that $p_i^2-1 \equiv 0 \bmod 8$, by Lemma 6.0.14, so let $p_i^2 - 1 = 8k_i$, for some $k_i \in \mathbb{Z}$. Then applying Lemma 8.4.2 yields

$$\begin{aligned}b^2 &= \big(1+(p_1^2-1)\big)^{e_1}\big(1+(p_2^2-1)\big)^{e_2}\dots\big(1+(p_m^2-1)\big)^{e_m}\\ &= (1+8k_1)^{e_1}(1+8k_2)^{e_2}\dots(1+8k_m)^{e_m} \qquad \text{(Substitution)}\\ &\equiv (1+8e_1k_1)(1+8e_2k_2)\dots(1+8e_mk_m) \bmod 64 \qquad \text{(Lemma 8.4.2)}\\ &\equiv 1+8\sum_{i=1}^{m} e_ik_i \bmod 64 \quad \text{(By the comment following Lemma 8.4.2)}\\ &\equiv 1+8e_1k_1+8e_2k_2+\cdots+8e_mk_m \bmod 64\\ &\equiv 1+e_1(p_1^2-1)+e_2(p_2^2-1)+\dots e_m(p_m^2-1) \bmod 64,\end{aligned}$$

(Substitution)

which implies that $b^2-1 \equiv e_1(p_1^2-1)+e_2(p_2^2-1)+\cdots+e_m(p_m^2-1) \bmod 64$. Since b is odd, $b^2-1 \equiv 0 \bmod 8$, by Lemma 6.0.14. Each $p_i^2-1 \equiv 0 \bmod 8$

as well, so by Theorem 4.3.19, we have

$$\frac{b^2-1}{8} \equiv \frac{e_1(p_1^2-1)}{8} + \cdots + \frac{e_m(p_m^2-1)}{8} \bmod 8.$$

Initially we had

$$[2/b] = (-1)^{e_1(p_1^2-1)/8+e_2(p_2^2-1)/8+\cdots+e_m(p_m^2-1)/8},$$

so combining these two results yields $[2/b] = (-1)^{(b^2-1)/8}$ as desired.

It follows that the five properties of Jacobi symbols hold. ∎

Now we look at some examples that utilize the properties of Legendre symbols, properties of Jacobi symbols, and the Law of Quadratic Reciprocity.

Example 8.4.4 Consider $x^2 \equiv 273 \bmod 110$. The Jacobi symbol for this congruence is $\left[\frac{273}{110}\right]$ and we can apply the properties of Legendre and Jacobi

symbols to evaluate it.

$$\begin{aligned}
\left[\frac{273}{110}\right] &= \left[\frac{3}{110}\right]\left[\frac{7}{110}\right]\left[\frac{13}{110}\right] && \text{(Property 2 of Jacobi symbols)}\\
&= \left(\frac{3}{2}\right)\left(\frac{3}{5}\right)\left(\frac{3}{11}\right)\left(\frac{7}{2}\right)\left(\frac{7}{5}\right)\left(\frac{7}{11}\right)\left(\frac{13}{2}\right)\left(\frac{13}{5}\right)\left(\frac{13}{11}\right)\\
& && \text{(Definition of Jacobi symbol)}\\
&= \left(\frac{1}{2}\right)\left(\frac{3}{5}\right)\left(\frac{3}{11}\right)\left(\frac{1}{2}\right)\left(\frac{2}{5}\right)\left(\frac{7}{11}\right)\left(\frac{1}{2}\right)\left(\frac{3}{5}\right)\left(\frac{2}{11}\right)\\
& && \text{(Property 3 of Legendre symbols)}\\
&= (1)\left(\frac{3}{5}\right)\left(\frac{3}{11}\right)(1)\left(\frac{2}{5}\right)\left(\frac{7}{11}\right)(1)\left(\frac{3}{5}\right)\left(\frac{2}{11}\right)\\
& && \text{(Property 1 of Legendre symbols)}\\
&= \left(\frac{5}{3}\right)(-1)\left(\frac{11}{3}\right)\left(\frac{2}{5}\right)(-1)\left(\frac{11}{7}\right)\left(\frac{5}{3}\right)\left(\frac{2}{11}\right)\\
& && \text{(Law of Quadratic Reciprocity)}\\
&= \left(\frac{2}{3}\right)\left(\frac{2}{3}\right)\left(\frac{2}{5}\right)\left(\frac{4}{7}\right)\left(\frac{2}{3}\right)\left(\frac{2}{11}\right)\\
& && \text{(Property 3 of Legendre symbols)}\\
&= \left(\frac{2}{3}\right)^3\left(\frac{2}{5}\right)(1)\left(\frac{2}{11}\right) && \text{(Property 4 of Legendre symbols)}\\
&= \left((-1)^{(3^2-1)/8}\right)^3(-1)^{(5^2-1)/8}(-1)^{(11^2-1)/8}\\
& && \text{(Law of Quadratic Reciprocity)}\\
&= (-1)^3(-1)^3(-1)^{15} && \text{(Arithmetic)}\\
&= -1,
\end{aligned}$$

so the congruence has no solution. □

Example 8.4.5 Consider $x^2 \equiv 1534 \bmod 2805$.

$$\left[\frac{1534}{2805}\right] = \left(\frac{1534}{3}\right)\left(\frac{1534}{5}\right)\left(\frac{1534}{11}\right)\left(\frac{1534}{17}\right) \quad \text{(Definition of Jacobi symbol)}$$

$$= (1/3)(4/5)(5/11)(4/17) \quad \text{(Property 3 of Legendre symbols)}$$

$$= (1)(1)(5/11)(1) \quad \text{(Property 4 of Legendre symbols)}$$

$$= (11/5) \quad \text{(Law of Quadratic Reciprocity)}$$

$$= (1/5) \quad \text{(Property 3 of Legendre symbols)}$$

$$= 1 \quad \text{(Property 4 of Legendre symbols)}$$

In this example, the result is 1, but we stated earlier that there can be some uncertainty as to what a result of 1 actually means. If we consider the original congruence again, we can apply Corollary 6.1.2 to split it into the system of congruences

$$x^2 \equiv 1534 \bmod 3$$

$$x^2 \equiv 1534 \bmod 5$$

$$x^2 \equiv 1534 \bmod 11$$

$$x^2 \equiv 1534 \bmod 17.$$

Now as we evaluated the corresponding Legendre symbol for each of the congruences in this system, notice that each of them had an output of 1. Thus each of the congruences in the system was solvable, which in turns means that the system is solvable. So in this case, having an output of 1 means that our original congruence does have a solution. □

Theorem 8.4.6 (Reciprocity Law for the Jacobi Symbol) *Let a and b be odd, positive integers, where* $\gcd(a, b) = 1$. *Then*

$$[a/b][b/a] = (-1)^{((a-1)/2)((b-1)/2)}.$$

Proof: Assume that both a and b are odd, positive integers and represent a and b by their prime power decompositions. Then $a = q_1^{a_1} q_2^{a_2} \dots q_n^{a_n}$ and $b = p_1^{b_1} p_2^{b_2} \dots p_m^{b_m}$.

Then

$$\begin{aligned}
[a/b] &= (a/p_1)^{b_1}(a/p_2)^{b_2} \dots (a/p_m)^{b_m} && \text{(Substitution for } b\text{)} \\
&= \prod_{i=1}^{m} (a/p_i)^{b_i} && \text{(Write as product over } i\text{)} \\
&= \prod_{i=1}^{m} \prod_{j=1}^{n} (q_j/p_i)^{a_j b_i} && \text{(Substitution for } a\text{)}
\end{aligned}$$

and

$$\begin{aligned}
[b/a] &= (b/q_1)^{a_1}(b/q_2)^{a_2} \dots (b/q_n)^{a_n} && \text{(Substitution for } a\text{)} \\
&= \prod_{j=1}^{n} (b/q_j)^{a_j} && \text{(Write as product over } j\text{)} \\
&= \prod_{j=1}^{n} \prod_{i=1}^{m} (p_i/q_j)^{b_i a_j}. && \text{(Substitution for } b\text{)}
\end{aligned}$$

Combining these results yields

$$[a/b][b/a] = \prod_{i=1}^{m} \prod_{j=1}^{n} \big((q_j/p_i)(p_i/q_j)\big)^{a_j b_i}.$$

By the Law of Quadratic Reciprocity, we have

$$(q_j/p_i)(p_i/q_j) = (-1)^{((q_j-1)/2)((p_i-1)/2)},$$

thus

$$\begin{aligned}
[a/b][b/a] &= \prod_{i=1}^{m}\prod_{j=1}^{n}\left((-1)^{((q_j-1)/2)((p_i-1)/2)}\right)^{a_j b_i} && \text{(Substitution)}\\
&= \prod_{i=1}^{m}\prod_{j=1}^{n}(-1)^{b_i((p_i-1)/2)\cdot a_j((q_j-1)/2)} && \text{(Properties of Exponents)}\\
&= (-1)^{\sum_{i=1}^{m}\sum_{j=1}^{n} b_i((p_i-1)/2)\cdot a_j((q_j-1)/2)}. && \text{(Properties of Exponents)}
\end{aligned}$$

Notice that

$$\sum_{i=1}^{m}\sum_{j=1}^{n} b_i\left(\frac{p_i-1}{2}\right)\cdot a_j\left(\frac{q_j-1}{2}\right) = \sum_{i=1}^{m} b_i\left(\frac{p_i-1}{2}\right)\cdot\sum_{j=1}^{n} a_j\left(\frac{q_j-1}{2}\right).$$

Recall that in the proof of Property 4 of the Jacobi symbol, we showed that

$$\frac{b-1}{2} \equiv \frac{e_1(p_1-1)}{2} + \frac{e_2(p_2-1)}{2} + \cdots + \frac{e_m(p_m-1)}{2} \bmod 2.$$

If we apply this result twice to the right side of our equation above, we have

$$\sum_{i=1}^{m} b_i\left(\frac{p_i-1}{2}\right) \equiv \frac{b-1}{2} \bmod 2$$

and

$$\sum_{j=1}^{m} a_j\left(\frac{q_j-1}{2}\right) \equiv \frac{a-1}{2} \bmod 2.$$

Hence,

$$\sum_{i=1}^{m}\sum_{j=1}^{n} b_i\left(\frac{p_i-1}{2}\right)\cdot a_j\left(\frac{q_j-1}{2}\right) \equiv \frac{b-1}{2}\cdot\frac{a-1}{2} \bmod 2.$$

Combining these results yields

$$[a/b][b/a] = (-1)^{((a-1)/2)((b-1)/2)},$$

as desired. ∎

Example 8.4.7 We saw in Example 8.4.4 that $\left[\frac{273}{110}\right] = -1$. By the Reciprocity Law for the Jacobi Symbol,

$$\begin{aligned}\left[\frac{273}{110}\right]\left[\frac{110}{273}\right] &= (-1)^{(273-1)(110-1)/4} && \text{(Reciprocity Law for Jacobi Symbol)}\\ &= (-1)^{7412} && \text{(Arithmetic)}\\ &= 1.\end{aligned}$$

Thus it must be the case that $\left[\frac{110}{273}\right] = -1$ as well. This can in fact be verified by manipulations very similar to those done in Example 8.4.4. □

At first glance, it might seem like having this tool available now makes determination of quadratic residues a breeze, but in the Law of Quadratic Reciprocity, we were given very specific criteria for which we can interchange (p/q) and (q/p), and we are not given any similar guidelines with the Jacobi symbol. We are also restricted to both a and b being odd and positive to even be able to apply the Reciprocity Law for the Jacobi symbol, so we must use caution and be aware that we can not just swap one out for the other the way we could with Legendre symbols, so while it's yet another tool to use in determining whether or not quadratic congruences have solutions, one must still be cautious and not invoke any craziness.

8.5 Why do we care about any of this?

Quadratic residues and the Law of Quadratic Reciprocity have led to many different applications in various areas. A few such applications are in acoustics, cryptography, and graph theory [19].

8.5.1 Acoustics

Acoustic equipment, and more specifically sound diffusors, have been greatly improved because of the use of quadratic residues. Early sound diffusors were called Maximum Length Sequence (MLS) Diffusors and used a strictly geometric pattern to diffuse sound. They were somewhat restricted in terms of bandwidth, so they weren't very effective at certain frequencies. A diffusor called the quadratic-residue diffusor was developed that is an improvement on the MLS diffusor, because it can diffuse sound in either one or two directions, and its bandwidth is much wider, so it has a greater range of frequencies for which it is effective [15], [19].

8.5.2 Cryptography

With all of the activity taking place on the internet, cryptography has become a huge field, and methods must continually improve, as computers become faster and more powerful, and computing time of difficult problems is reduced. The backbone for one method involves finding solutions to congruences of

the form $x^2 \equiv a \bmod n$, where n is composite, because this is a difficult problem when n is a large number. In fact, in terms of level of difficulty and computation time, it is similar to the problem of trying to factor large numbers. Thus quadratic residues have been used as the basis for two methods known as the Rabin cryptosystem and oblivious transfer. Additionally, there is a specific problems called the quadratic residuosity problem that is at the heart of the Goldwasser-Micali cryptosystem [19].

Factorization of large integers is another area upon which cryptography methods are built. In Volume VI of the *Disquisitiones Arithmeticae*, Gauss apparently explained two different algorithms for factoring that were based on quadratic residues and the Law of Quadratic Reciprocity. There are factoring algorithms that are still being used today that are based on quadratic residues as well. Some of these are the continued fraction method, Dixon's algorithms, the number field sieve, and the quadratic sieve [19].

Closely related to the factorization of large integers is something called primality testing, where methods are developed to try to determine whether large numbers are prime or not. There is a procedure known as the Solovay-Strassen primality test that can be used to try to determine whether a given integer n is prime or not. Basically, a random integer a is chosen and the Legendre symbol (a/n) is computer using Euler's criterion, and then the congruence $a^{(n-1)/2} \equiv (a/n) \bmod n$ is examined. If n is a prime number, then

the congruence holds for all $a \in \mathbb{Z}$. Thus the general strategy for the test is to pick random values of a and check the congruence. As soon as an a is found for which the congruence is false, then it is known that n is prime. The value of a for which the congruence is false is called an *Euler witness for* n. On the other hand, the values of a for which the congruence is true when n is actually composite are called *Euler liars for* n. If a very large number of values of a are tested and the congruence holds, then n is termed a "probable prime" [19], [21]. There is another primality test that is loosely based on the use of quadratic residues, which is called the Miller-Rabin test. It is similar to the Solovay-Strassen primality test, but the Miller-Rabin test is said to be stronger and more accurate, because it allegedly produces "stronger" Euler witnesses and liars for n, and thus the probability that n is prime is much higher than other tests [16].

8.5.3 Graph Theory

There are a certain type of graphs in graph theory that are called Paley graphs, which have ties to quadratic residues. Paley graphs are undirected graphs that are constructed from elements of a finite field that differ by only a quadratic residue. Study of these graphs led to the development of something called Paley construction, which is used to create Hadamard matrices from quadratic residues. These matrices have been studied extensively, because they have

many interesting properties that fascinate mathematicians [17], [19].

These are just a few of the applications of quadratic residues and the Law of Quadratic Reciprocity that we were able to find. There may be other applications out there as well, and it may turn out that there will be future uses for these concepts that have not been thought of yet.

Chapter 9

Gauss and Jacobi Sums

9.1 Quadratic Gauss Sums

Gauss spent a lot of time studying cyclotomy, or how to divide a circle into n equal parts using only a compass and a straightedge [12]. But this leads to having n points equally spaced on the edge of a circle, which are the n^{th} roots of unity. Thus his studies gave him vast knowledge of the properties of sums of roots of unity [7].

It is this knowledge that led to Gauss' fourth and sixth proofs of the Law of Quadratic Reciprocity. The sums of roots of unity are now known as Gauss sums. The values of quadratic Gauss sums are used directly in Gauss' fourth proof, but his sixth proof uses them without evaluating them first [7]. Gauss' fourth and sixth proofs are not presented in this thesis, but

we introduce quadratic Gauss sums here so that we can generalize them later in this chapter. The generalized sums will play a role in our work with cubic reciprocity.

In Section 1, we examine various sums of roots of unity in general and then review the Kronecker δ-function. We look at some sums of Legendre symbols and develop important results, then define what it means to be a quadratic Gauss sum. In the second section, we define the Gauss sum in general, and the characters that we introduced earlier play a role. We establish more results and then in the third section, we define Jacobi sums. The remainder of the chapter is spent tying these ideas together. The Gauss and Jacobi sums are at the heart of several theorems we prove, and we establish some properties of Jacobi sums involving characters.

Recall that the n^{th} roots of unity are solutions to the equation $x^n = 1$. Earlier we defined ζ to be a primitive n^{th} root of unity if ζ is a generator for the group of n^{th} roots of unity. In this section, unless otherwise specified, ζ will represent $e^{2\pi i/p}$, which is a primitive p^{th} root of unity, for some prime $p \in \mathbb{Z}$.

Theorem 9.1.1 *Suppose p is prime. Then*

$$\sum_{t=0}^{p-1} \zeta^{at} = \begin{cases} p, & a \equiv 0 \bmod p \\ 0, & a \not\equiv 0 \bmod p. \end{cases}$$

Example 9.1.2 Let $p = 11$ and $a = 2$. Then examine $\sum_{t=0}^{10} \zeta^{2t}$. Recall that a geometric series is of the form $\sum_{k=0}^{n-1} ar^k$ and its sum is given by $a \cdot \frac{1-r^n}{1-r}$. If we rearrange our sum slightly, we have $\sum_{t=0}^{10} \left(\zeta^2\right)^t$, and it is now obvious that this is in fact a geometric sum with $r = \zeta^2$. Thus the sum is

$$\begin{aligned}
\sum_{t=0}^{10} \left(\zeta^2\right)^t &= \frac{1-\left(\zeta^2\right)^{11}}{1-\zeta^2} && \text{(Sum of finite geometric series)} \\
&= \frac{1-\left(\zeta^{11}\right)^2}{1-\zeta^2} && \text{(Properties of exponents)} \\
&= \frac{1-1^2}{1-\zeta^2} && (\zeta^{11} = 1) \\
&= 0.
\end{aligned}$$

Suppose instead that $a = 22$. Then

$$\begin{aligned}
\sum_{t=0}^{10} \zeta^{22t} &= \sum_{t=0}^{10} \left(\zeta^{11}\right)^{2t} && \text{(Properties of exponents)} \\
&= \sum_{t=0}^{10} 1 && (\zeta^{11} = 1) \\
&= 11.
\end{aligned}$$

Thus the sum is 0 when $a \not\equiv 0 \bmod p$ and p when a is a multiple of p. □

The proof of this Lemma is straightforward, and in fact mirrors the example almost exactly.

Proof: Suppose $a \equiv 0 \bmod p$. Then $a = kp$ for some $k \in \mathbb{Z}$, and

$$\begin{aligned}
\sum_{t=0}^{p-1} \zeta^{at} &= \sum_{t=0}^{p-1} \zeta^{kpt} && \text{(Substitution)} \\
&= \sum_{t=0}^{p-1} \left(\zeta^{p}\right)^{kt} && \text{(Properties of exponents)} \\
&= \sum_{t=0}^{p-1} 1 && (\zeta^{p} = 1) \\
&= p. && \text{(Arithmetic)}
\end{aligned}$$

Suppose now that $a \not\equiv 0 \bmod p$. Then a is not a multiple of p, so $\zeta^{a} \neq 1$. Thus

$$\begin{aligned}
\sum_{t=0}^{p-1} \zeta^{at} &= \sum_{t=0}^{p-1} \left(\zeta^{a}\right)^{t} && \text{(Properties of exponents)} \\
&= \frac{1 - \left(\zeta^{a}\right)^{p}}{1 - \zeta^{a}} && \text{(Sum of a finite geometric series)} \\
&= \frac{1 - \left(\zeta^{p}\right)^{a}}{1 - \zeta^{a}} && \text{(Properties of exponents)} \\
&= 0. && (\zeta^{p} = 1)
\end{aligned}$$

Hence the result holds as desired. ∎

Leopold Kronecker is credited with coming up with a simple function of two variables such that the output is 1 if the variables are equal and 0 if they are different. It is called the Kronecker δ-function, and has applications throughout mathematics, in fields such as linear algebra, calculus, and is even used in signal processing [13]. It is defined as follows.

For $x, y \in \mathbb{Z}$ and a prime p, define $\delta(x, y)$ by

$$\delta(x,y) = \begin{cases} 1, & x \equiv y \bmod p \\ 0, & x \not\equiv y \bmod p. \end{cases}$$

We will use the Kronecker δ-function in the following Corollary.

Corollary 9.1.3 *Suppose p is prime. Then $p^{-1} \cdot \sum_{t=0}^{p-1} \zeta^{t(x-y)} = \delta(x, y)$.*

Proof: Suppose $x \equiv y \bmod p$. Then $x - y \equiv 0 \bmod p$. Thus

$$\begin{aligned} p^{-1} \cdot \sum_{t=0}^{p-1} \zeta^{t(x-y)} &= p^{-1} \cdot p && \text{(Theorem 9.1.1)} \\ &= 1. && \text{(Multiplicative inverses)} \end{aligned}$$

Now suppose $x \not\equiv y \bmod p$. Then $x - y \not\equiv 0 \bmod p$, so

$$\begin{aligned} p^{-1} \cdot \sum_{t=0}^{p-1} \zeta^{t(x-y)} &= p^{-1} \cdot 0 && \text{(Theorem 9.1.1)} \\ &= 0. \end{aligned}$$

Thus the result holds for all $x, y \in \mathbb{Z}$ as desired. ∎

Lemma 9.1.4 *Suppose p is an odd prime. Then $\sum_{t=0}^{p-1} (t/p) = 0$, where (t/p) is the Legendre symbol.*

Proof: First note that $(0/p) = 0^{(p-1)/2} = 0$. Also, recall from Corollary 8.1.9, that there are as many residues as nonresidues, for any given prime

p. So we have

$$\begin{aligned}
\sum_{t=0}^{p-1}(t/p) &= (0/p) + \sum_{t=1}^{p-1}(t/p) && \text{(Split the sum)} \\
&= 0 + \left(\frac{p-1}{2}\right)(1) + \left(\frac{p-1}{2}\right)(-1) && \text{(Corollary 8.1.9)} \\
&= 0, && \text{(Arithmetic)}
\end{aligned}$$

as desired. ∎

We are now in a position to define the *quadratic Gauss sum* that will be developed in this section and then generalized later in the chapter. Gauss sums will be used together with *Jacobi sums* in the cubic reciprocity chapter.

Definition 9.1.5 The sum $g_a = \sum_{t=0}^{p-1}(t/p)\zeta^{at}$ is called a *quadratic Gauss sum*. In this sum, p is an odd prime and ζ is a p^{th} root of unity. ♢

Consider the cosets formed by the least residues of $\mathbb{Z}$ modulo p. Each coset contains integers that all have the same residue. If we choose one representative from each coset, this gives us a *complete set of representatives*, since each residue r such that $0 \leqslant r \leqslant p-1$ will be present exactly once. This can also be called a *complete system of residues*.

For example, if we take one element from a group and multiply it by each of the other elements of the group, we get a permutation of the group. So if $k \in \mathbb{Z}_p^*$, then $\{kt \bmod p : 1 \leqslant t \leqslant p-1\} = \mathbb{Z}_p^*$. Since $k \cdot 0 = 0$, we can extend this to $\{kt \bmod p : 0 \leqslant t \leqslant p-1\} = \{0, 1, \ldots, p-1\}$. Thus, when we

start with an element from $\mathbb{Z}_p$ and multiply it by each element in the group, the result is a complete system of residues, since every least residue for the given prime p is present in the set.

Theorem 9.1.6 *Suppose p is an odd prime. Then $g_a = (a/p)g_1$.*

Proof: By definition of quadratic Gauss sum,

$$g_a = \sum_{t=0}^{p-1} (t/p)\zeta^{at}.$$

Suppose $a \equiv 0 \bmod p$, which implies that $\zeta^{at} = 1$ for all t. Hence

$$g_a = \sum_{t=0}^{p-1} (t/p). \tag{9.1}$$

But by Lemma 9.1.4, we know that the sum on the right-hand side of Equation (9.1) is 0, so $g_a = 0$. Since $(0/p) = 0$ for all p, $(a/p) \cdot g_1 \iff 0 \cdot g_1$, when $a \equiv 0 \bmod p$. Combining these results yields $g_a = 0 = 0 \cdot g_1 = (a/p) \cdot g_1$, when $a \equiv 0 \bmod p$, which is the desired result.

Now suppose that $a \not\equiv 0 \bmod p$. Then

$$g_a = \sum_{t=0}^{p-1} (t/p)\zeta^{at} \qquad \text{(Definition of quadratic Gauss sum)}$$

$$\iff (a/p) \cdot g_a = (a/p) \cdot \sum_{t=0}^{p-1} (t/p)\zeta^{at} \qquad \text{(Multiplication Property of Equality)}$$

$$\iff (a/p) \cdot g_a = \sum_{t=0}^{p-1} (at/p)\zeta^{at} \qquad \text{(Property 2 of Legendre symbols)}$$

$$\iff (a/p) \cdot g_a = \sum_{k=0}^{p-1} (k/p)\zeta^{k}$$

(Group property; Complete system of residues)

$$\iff (a/p) \cdot g_a = g_1. \qquad \text{(Definition of } g_1\text{)}$$

Multiplying both sides of the last equation by (a/p) yields $g_a = (a/p) \cdot g_1$. ∎

Lemma 9.1.7 *If p is an odd prime, then*

$$\sum_{x=0}^{p-1} \sum_{y=0}^{p-1} \left(\frac{x}{p}\right) \left(\frac{y}{p}\right) \delta(x,y)p = (p-1)p.$$

This proof is going to be a little complicated because of the nested sums, so looking at a simple example might help to clarify things before we attempt the proof.

Example 9.1.8 Let $p = 3$ and recall that $\delta(i,j) = 1$ when $i = j$ and 0 otherwise. Also recall that $(0/p) = 0$ and $(a/p)^2 = 1$ when $p \nmid a$, by the properties of the Legendre symbol. Then expansion of the sums about x

yields

$$\begin{aligned}
&\sum_{x=0}^{2}\sum_{y=0}^{2}\left(\frac{x}{p}\right)\left(\frac{y}{p}\right)\delta(x,y)p \\
&= \left(\frac{0}{p}\right)\sum_{y=0}^{p}\left(\frac{y}{p}\right)\delta(0,y)p + \left(\frac{1}{p}\right)\sum_{y=0}^{p}\left(\frac{y}{p}\right)\delta(1,y)p + \left(\frac{2}{p}\right)\sum_{y=0}^{p}\left(\frac{y}{p}\right)\delta(x,y)p \\
&= 0 + \left(\frac{1}{p}\right)\left(\frac{1}{p}\right)\cdot 1\cdot p + \left(\frac{2}{p}\right)\left(\frac{2}{p}\right)\cdot 1\cdot p \\
&= p + p \\
&= 2p.
\end{aligned}$$

But since $p = 3$, $2p = (p-1)p$. □

Before we dive into the proof, it should be noted that for a generic prime p, as we iterate through the sums, each time $x = y$, we will get a term that looks like $(x/p)^2\,\delta(x,x)\cdot p$ in the sum, and in fact there will be exactly $p-1$ of these, since when $x = 0$, $(0/p)$ effectively "kills" the terms of the sum over y.

Proof: Suppose p is an odd prime. Then expansion of the sums yields

$$\begin{aligned}
&\sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\left(\frac{x}{p}\right)\left(\frac{y}{p}\right)\delta(x,y)p \\
&= \left(\frac{0}{p}\right)\sum_{y=0}^{p-1}\left(\frac{y}{p}\right)\delta(0,y)p + \cdots + \left(\frac{p-1}{p}\right)\sum_{y=0}^{p-1}\left(\frac{y}{p}\right)\delta(p-1,y)p \\
&= 0 + \left(\frac{1}{p}\right)^2\delta(1,1)p + \cdots + \left(\frac{p-1}{p}\right)^2\delta(p-1,p-1)p \\
&= (p-1)p,
\end{aligned}$$

which is the desired result. ∎

Theorem 9.1.9 *Suppose p is an odd prime. Then $(g_1)^2 = (-1)^{(p-1)/2}p$.*

Proof: The general idea of this proof is to examine $g_a \cdot g_{-a}$ in two different ways and then equate the results. Suppose $a \not\equiv 0 \bmod p$. Then

$$\begin{aligned} g_a \cdot g_{-a} &= (a/p) \cdot g_1 \cdot (-a/p) \cdot g_1 && \text{(Theorem 9.1.6)} \\ &= (-a^2/p)(g_1)^2 && \text{(Property 2 of Legendre Symbol)} \\ &= (-1/p)(a^2/p)(g_1)^2 && \text{(Property 2 of Legendre Symbol)} \\ &= (-1/p)(g_1)^2. && \text{(Property 4 of Legendre Symbol)} \end{aligned}$$

Summing both sides of this equation over a from 0 to $p-1$ yields

$$\begin{aligned} \sum_{a=0}^{p-1} \left(g_a \cdot g_{-a}\right) &= \sum_{a=0}^{p-1} (-1/p)(g_1)^2 && \text{(Property 4 of Legendre Symbol)} \\ &= (-1/p) \sum_{a=1}^{p-1} (g_1)^2 && \text{(Properties of sums)} \\ &= (-1/p)(p-1)(g_1)^2. \end{aligned}$$

But we could look at $g_a \cdot g_{-a}$ in another way.

$$\begin{aligned} g_a \cdot g_{-a} &= \left(\sum_{x=0}^{p-1} \left(\frac{x}{p}\right) \zeta^{ax}\right) \left(\sum_{y=0}^{p-1} \left(\frac{y}{p}\right) \zeta^{-ay}\right) && \text{(Definition 9.1.5)} \\ &= \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} \left(\frac{x}{p}\right) \left(\frac{y}{p}\right) \zeta^{ax} \zeta^{-ay} && \text{(Properties of sums)} \\ &= \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} \left(\frac{x}{p}\right) \left(\frac{y}{p}\right) \zeta^{a(x-y)} && \text{(Properties of exponents)} \end{aligned}$$

Recall from Corollary 9.1.3 that $\delta(x,y)p = \sum_{t=0}^{p-1} \zeta^{t(x-y)}$. Thus, summing

$g_a \cdot g_{-a} = \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} \left(\frac{x}{p}\right) \left(\frac{y}{p}\right) \zeta^{a(x-y)}$ over a yields

$$\begin{aligned}
\sum_{a=0}^{p-1} \left(g_a \cdot g_{-a}\right) &= \sum_{a=0}^{p-1} \left(\sum_{x=0}^{p-1} \sum_{y=0}^{p-1} \left(\frac{x}{p}\right) \left(\frac{y}{p}\right) \zeta^{a(x-y)} \right) \\
&= \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} \left(\sum_{a=0}^{p-1} \left(\frac{x}{p}\right) \left(\frac{y}{p}\right) \zeta^{a(x-y)} \right) && \text{(Properties of sums)} \\
&= \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} \left(\frac{x}{p}\right) \left(\frac{y}{p}\right) \left(\sum_{a=0}^{p-1} \zeta^{a(x-y)} \right) && \text{(Properties of sums)} \\
&= \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} \left(\frac{x}{p}\right) \left(\frac{y}{p}\right) \delta(x,y) \cdot p && \text{(Corollary 9.1.3)} \\
&= (p-1) \cdot p && \text{(Lemma 9.1.7)}
\end{aligned}$$

So now we have

$$\sum_{a=0}^{p-1} \left(g_a \cdot g_{-a}\right) = (-1/p)(p-1)(g_1)^2 \text{ and } \sum_{a=0}^{p-1} \left(g_a \cdot g_{-a}\right) = (p-1) \cdot p.$$

Combining these two results yields

$$\begin{aligned}
& (-1/p)(p-1)(g_1)^2 = (p-1) \cdot p \\
\iff & (-1/p)(g_1)^2 = p && \text{(Cancellation Law)} \\
\iff & (g_1)^2 = (-1/p) \cdot p && \text{(Multiplication property of equality)} \\
\iff & (g_1)^2 = (-1)^{(p-1)/2} \cdot p, && \text{(Law of Quadratic Reciprocity)}
\end{aligned}$$

which is the desired result. ∎

Recall that we previously described what it means to have a complete set of representatives. We now look at a specific set of integers that form a complete set of representatives.

Lemma 9.1.10 *The integers $\pm(4k-2)$, where $k = 1, 2, \ldots (p-1)/2$, are a complete set of representatives of the nonzero cosets modulo p.*

Proof: Assume that $4k-2 \equiv 4k'-2 \bmod p$. Then $4(k-k') \equiv 0 \bmod p$. By Corollary 4.3.20, this implies that $k-k' \equiv 0 \bmod p$, and $k \equiv k' \bmod p$. But $1 \leqslant k, k' \leqslant \dfrac{p-1}{2}$, so the only way they could be equivalent modulo p is if they are equal. A similar argument reveals that if $-(4k-2) \equiv -(4k'-2) \bmod p$, then $k = k'$.

Now we need to show that $4k-2 \not\equiv -(4k'-2) \bmod p$, so assume that $4k-2 \equiv -(4k'-2) \bmod p$. Then

$$
\begin{aligned}
& 4k-2 \equiv -(4k'-2) \bmod p \\
\iff & 4k-2+4k'-2 \equiv 0 \bmod p && \text{(Arithmetic)} \\
\iff & 4(k+k'-1) \equiv 0 \bmod p && \text{(Distributive Property)} \\
\implies & k+k'-1 \equiv 0 \bmod p && \text{(Corollary 4.3.20)} \\
\implies & k+k' \equiv 1 \bmod p. && \text{(Arithmetic)}
\end{aligned}
$$

But $1 \leqslant k, k' \leqslant (p-1)/2$, so $2 \leqslant k+k' \leqslant p-1$. Thus it's not possible for their sum to be 1, and it follows that $4k-2 \not\equiv -(4k'-2) \bmod p$.

So we have $p-1$ total values, and each is distinct, so they are a complete system of residues, and in fact they are a complete set of representatives of the nonzero cosets modulo p. ∎

Theorem 9.1.11 *Suppose p is an odd prime. Then*

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

Proof: Since we know that ζ is a root of the equation $x^p = 1$, we can factor $x^p - 1$ as follows.

$$\begin{aligned} x^p - 1 &= (x-1)(x^{p-1} + x^{p-2} + \cdots + x + 1) \\ &= (x-1)\big(x - \zeta^{p-1}\big)\big(x - \zeta^{p-2}\big) \ldots \big(x - \zeta^2\big)\big(x - \zeta\big) \end{aligned}$$

Thus

$$x^p - 1 = (x-1)\prod_{j=1}^{p-1} \big(x - \zeta^j\big). \tag{9.2}$$

Dividing both sides of (9.2) by $x - 1$ yields

$$x^{p-1} + x^{p-2} + \cdots + x + 1 = \prod_{j=1}^{p-1} \big(x - \zeta^j\big). \tag{9.3}$$

If we set $x = 1$ in (9.3) the result is $p = \prod_r (1 - \zeta^r)$, where the product is taken over any complete set of representatives of the nonzero cosets modulo p. Now

applying Lemma 9.1.10 yields

$$\begin{aligned} p &= \prod_{k=1}^{(p-1)/2} \left(1-\zeta^{4k-2}\right) \prod_{k=1}^{(p-1)/2} \left(1-\zeta^{-(4k-2)}\right) \\ &= \prod_{k=1}^{(p-1)/2} \left(1-\left(\zeta^{2k-1}\right)^2\right) \prod_{k=1}^{(p-1)/2} \left(1-\left(\zeta^{-(2k-1)}\right)^2\right) \end{aligned}$$

(Properties of exponents)

$$= \prod_{k=1}^{(p-1)/2} \left(\zeta^{-(2k-1)}\right)\left(1-\left(\zeta^{2k-1}\right)^2\right) \prod_{k=1}^{(p-1)/2} \left(\zeta^{2k-1}\right)\left(1-\left(\zeta^{-(2k-1)}\right)^2\right)$$

(Multiplication by $1 = \zeta^{-(2k-1)} \cdot \zeta^{2k-1}$)

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

(Distributive Property)

Now notice that

$$\left(\zeta^{-(2k-1)}-\zeta^{2k-1}\right) = -\left(\zeta^{2k-1}-\zeta^{-(2k-1)}\right),$$

so we can rewrite this last equation. Thus

$$p = (-1)^{(p-1)/2} \prod_{k=1}^{(p-1)/2} \left(\zeta^{2k-1}-\zeta^{-(2k-1)}\right)^2. \tag{9.4}$$

Multiplying both sides of Equation (9.4) by $(-1)^{(p-1)/2}$ yields

$$(-1)^{(p-1)/2}p = \prod_{k=1}^{(p-1)/2} \left(\zeta^{2k-1}-\zeta^{-(2k-1)}\right)^2,$$

which is the desired result. ∎

Theorem 9.1.12 *If p is an odd prime, then*

$$\prod_{k=1}^{(p-1)/2} \left(\zeta^{2k-1}-\zeta^{-(2k-1)}\right) = \begin{cases} \pm\sqrt{p}, & p \equiv 1 \bmod 4 \\ \pm i\sqrt{p}, & p \equiv 3 \bmod 4. \end{cases}$$

Proof: By Theorem 9.1.11, we know that

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

Suppose first that $p \equiv 1 \bmod 4$. Then $\dfrac{p-1}{2}$ is even, so

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

Suppose now that $p \equiv 3 \bmod 4$. Then $\dfrac{p-1}{2}$ is odd, so

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

Hence $\displaystyle\prod_{k=1}^{(p-1)/2} \left(\zeta^{2k-1} - \zeta^{-(2k-1)}\right) = \begin{cases} \pm\sqrt{p}, & p \equiv 1 \bmod 4 \\ \pm i\sqrt{p}, & p \equiv 3 \bmod 4. \end{cases}$ ∎

In the remainder of this section, the Gauss Sum g_1 will be denoted $g_1(\chi)$, where $\chi(t) = (t/p)$, and (t/p) is the Legendre symbol. Thus we can write

$$g_a(\chi) = \sum_{t=0}^{p-1} \chi(t)\zeta^{at}.$$

This allows us to generalize the Gauss sums to other characters.

Recall that in Theorem 9.1.9, we showed $\left(g_1(\chi)\right)^2 = (-1)^{(p-1)/2}p$. By Theorem 9.1.11, we also have $\displaystyle\prod_{k=1}^{(p-1)/2} \left(\zeta^{2k-1} - \zeta^{-(2k-1)}\right)^2 = (-1)^{(p-1)/2}p$. Combining these two results yields

$$\left(g_1(\chi)\right)^2 = \prod_{k=1}^{(p-1)/2} \left(\zeta^{2k-1} - \zeta^{-(2k-1)}\right)^2.$$

Thus $g_1(\chi) = \pm \prod_{k=1}^{(p-1)/2} \left(\zeta^{2k-1} - \zeta^{-(2k-1)}\right)$ and combining this with the result of Theorem 9.1.12, we have

$$g_1(\chi) = \begin{cases} \pm\sqrt{p}, & p \equiv 1 \bmod 4 \\ \pm i\sqrt{p}, & p \equiv 3 \bmod 4. \end{cases}$$

Proposition 9.1.13 *For p an odd prime, $g_1(\chi) = \prod_{k=1}^{(p-1)/2} \left(\zeta^{2k-1} - \zeta^{-(2k-1)}\right)$, and thus* $g_1(\chi) = \begin{cases} \sqrt{p}, & p \equiv 1 \bmod 4 \\ i\sqrt{p}, & p \equiv 3 \bmod 4. \end{cases}$

The proof of this proposition is very difficult, but it can be tackled by looking at the sin function or by using Taylor polynomials. A version of the proof can be found in [8].

In the late 1700s, Gauss wrote in his diary that he had discovered a connection between the n^{th} roots of unity and what he called the "golden theorem" (quadratic reciprocity). Two of the versions of Gauss' proofs of the law of quadratic reciprocity were based on properties of sums of roots of unity, and in fact that is where Gauss sums originated [7].

In this chapter, we work more with the multiplicative characters that we defined in Chapter 7 and develop some useful properties and theorems associated with them. We will then examine Gauss sums and make some connections between characters and the sums.

In the first half of the 1800s, both Eisenstein and Jacobi used the ring $\mathbb{Z}[\omega]$ in their studies of cubic reciprocity. Jacobi sums arose from the ties between multiplicative characters and roots of unity. We will explore Jacobi sums in great detail and develop some theorems that we will need for our work with cubic reciprocity.

9.2 Gauss Sums

Recall that we introduced multiplicative characters in Definition 7.3.1. We defined a multiplicative character χ to be a homomorphism $\chi : \mathbb{Z}_p^* \to \mathbb{C}^*$, such that $\chi(ab) = \chi(a)\chi(b)$ for all $a, b \in \mathbb{Z}_p^*$. The trivial character is ε, since $\varepsilon(a) = 1$ for all $a \in \mathbb{Z}_p^*$. If we define $\chi(0) = 0$, for $\chi \neq \varepsilon$, and $\varepsilon(0) = 0$, then we can extend the domain so that $\chi : \mathbb{Z}_p \to \mathbb{C}$. We proved in Theorem 7.3.4 that the set of characters on $\mathbb{Z}_p$ is a cyclic group of order $p-1$, under the usual function multiplication. In Theorem 7.3.2, we established three properties about multiplicative characters. For χ, a multiplicative character, and $a \in \mathbb{Z}_p^*$, $\chi(1) = 1$, $\chi(a)$ is a $(p-1)^{st}$ root of unity, and $\chi(a^{-1}) = \big(\chi(a)\big)^{-1} = \overline{\chi(a)}$.

Definition 9.2.1 Let χ be a multiplicative character on $\mathbb{Z}_p$ and let $a \in \mathbb{Z}_p$. Set

$$g_a(\chi) = \sum_{t=0}^{p-1} \chi(t)\zeta^{at},$$

where $\zeta = e^{2\pi i/p}$. Then $g_a(\chi)$ is a *Gauss sum* on $\mathbb{Z}_p$ belonging to χ. $\diamondsuit$

Theorem 9.2.2 *Let χ be a multiplicative character on $\mathbb{Z}_p$ and let $a \in \mathbb{Z}_p$. Then*

1. *If $a \neq 0$ and $\chi \neq \varepsilon$, we have $g_a(\chi) = \chi(a^{-1})g_1(\chi)$.*

2. *If $a \neq 0$ and $\chi = \varepsilon$, we have $g_a(\varepsilon) = 0$.*

3. *If $a = 0$ and $\chi \neq \varepsilon$, we have $g_0(\chi) = 0$.*

4. *If $a = 0$ and $\chi = \varepsilon$, we have $g_0(\varepsilon) = p$.*

Proof: Assume χ is a character on $\mathbb{Z}_p$ and let $a \in \mathbb{Z}_p$.

1. Suppose $a \neq 0$ and $\chi \neq \varepsilon$. Then by Definition 9.2.1,

$$\begin{aligned}
\chi(a) \cdot g_a(\chi) &= \chi(a) \sum_{t=0}^{p-1} \chi(t)\zeta^{at} && \text{(Multiply both sides by } \chi(a)\text{)} \\
&= \sum_{t=0}^{p-1} \chi(a)\chi(t)\zeta^{at} \\
&= \sum_{t=0}^{p-1} \chi(at)\zeta^{at} && \text{(Homomorphism Property)} \\
&= \sum_{k=0}^{p-1} \chi(k)\zeta^{k} && \text{(See below)} \\
&= g_1(\chi). && \text{(Definition 9.2.1)}
\end{aligned}$$

Note that in the fourth step, we can make the substitution $k = at$ because

at runs over all of the elements of $\mathbb{Z}_p$ as t does. So

$$\begin{aligned}
&\chi(a) \cdot g_a(\chi) = g_1(\chi) \\
\iff &g_a(\chi) = \big(\chi(a)\big)^{-1} \cdot g_1(\chi) && \text{(Left multiplication by } \big(\chi(a)\big)^{-1}\text{)} \\
\iff &g_a(\chi) = \chi(a^{-1}) \cdot g_1(\chi). && \text{(Theorem 7.3.2)}
\end{aligned}$$

2. Suppose $a \neq 0$ and $\chi = \varepsilon$. Then

$$\begin{aligned}
g_a(\varepsilon) &= \sum_{t=0}^{p-1} \varepsilon(t) \cdot \zeta^{at} && \text{(Definition 9.2.1)} \\
&= \sum_{t=0}^{p-1} \zeta^{at} && \text{(Definition 7.3.1)} \\
&= 0. && \text{(Theorem 9.1.1)}
\end{aligned}$$

3. Suppose $a = 0$ and $\chi \neq \varepsilon$. Then

$$\begin{aligned}
g_0(\chi) &= \sum_{t=0}^{p-1} \chi(t) \cdot \zeta^0 && \text{(Definition 9.2.1)} \\
&= \sum_{t=0}^{p-1} \chi(t) && (\zeta^0 = 1) \\
&= 0. && \text{(Theorem 7.3.3)}
\end{aligned}$$

4. Suppose $a = 0$ and $\chi = \varepsilon$. Then

$$\begin{aligned}
g_0(\varepsilon) &= \sum_{t=0}^{p-1} \varepsilon(t) \cdot \zeta^0 && \text{(Definition 9.2.1)} \\
&= \sum_{t=0}^{p-1} \varepsilon(t) && (\zeta^0 = 1) \\
&= p. && \text{(Theorem 7.3.3)}
\end{aligned}$$

So all four results hold as desired. ∎

Theorem 9.2.3 *Let χ be a character on $\mathbb{Z}_p$. If $\chi \neq \varepsilon$, then $|g_1(\chi)| = \sqrt{p}$.*

Proof: Let χ be a character on $\mathbb{Z}_p$ and let $a \in \mathbb{Z}_p$. If $a \neq 0$, then

$$g_a(\chi) = \chi(a^{-1}) \cdot g_1(\chi),$$

by Theorem 9.2.2. Also note that

$$\begin{aligned} \overline{g_a(\chi)} &= \overline{\chi(a^{-1}) \cdot g_1(\chi)} && \text{(Complex conjugate of } g_a(\chi)) \\ &= \chi(a) \cdot \overline{g_1(\chi)}. && \text{(Property 3 of Characters)} \end{aligned}$$

Multiplying $g_a(\chi)$ and $\overline{g_a(\chi)}$ together yields

$$\begin{aligned} g_a(\chi) \cdot \overline{g_a(\chi)} &= \chi(a^{-1}) \cdot g_1(\chi) \cdot \chi(a) \cdot \overline{g_1(\chi)} \\ &= \chi(a^{-1}) \cdot \chi(a) \cdot g_1(\chi)\overline{g_1(\chi)} && \text{(Commutativity in } \mathbb{C}) \\ &= \left|g_1(\chi)\right|^2. && (\chi(a^{-1}) \cdot \chi(a) = 1) \end{aligned}$$

Hence, $g_a(\chi) \cdot \overline{g_a(\chi)} = \left|g_1(\chi)\right|^2$ implies that

$$\begin{aligned} \sum_{a=0}^{p-1} g_a(\chi) \cdot \overline{g_a(\chi)} &= g_0(\chi) \cdot \overline{g_0(\chi)} + \sum_{a=1}^{p-1} g_a(\chi) \cdot \overline{g_a(\chi)} && \text{(Sum both sides over } a) \\ &= 0 + (p-1) \cdot |g_1(\chi)|^2. \end{aligned}$$

Now examine $g_a(\chi) \cdot \overline{g_a(\chi)}$ using Definition 9.2.1. We have

$$\begin{aligned} g_a(\chi) \cdot \overline{g_a(\chi)} &= \sum_{x=0}^{p-1} \chi(x)\zeta^{ax} \cdot \sum_{y=0}^{p-1} \overline{\chi(y)}\zeta^{-ay} && \text{(Definition 9.2.1)} \\ &= \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} \chi(x)\overline{\chi(y)}\zeta^{ax-ay}. && \text{(Rearrange sums)} \end{aligned}$$

Summing both sides of the last equation over a yields

$$\begin{aligned}
\sum_{a=0}^{p-1} g_a(\chi)\cdot\overline{g_a(\chi)} &= \sum_{a=0}^{p-1}\left(\sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\chi(x)\overline{\chi(y)}\zeta^{ax-ay}\right)\\
&= \sum_{a=0}^{p-1}\left(\sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\chi(x)\overline{\chi(y)}\zeta^{a(x-y)}\right) \quad \text{(Properties of exponents)}\\
&= \sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\chi(x)\overline{\chi(y)}\big(\delta(x,y)\cdot p\big) \quad \text{(Corollary 9.1.3)}
\end{aligned}$$

Now, we need to consider what is happening in this final step. If we expand the right side over y, then we have

$$p\sum_{x=0}^{p-1}\chi(x)\left(\overline{\chi(1)}\delta(x,1)+\overline{\chi(2)}\delta(x,2)+\cdots+\overline{\chi(y_{p-1})}\delta(x,y_{p-1})\right).$$

As we iterate through x, each iteration produces exactly one term that looks like $\chi(k)\overline{\chi(k)}\delta(k,k)p$, where $k\in\{1,2,\ldots,p-1\}$. We know from the properties of characters that $\overline{\chi(k)}=\big(\chi(k)\big)^{-1}$. We also know from Corollary 9.1.3 that $\delta(x,y)=1$ whenever $x\equiv y \bmod p$ and $\delta(x,y)=0$ when $x\not\equiv y \bmod p$. Thus, for each iteration of x where $x=0$, we will have $p-2$ terms equal to 0, since the $\delta(x,y)$ factor will be equal to 0. The remaining term in each iteration is then $\chi(k)\big(\chi(k)\big)^{-1}\cdot 1\cdot p$. When $x=0$, $\chi(x)=0$ as well, so it effectively "kills" the rest of the terms. We can simplify this further since $\chi(k)\big(\chi(k)\big)^{-1}=1$, thus we will have exactly $p-1$ terms from the entire sum that are equal to p. It follows that

$$\sum_{a=0}^{p-1} g_a(\chi)\cdot\overline{g_a(\chi)} = (p-1)p.$$

But we also have

$$\sum_{a=0}^{p-1} g_a(\chi) \cdot \overline{g_a(\chi)} = (p-1)\big|g_1(\chi)\big|^2.$$

Combining the two results yields

$$\begin{aligned}
&(p-1) \cdot \big|g_1(\chi)\big|^2 = (p-1) \cdot p \\
\iff &\big|g_1(\chi)\big|^2 = p \qquad\qquad \text{(Left multiplication by } (p-1)^{-1}\text{)} \\
\iff &|g_1(\chi)| = \sqrt{p},
\end{aligned}$$

as desired. ∎

9.3 Jacobi Sums

We want to extend the results we've developed about solutions to equations. If we examine $x^2 + y^2 = 1$ over the field $\mathbb{Z}_p$, we know that there can be only finitely many solutions, since for any prime p, $\mathbb{Z}_p$ is finite. Using the same notation as in the previous section, let $\mathcal{N}(x^2 + y^2 = 1)$ denote the number of solutions.

Our goal is determine explicitly what this number is, but first we need to revisit $\mathbb{Z}_p$ and look at some basic behaviors of its elements. We know that there are p elements in $\mathbb{Z}_p$, and $p-1$ of them are nonzero. Since $0^2 = 0$, we will set 0 aside for now and examine the other elements. Notice that since $p-1$ is even for any $p > 2$, if we choose $k \in \mathbb{Z}_p$ such that $1 \leqslant k \leqslant \dfrac{p-1}{2}$, then $k^2 \equiv (p-k)^2 \bmod p$, since $(p-k)^2 = p^2 - 2pk + k^2 \equiv k^2 \bmod p$. This

is important, because when we square the nonzero elements of $\mathbb{Z}_p$, each least residue either appears exactly twice or does not appear. This means that one of the ways for $x^2+y^2=1$ to have solutions is for one of x or y to be 0 and the other to be either 1 or $p-1$. Otherwise, we have $x^2+y^2=1$, where $x \neq 0 \neq y$. Let $a = x^2$ and $b = y^2$. Then we are simultaneously solving for $a = x^2$ and $b = y^2$ whenever $a + b = 1$.

Hence, we can consider $\mathcal{N}(x^2+y^2=1) = \sum_{a+b=1} \mathcal{N}(x^2=a) \cdot N(y^2=b)$. Notice that $x^2 = a$ really means that we are looking for the number of solutions to $x^2 \equiv a \bmod p$. We know that $(a/p) = 1$ if a solution exists and $(a/p) = -1$ otherwise. Furthermore, we know that if a solution exists, then there are exactly two, since $\mathbb{Z}_p$ is a field. Thus $\mathcal{N}(x^2 = a) = 1 + (a/p)$, since the sum will be 0 if there is not a solution and 2 if there is a solution. Finally, it should be clear that there are p ways to have $a+b=1$ when $a, b \in \mathbb{Z}_p$, since $0+1=1$, and the other elements pair up as follows: $2+p-1$, $3+p-2$, and so on, with the element $\dfrac{p+1}{2}$ paired with itself. This gives us $\dfrac{p+1}{2}$ of the pairs. Then switching the roles of a and b and not counting the pair $\dfrac{p-1}{2}, \dfrac{p-1}{2}$ twice gives us the other $\dfrac{p-1}{2}$ pairs.

So now we have

$$\begin{aligned}
\mathcal{N}(x^2+y^2=1) &= \sum_{a+b=1} \mathcal{N}(x^2=a)\cdot\mathcal{N}(y^2=b) && \text{(Substitution)}\\
&= \sum_{a+b=1} \big(1+(a/p)\big)\big(1+(b/p)\big) && \text{(Substitution)}\\
&= \sum_{a+b=1} \big(1+(b/p)+(a/p)+(a/p)(b/p)\big) && \text{(Distributive Property)}\\
&= p+\sum_{a=0}^{p-1}(a/p)+\sum_{b=0}^{p-1}(b/p)+\sum_{a+b=1}(a/p)(b/p). && \text{(Split the sum)}
\end{aligned}$$

Now recall that there are as many quadratic residues as nonresidues and $(0/p)=0$. Thus $\sum_{a=0}^{p-1}(a/p)=0$, and likewise $\sum_{b=0}^{p-1}(b/p)=0$.

So our problem is now reduced to $\mathcal{N}(x^2+y^2=1)=p+\sum_{a+b=1}(a/p)(b/p)$. We will return to this problem shortly to calculate the actual value.

Definition 9.3.1 Let χ and λ be characters of $\mathbb{Z}_p$ and let $a,b\in\mathbb{Z}_p$. Then

$$J(\chi,\lambda)=\sum_{a+b=1}\chi(a)\lambda(b)$$

is called a *Jacobi sum*. ♢

Lemma 9.3.2 Let $a,b\in\mathbb{Z}_p$. Then $\sum_{a+b=1} 1=p$, where the sum is over all pairs a and b such that $a+b\equiv 1 \bmod p$.

Proof: This follows immediately from the discussion preceding Definition 9.3.1. ∎

Theorem 9.3.3 *Let χ and λ be nontrivial characters. Then*

1. $J(\varepsilon, \varepsilon) = p$.

2. $J(\varepsilon, \chi) = 0$.

3. $J(\chi, \chi^{-1}) = -\chi(-1)$.

4. *If $\chi\lambda \neq \varepsilon$, then* $J(\chi, \lambda) = \dfrac{g(\chi)g(\lambda)}{g(\chi\lambda)}$.

Proof: Let χ and λ be nontrivial characters and let $a, b \in \mathbb{Z}_p$.

1. We have

$$\begin{aligned} J(\varepsilon, \varepsilon) &= \sum_{a+b=1} \varepsilon(a) \cdot \varepsilon(b) && \text{(Definition 9.3.1)} \\ &= \sum_{a+b=1} 1 && \text{(Definition 7.3.1)} \\ &= p, && \text{(Lemma 9.3.2)} \end{aligned}$$

which is the desired result.

2. By Definition 9.3.1, we have

$$\begin{aligned} J(\varepsilon, \chi) &= \sum_{a+b=1} \varepsilon(a) \cdot \chi(b) \\ &= \sum_{b=0}^{p-1} \chi(b) && \text{(Definition 7.3.1)} \\ &= 0. && \text{(Theorem 7.3.3)} \end{aligned}$$

In the second step, note that we changed from the sum being over all pairs of a, b such that $a + b = 1$, to the sum over all $b \in \mathbb{Z}_p$. This follows

from Lemma 9.3.2, because each value of b appears in a unique pair and $\varepsilon(a) = 1$ for all a.

3. By Definition 9.3.1, we have

$$\begin{aligned} J(\chi, \chi^{-1}) &= \sum_{\substack{a+b=1 \\ b\neq 0}} \chi(a) \cdot \big(\chi(b)\big)^{-1} \\ &= \sum_{\substack{a+b=1 \\ b\neq 0}} \chi(a) \cdot \chi(b^{-1}) && \text{(Theorem 7.3.2)} \\ &= \sum_{\substack{a+b=1 \\ b\neq 0}} \chi(ab^{-1}) && \text{(Multiplicative character)} \\ &= \sum_{a\neq 1} \chi\big(a(1-a)^{-1}\big) && (b = 1-a) \end{aligned}$$

Note that in the second and third steps, we restrict the bounds of the sum to exclude $b = 0$ as an option. Similarly, in the fourth step, we have made the substitution $b = 1 - a$, and since $b \neq 0$, this forces $a \neq 1$.

Now set $c = a(1-a)^{-1}$. We know $c \neq -1$, since $c = -1$ would result in

$$\begin{aligned} & -1 = a(1-a)^{-1} \\ \iff & -(1-a) = a && \text{(Right multiplication by } (1-a)\text{)} \\ \iff & -1 + a = a && \text{(Distributive Property)} \\ \iff & -1 = 0. && \text{(Subtraction Property of Equality)} \end{aligned}$$

Thus for $c \neq -1$,

$$\begin{aligned}
& c = a(1-a)^{-1} \\
\iff & c(1-a) = a && \text{(Right multiplication by } (1-a)\text{)} \\
\iff & c - ca = a && \text{(Distributive Property)} \\
\iff & c = a + ca && \text{(Addition Property of Equality)} \\
\iff & c = a(1+c) && \text{(Distributive Property)} \\
\iff & c(1+c)^{-1} = a. && \text{(Right multiplication by } (1+c)^{-1}\text{)}
\end{aligned}$$

So $J(\chi, \chi^{-1}) = \sum_{a \neq 1} \chi\big(a(1-a)^{-1}\big)$ is now $J(\chi, \chi^{-1}) = \sum_{c \neq -1} \chi(c)$, and as a varies over $\mathbb{Z}_p \backslash \{1\}$, c varies over $\mathbb{Z}_p \backslash \{-1\}$. Thus we have

$$\begin{aligned}
\sum_{c \neq -1} \chi(c) + \chi(-1) &= \sum_{c=0}^{p-1} \chi(c) \\
&= 0, && \text{(Part 2 above)}
\end{aligned}$$

which tells us that

$$\sum_{c \neq -1} \chi(c) + \chi(-1) = 0 \iff \sum_{c \neq -1} \chi(c) = -\chi(-1).$$

Putting everything together yields

$$J(\chi, \chi^{-1}) = -\chi(-1).$$

4. First we want to examine the product $g_1(\chi)g_1(\lambda)$ from Definition 9.2.1.

$$\begin{aligned}
g_1(\chi)g_1(\lambda) &= \left(\sum_{x=0}^{p-1}\chi(x)\zeta^x\right)\left(\sum_{y=0}^{p-1}\lambda(y)\zeta^y\right) && \text{(Definition 9.2.1)}\\
&= \sum_{x,y=0}^{p-1}\chi(x)\lambda(y)\zeta^{x+y} && \text{(Rearrange sum)}\\
&= \sum_{t=0}^{p-1}\left(\sum_{x+y=t}\chi(x)\lambda(y)\right)\zeta^t && \text{(Rearrange sum)}
\end{aligned}$$

In the last step, we rearrange the sum by setting $t = x + y$ and factoring.

Now if $t = 0$,

$$\begin{aligned}
\sum_{x+y=0}\chi(x)\lambda(y) &= \sum_{x=0}^{p-1}\chi(x)\lambda(-x) && (y=-x)\\
&= \sum_{x=0}^{p-1}\chi(x)\lambda(-1\cdot x) && (-x=-1\cdot x)\\
&= \sum_{x=0}^{p-1}\chi(x)\lambda(-1)\lambda(x) && \text{(Multiplicative character)}\\
&= \lambda(-1)\sum_{x=0}^{p-1}\chi(x)\lambda(x) && \text{(Rearrange sum)}\\
&= \lambda(-1)\sum_{x=0}^{p-1}\chi\lambda(x) && \text{(Function multiplication)}\\
&= 0, && \text{(Part 2 above)}
\end{aligned}$$

since the group of characters is closed under function multiplication, and by our initial assumption $\chi\lambda \neq \varepsilon$.

Since $x, y \in \mathbb{Z}_p$, if $t \neq 0$, then there exist u and v such that $x = tu$ and

$y = tv$. Then

$$\begin{aligned} & x + y = t \\ \iff & tu + tv = t && \text{(Substitution)} \\ \iff & u + v = 1. && \text{(Left multiplication by } t^{-1}\text{)} \end{aligned}$$

So

$$\begin{aligned} \sum_{x+y=t} \chi(x)\lambda(y) &= \sum_{u+v=1} \chi(tu)\lambda(tv) && \text{(Substitution)} \\ &= \sum_{u+v=1} \chi\lambda(t) \cdot \chi(u)\lambda(v) && \text{(Multiplicative characters)} \\ &= \chi\lambda(t) \cdot J(\chi, \lambda). && \text{(Definition 9.3.1)} \end{aligned}$$

Combining results yields

$$\begin{aligned} g_1(\chi)g_1(\lambda) &= \sum_{t=0}^{p-1} \left(\sum_{x+y=t} \chi(x)\lambda(y) \right) \zeta^t \\ &= \sum_{t=0}^{p-1} \big(\chi\lambda(t) \cdot J(\chi, \lambda)\big)\zeta^t && \text{(Substitution)} \\ &= J(\chi, \lambda) \cdot g_1(\chi\lambda), && \text{(Definition of } g_1(\chi\lambda)\text{)} \end{aligned}$$

which implies that $J(\chi, \lambda) = \dfrac{g_1(\chi)g_1(\lambda)}{g_1(\chi\lambda)}$ as desired.

Therefore, all four properties hold, as claimed. ∎

We are now in a position to finish the work we started at the beginning of this section. We left off with $\mathcal{N}(x^2 + y^2 = 1) = p + \sum_{a+b=1} (a/p)(b/p)$. Recall that earlier we were working with the character $\chi(t) = (t/p)$. Thus our problem

has now become $\mathcal{N}(x^2+y^2=1) = p + \sum_{a+b=1} \chi(a)\cdot\chi(b)$. But $a+b=1$ implies that $b = 1-a$. Since $\mathbb{Z}_p$ is an additive group, this means that $b = 1-a$ is the additive inverse of a, so by Property 3 of Theorem 9.3.3, this can be rewritten as

$$\mathcal{N}(x^2+y^2=1) = p + \sum_{a=0}^{p-1} \chi(a)\cdot\chi^{-1}(a) = p + J(\chi,\chi^{-1}) = p - \chi(-1).$$

Recall that earlier we said that $\chi(t)$ would represent the Legendre symbol (t/p). Thus $\chi(-1) = (-1/p)$, so $-\chi(-1) = -(-1/p)$. But we know that for odd primes p, either $p \equiv 1 \bmod 4$ or $p \equiv 3 \bmod 4$, so

$$\mathcal{N}(x^2+y^2=1) = \begin{cases} p+1, & p \equiv 1 \bmod 4 \\ \\ p-1, & p \equiv 3 \bmod 4. \end{cases}$$

Corollary 9.3.4 *Let χ and λ be nontrivial characters. If $\chi\lambda \neq \varepsilon$, then $|J(\chi,\lambda)| = \sqrt{p}$.*

Proof: Assume that χ and λ are nontrivial characters with $\chi\lambda \neq \varepsilon$. Then from Theorem 9.3.3, we have

$$J(\chi,\lambda) = \frac{g_1(\chi)g_1(\lambda)}{g_1(\chi\lambda)}.$$

Working with this equation yields

$$\begin{aligned}
|J(\chi,\lambda)| &= \left|\frac{g_1(\chi)g_1(\lambda)}{g_1(\chi\lambda)}\right| && \text{(Take absolute value of both sides)}\\
&= \frac{|g_1(\chi)|\cdot|g_1(\lambda)|}{|g_1(\chi\lambda)|} && \text{(Properties of absolute value)}\\
&= \frac{\sqrt{p}\sqrt{p}}{\sqrt{p}} && \text{(Theorem 9.2.3)}\\
&= \sqrt{p},
\end{aligned}$$

as desired. ∎

Recall that in Example 5.3.5, for $\alpha = a + bi \in \mathbb{Z}[i]$, the norm is given by $N(\alpha) = a^2 + b^2$. Similarly, by Definition 5.4.1, for $\beta \in \mathbb{Z}[\omega]$, the norm is $N(\beta) = a^2 - ab + b^2$.

Theorem 9.3.5 *If $p \equiv 1 \bmod 4$, then there exist integers a and b such that*

$$a^2 + b^2 = p.$$

If $p \equiv 1 \bmod 3$, then there exist integers a and b such that

$$a^2 - ab + b^2 = p.$$

Proof: Suppose $p \equiv 1 \bmod 4$. Then $p = 4k + 1$ for some $k \in \mathbb{Z}$. By Theorem 7.3.2, for $a \in \mathbb{Z}_p^*$, $\chi(a)$ is a $(p-1)^{st}$ root of unity, so $\big(\chi(a)\big)^{p-1} = 1$. Recall that the characters form a cyclic group, thus there is some character λ that generates the group, so $\lambda^{p-1} = 1$. Set $\chi = \lambda^{(p-1)/4}$, and note that χ is order 4.

Since χ has order 4, each $\chi(a)$ is a root of $x^4 = 1$, thus $\chi(a)$ takes on the values 1, -1, i, and $-i$. This means that $J(\chi, \chi) = \sum_{s+t=1} \chi(s)\chi(t)$ is a Gaussian integer. In other words, $J(\chi, \chi) = a + bi \in \mathbb{Z}[i]$. So

$$J(\chi, \chi) = a + bi \Rightarrow |J(\chi, \chi)| = |a + bi|,$$

but we know from Corollary 9.3.4 that since χ is nontrivial, $|J(\chi, \chi)| = \sqrt{p}$. Thus

$$|a + bi| = |J(\chi, \chi)| = \sqrt{p}.$$

Recall from complex analysis that $|a + bi| = \sqrt{a^2 + b^2}$ by definition. Thus, since $|a + bi| = \sqrt{p}$, it follows that $|a^2 + b^2| = p$.

Now suppose $p \equiv 1 \bmod 3$. Then by a similar argument as that used in the first part of this proof, there is some character χ that has order 3. Each $\chi(a)$ is a root of $x^3 = 1$, so $\chi(a)$ takes on the values 1, ω, and ω^2, where $\omega = e^{2\pi i/3} = \dfrac{-1 + \sqrt{-3}}{2}$. Thus, $J(\chi, \chi) = \sum_{u+v=1} \chi(u)\chi(v)$ is an Eisenstein integer, which means that $J(\chi, \chi) = a + b\omega \in \mathbb{Z}[\omega]$. So

$$J(\chi, \chi) = a + b\omega \Rightarrow |J(\chi, \chi)| = |a + b\omega|.$$

But by Corollary 9.3.4, $|J(\chi, \chi)| = \sqrt{p}$. Combining these results yields

$$\begin{aligned} & |a + b\omega| = |J(\chi, \chi)| = \sqrt{p} \\ \iff & N(a + b\omega) = |J(\chi, \chi)|^2 = \left(\sqrt{p}\right)^2 \\ \iff & a^2 - ab + b^2 = p, \end{aligned}$$

which is the desired result. ∎

Theorem 9.3.6 *If $p \equiv 1 \bmod 3$, then there are integers A and B such that*

$$4p = A^2 + 27B^2,$$

where A and B are uniquely determined up to sign.

Proof: Assume $p \equiv 1 \bmod 3$. Then $p = a^2 - ab + b^2$ by Theorem 9.3.5. Even if we restrict a and b to the positive integers, this representation of p is not unique, since

$$a^2 - a(a-b) + (a-b)^2 = a^2 - ab + b^2 = (b-a)^2 - (b-a)b + b^2.$$

But if $p = a^2 - ab + b^2$, then

$$\begin{aligned}
4p &= 4a^2 - 4ab + 4b^2 && \text{(Multiplication Property of Equality)} \\
&= 4a^2 - 4ab + b^2 + 3b^2 && (4b^2 = b^2 + 3b^2) \\
&= (2a-b)^2 + 3b^2 && \text{(Factor)} \\
&= (2b-a)^2 + 3a^2 \\
&= (a+b)^2 + 3(a-b)^2.
\end{aligned}$$

We claim that either $3 \mid a$, $3 \mid b$, or $3 \mid (a-b)$.

First recall that $p = a^2 - ab + b^2$, which implies $1 \equiv a^2 - ab + b^2 \bmod 3$, since $p \equiv 1 \bmod 3$. If $3 \mid a$, then $a \equiv 0 \bmod p$, so $1 \equiv b^2 \bmod 3$, which yields $b \equiv \pm 1 \bmod 3$. Likewise, if $3 \mid b$, then $a \equiv \pm 1 \bmod 3$. If $a \neq 0 \bmod 3$ and $b \neq 0 \bmod 3$, then $a^2 \equiv b^2 \equiv 1 \bmod 3$, so $1 \equiv 1 - ab + 1 \bmod 3$, so $ab \equiv 1 \bmod 3$.

But this implies that either $a \equiv b \equiv 1 \bmod 3$ or $a \equiv b \equiv -1 \bmod 3$, and either way, we have $a - b \equiv 0 \bmod 3$, so $3 \mid (a - b)$.

So either $3 \mid a$, $3 \mid b$, or $3 \mid (a - b)$. Recall that we also showed that

$$4p = (2a - b)^2 + 3b^2 = (2b - a)^2 + 3a^2 = (a + b)^2 + 3(a - b)^2.$$

If $3 \mid a$, then $a = 3k$ for some k, and $4p = (2b-a)^2+3a^2 = \big(2b-(3k)\big)^2+3(3k)^2$, which is of the form $4p = A^2 + 27B^2$, for some A and B. Similarly, if $3 \mid b$, then $4p = (2a-b)^2+3b^2 = \big(2a-(3j)\big)^2+3(3j)^2$, for some j. Finally, $3 \mid (a-b)$ implies that $4p = (a + b)^2 + 3(3l)^2$. When we put these results together, it follows that there exist $A, B \in \mathbb{Z}$, such that $4p = A^2 + 27B^2$.

By [8], A and B are unique up to sign. ∎

Lemma 9.3.7 *If χ is a character, then $\overline{g_1(\chi)} = \chi(-1) \cdot g_1(\overline{\chi})$.*

Proof: Let χ be a character. Then

$$\begin{aligned}
\overline{g_1(\chi)} &= \overline{\sum_{t=0}^{p-1} \chi(t)\zeta^t} && \text{(Definition of } g_1(\chi)) \\
&= \sum_{t=0}^{p-1} \overline{\chi}(t)\zeta^{-t} \\
&= \sum_{t=0}^{p-1} \overline{\chi}(-t)\zeta^{t} \\
&= \sum_{t=0}^{p-1} \overline{\chi}(-1)\overline{\chi}(t)\zeta^{t} \\
&= \overline{\chi}(-1) \sum_{t=0}^{p-1} \overline{\chi}(t)\zeta^{t} \\
&= \overline{\chi}(-1) g_1(\overline{\chi}) && (\overline{\chi}(-1) = \chi\big(-1)^{-1}\big) = \chi(-1)) \\
&= \chi(-1) g_1(\overline{\chi}),
\end{aligned}$$

so $\overline{g_1(\chi)} = \chi(-1)g_1(\overline{\chi})$. ∎

Theorem 9.3.8 *Suppose that $p \equiv 1 \bmod n$ and assume that χ is a character of order $n > 2$. Then*

$$\big(g(\chi)\big)^n = \chi(-1)pJ(\chi,\chi)J(\chi,\chi^2)\dots J(\chi,\chi^{n-2}).$$

Proof: Assume $p \equiv 1 \bmod n$ and let χ be a character of order $n > 2$. Then we can apply part 4 of Theorem 9.3.3, which gives us

$$\begin{aligned}
J(\chi,\chi) &= \frac{g_1(\chi)g_1(\chi)}{g_1(\chi\chi)} \\
&= \frac{\big(g_1(\chi)\big)^2}{g_1(\chi^2)},
\end{aligned}$$

so $\big(g_1(\chi)\big)^2 = g_1(\chi^2)J(\chi.\chi)$. Multiplying both sides of this equation by $g_1(\chi)$ yields

$$\big(g_1(\chi)\big)^3 = g_1(\chi)g_1(\chi^2)J(\chi,\chi).$$

Now,

$$J(\chi,\chi^2) = \frac{g_1(\chi)g_1(\chi^2)}{g_1(\chi\chi^2)} \qquad \text{(Theorem 9.3.3)}$$

$$\iff g_1(\chi^3)J(\chi,\chi^2) = g_1(\chi)g_1(\chi^2).$$

By substitution, we have

$$\big(g_1(\chi)\big)^3 = g_1(\chi^3)J(\chi,\chi^2)J(\chi,\chi).$$

Again multiplying both sides of the equation by $g_1(\chi)$ yields

$$\big(g_1(\chi)\big)^4 = g_1(\chi)g_1(\chi^3)J(\chi,\chi^2)J(\chi,\chi).$$

But

$$J(\chi,\chi^3) = \frac{g_1(\chi)g_1(\chi^3)}{g_1(\chi,\chi^3)} \qquad \text{(Theorem 9.3.3)}$$

$$\iff g_1(\chi^4)J(\chi,\chi^3) = g_1(\chi)g_1(\chi^3).$$

So if we substitute again, we have

$$\big(g_1(\chi)\big)^4 = g_1(\chi^4)J(\chi,\chi^3)J(\chi,\chi^2)J(\chi,\chi).$$

If we continue in this manner, we will eventually have

$$\big(g_1(\chi)\big)^{n-1} = g\big(\chi^{n-1}\big)J\big(\chi,\chi^{n-2}\big)J\big(\chi,\chi^{n-3}\big)\ldots J\big(\chi,\chi^2\big)J(\chi,\chi). \qquad (9.5)$$

Recall that χ has order n, so $\chi^{n-1} = \chi^{-1}$, but $\chi^{-1} = \overline{\chi}$, by Property 3 of multiplicative characters. Thus

$$\begin{aligned} g_1(\chi)g_1(\chi^{n-1}) &= g_1(\chi)g_1(\chi^{-1}) && (\chi^{n-1} = \chi^{-1}) \\ &= g_1(\chi)g_1(\overline{\chi}) && (\chi^{-1} = \overline{\chi}) \\ &= g_1(\chi)\overline{g_1(\chi)}\chi(-1) && \text{(Lemma 9.3.7)} \\ &= \left|g_1(\chi)\right|^2\chi(-1) && \text{(Theorem 9.2.3)} \\ &= p\chi(-1). && \text{(Theorem 9.2.3)} \end{aligned}$$

So, if we multiply both sides of Equation (9.5) by $g_1(\chi)$, we have

$$\begin{aligned} \big(g_1(\chi)\big)^n &= g_1(\chi)g_1(\overline{\chi})J(\chi,\chi^{n-2})J(\chi,\chi^{n-3})\ldots J(\chi,\chi^2)J(\chi,\chi) \\ &= p\chi(-1)J(\chi,\chi^{n-2})J(\chi,\chi^{n-3})\ldots J(\chi,\chi^2)J(\chi,\chi), \end{aligned}$$

which is the desired result. ∎

Corollary 9.3.9 *If χ is a cubic character, then*

$$\big(g_1(\chi)\big)^3 = pJ(\chi,\chi).$$

Proof: By Theorem 9.3.8,

$$\big(g_1(\chi)\big)^3 = p\chi(-1)J(\chi,\chi).$$

But since χ is a cubic character, $\big(\chi(-1)\big)^3 = 1$. However, by the definition of function multiplication, $\big(\chi(-1)\big)^3 = \big(\chi(-1)^3\big) = \chi(-1)$, and it follows that $\chi(-1) = 1$. Thus, we have $\big(g(\chi)\big)^3 = pJ(\chi,\chi)$, as desired. ∎

We want to see if we can determine the number of solutions to the equation $x^3 + y^3 = 1$ over the field $\mathbb{Z}_p$. As before, we will denote the number of solutions as $\mathcal{N}(x^3 + y^3 = 1)$. We begin the same way we did with the quadratic version, so

$$\mathcal{N}(x^3 + y^3 = 1) = \sum_{a+b=1} \mathcal{N}(x^3 = a)\mathcal{N}(y^3 = b).$$

Suppose $x^3 = 0$. The only solution to this equation in $\mathbb{Z}_p$ is $x = 0$.

Suppose now that $p \equiv 2 \bmod 3$. Recall that $\mathbb{Z}_p^*$ is cyclic, so there is some g that generates it. Since $p \equiv 2 \bmod 3$, $\gcd(3, p-1) = 1$, so g^3 is also a generator of $\mathbb{Z}_p^*$, by Theorem 4.3.21. Thus there exists some $0 \leqslant k < p$ such that $a = \left(g^3\right)^k$. But we can rewrite this as $a = \left(g^k\right)^3$, so $x^3 = a$ has at least one solution, and it is in fact $x \equiv g^k \bmod p$. If another solution exists, then it is of the form $x \equiv g^l \bmod p$ for some $0 \leqslant l < p$, where $\left(g^l\right)^3 = a$. But then we have $g^{3k} = a = g^{3l}$, which implies that $3k \equiv 3l \bmod p$. But $\gcd(3, p-1) = 1$, so $k \equiv l \bmod p$, and since $0 \leqslant k, l < p$, it follows that $k = l$. Thus there is exactly one solution to the equation $x^3 = a$ for each a, so $\mathcal{N}(x^3 = a) = 1$ for all a. This implies that $\mathcal{N}(x^3 + y^3 = 1) = \sum_{a+b=1} 1 = p$, by Lemma 9.3.2.

Suppose instead that $p \equiv 1 \bmod 3$. By Theorem 7.3.4, we know that the set of characters on $\mathbb{Z}_p$ forms a cyclic group of order $p-1$. Since $p \equiv 1 \bmod 3$, we can see that $3 \mid (p-1)$. Let λ be a generator of the cyclic group of characters on $\mathbb{Z}_p$. Then $\chi = \lambda^{(p-1)/3}$ is a character of order 3, and the characters χ, χ^2,

and $\chi^3 = \varepsilon$ are all distinct cubic characters. By Theorem 7.3.7,

$$\mathcal{N}(x^3 = a) = \varepsilon(a) + \chi(a) + \big(\chi(a)\big)^2,$$

so

$$\begin{aligned}
\mathcal{N}(x^3 + y^3 = 1) &= \sum_{a+b=1} \mathcal{N}(x^3 = a)\mathcal{N}(y^3 = b) \\
&= \sum_{a+b=1} \sum_{i=0}^{2} \big(\chi(a)\big)^i \sum_{j=0}^{2} \big(\chi(b)\big)^j \\
&= \sum_{i=0}^{2} \sum_{j=0}^{2} \left(\sum_{a+b=1} \big(\chi(a)\big)^i \big(\chi(b)\big)^j \right).
\end{aligned}$$

As we did in the quadratic case, we will return to calculate this value shortly.

Recall that in Section 5.5, we defined algebraic integers to be complex numbers that are roots of a polynomial $x^n + b_1 x^{n-1} + \cdots + b_n = 0$, where each b_i is an integer. We also stated that the algebraic integers form a ring, which is denoted Ω. Finally, we proved Theorem 5.5.3 and looked at an example of the theorem at work. The theorem states that given $\omega_1, \omega_2 \in \Omega$ and some prime $p \in \mathbb{Z}$, then $\big(\omega_1 + \omega_2\big)^p \equiv \omega_1^p + \omega_2^p \bmod p$. Example 5.5.4 illustrated that we can take algebraic integers, which are not ordinary integers, and add them together modulo p, where p is an integer. This idea is going to come into play in the proof of this next theorem.

Theorem 9.3.10 *Suppose that $p \equiv 1 \bmod 3$ and assume that χ is a nontrivial cubic character. Set $J(\chi, \chi) = a + b\omega$. Then*

1. $b \equiv 0 \bmod 3$.

2. $a \equiv 2 \bmod 3$.

Proof:

$$\begin{aligned}
\big(g_1(\chi)\big)^3 &= \left(\sum_{t=0}^{p-1} \chi(t)\zeta^t\right)^3 && \text{(Definition of } g_1(\chi)\text{)} \\
&\equiv \sum_{t=0}^{p-1} \big(\chi(t)\big)^3\zeta^{3t} \bmod 3 && \text{(Theorem 5.5.3)} \\
&\equiv 0^3 + \sum_{t=1}^{p-1} \big(\chi(t)\big)^3\zeta^{3t} \bmod 3 && (\chi(0) = 0) \\
&\equiv \sum_{t=1}^{p-1} \zeta^{3t} \bmod 3 && (\chi \text{ is a cubic character}) \\
&\equiv \zeta^1 + \zeta^2 + \zeta^3 + \cdots + \zeta^{p-1}, &&
\end{aligned}$$

since ζ is a p^{th} root of unity and $3 \nmid p$, so $3t$ runs through $\{1, 2, \ldots, p-1\}$ as t does. But recall that ζ is a root of the polynomial $x^p - 1$. More specifically, ζ is a root of $x^{p-1} + \cdots + x + 1$, which is one of the factors of $x^p - 1$. Thus $\zeta^{p-1} + \cdots + \zeta^1 + 1 = 0$, which implies that $\zeta^{p-1} + \cdots + \zeta^1 = -1$. Hence

$$\big(g_1(\chi)\big)^3 \equiv 2 \bmod 3,$$

so

$$\begin{aligned}
2 &\equiv \big(g_1(\chi)\big)^3 \bmod 3 \\
&\equiv pJ(\chi,\chi) \bmod 3 && \text{(Corollary 9.3.9)} \\
&\equiv J(\chi,\chi) \bmod 3 && (p \equiv 1 \bmod 3) \\
&\equiv a + b\omega \bmod 3. &&
\end{aligned}$$

Thus $a + b\omega \equiv 2 \bmod 3$.

Now we want to repeat this idea for $\overline{\chi}$. We proved in Lemma 9.3.7 that $\overline{g_1(\chi)} = \chi(-1) \cdot g_1(\overline{\chi})$, but χ is a cubic character, so $\chi(-1) = 1$. Thus $\overline{g_1(\chi)} = g_1(\overline{\chi})$,. Note also that

$$\begin{aligned}
\overline{J(\chi,\chi)} &= \overline{\sum_{a+b=1} \chi(a)\chi(b)} && \text{(Definition of Jacobi sum)} \\
&= \sum_{a+b=1} \overline{\chi(a)\chi(b)} \\
&= \sum_{a+b=1} \overline{\chi(a)} \cdot \overline{\chi(b)} && \text{(Properties of complex conjugates)} \\
&= J(\overline{\chi},\overline{\chi}).
\end{aligned}$$

Thus

$$\begin{aligned}
\big(g_1(\overline{\chi})\big)^3 &= pJ(\overline{\chi},\overline{\chi}) && \text{(Corollary 9.3.9)} \\
&\equiv a + b\overline{\omega} \bmod 3 \\
&\equiv 2 \bmod 3.
\end{aligned}$$

Subtracting the results yields

$$\begin{aligned}
& a + b\omega - (a + b\overline{\omega}) \equiv 2 - 2 \bmod 3 \\
\iff & b(\omega - \overline{\omega}) \equiv 0 \bmod 3 \\
\iff & b\sqrt{-3} \equiv 0 \bmod 3.
\end{aligned}$$

But this implies that $-3b^2 \equiv 0 \bmod 9$, which in turn implies that $3 \mid b$. Thus $b \equiv 0 \bmod 3$ and since $a + b\omega \equiv 2 \bmod 3$, it follows that $a \equiv 2 \bmod 3$, as desired. ∎

Corollary 9.3.11 *Let* $A = 2a - b$ *and* $B = b/3$. *Then* $A \equiv 1 \bmod 3$ *and* $4p = A^2 + 27B^2$.

Proof: We know from Theorem 9.3.5 that $J(\chi, \chi) = a + b\omega$. We also have $\left|J(\chi, \chi)\right|^2 = p$, by Corollary 9.3.4. Combining these results yields

$$\begin{aligned} & p = a^2 - ab + b^2 \\ \iff & 4p = (2a - b)^2 + 3b^2 && \text{(Theorem 9.3.6)} \\ \iff & 4p = A^2 + 3(3B)^2 && \text{(Substitution)} \\ \iff & 4p = A^2 + 27B^2. \end{aligned}$$

Now, Theorem 9.3.10 indicates that $a \equiv -1 \bmod 3$ and $b \equiv 0 \bmod 3$, so

$$\begin{aligned} A &= 2a - b \\ &\equiv -2 \bmod 3 && \text{(Substitution)} \\ &\equiv 1 \bmod 3. \end{aligned}$$

Thus $4p = A^2 + 27B^2$ and $A \equiv 1 \bmod 3$. ∎

We are now in a position to return to our discussion about the number of solutions to the equation $x^3 + y^3 = 1$. Recall that we left off with

$$\mathcal{N}(x^3 + y^3 = 1) = \sum_{i=0}^{2} \sum_{j=0}^{2} \left(\sum_{a+b=1} \big(\chi(a)\big)^i \big(\chi(b)\big)^j \right).$$

From previous work, we know that ε is the identity character, so $\chi^0 = \varepsilon$.

Recall that we previously defined a Jacobi sum to be

$$J(\chi, \lambda) = \sum_{a+b=1} \chi(a)\lambda(b).$$

Thus it's easy to see that we are going to be adding together a bunch of Jacobi sums. In Theorem 9.3.3, we established some properties about Jacobi sums that we will need to use in evaluating our work. We proved that if χ and λ are nontrivial characters, then

- $J(\varepsilon, \varepsilon) = p$
- $J(\varepsilon, \chi) = 0$
- $J(\chi, \chi^{-1}) = -\chi(-1)$.

So if we expand the right side of the equation about i and j, we have

$$\begin{aligned}
\mathcal{N}(x^3 + y^3 = 1) = &\sum_{a+b=1} \varepsilon(a)\varepsilon(b) + \sum_{a+b=1} \varepsilon(a)\chi(b) + \sum_{a+b=1} \varepsilon(a)\chi(b) \\
&+ \sum_{a+b=1} \chi(a)\varepsilon(b) + \sum_{a+b=1} \chi(a)\chi(b) + \sum_{a+b=1} \chi(a)\chi^{-1}(b) \\
&+ \sum_{a+b=1} \chi^{-1}(a)\varepsilon(b) + \sum_{a+b=1} \chi^{-1}(a)\chi(b) + \sum_{a+b=1} \chi^{-1}(a)\chi^{-1}(b) \\
&= p + 0 + 0 + 0 + J(\chi, \chi) - \chi(-1) + 0 - \chi^2(-1) + J(\chi^{-1}, \chi^{-1}) \\
&= p + J(\chi, \chi) - 1 - 1 + J(\chi^2, \chi^2) \\
&= p - 2 + J(\chi, \chi) + J(\chi^2, \chi^2).
\end{aligned}$$

To justify the work between the second and third steps above, recall that χ is a cubic character and $(-1)^3 = -1$. Thus $\chi(-1) = 1$, which implies that $-\chi(-1) = -1$.

Now we set that result aside for a moment and examine $J(\chi^2, \chi^2)$.

$$\begin{aligned} J(\chi^2, \chi^2) &= \sum_{a+b=1} \chi^{-1}(a)\chi^{-1}(b) \\ &= \sum_{a+b=1} \overline{\chi(a)} \cdot \overline{\chi(b)} \\ &= \sum_{a+b=1} \overline{\chi(a)\chi(b)} \\ &= \overline{\sum_{a+b=1} \chi(a)\chi(b)} \\ &= \overline{J(\chi, \chi)} \end{aligned}$$

But we know that $J(\chi, \chi)$ is a complex number, and we know that the sum of complex conjugates is just twice the real part of the complex number, so we can return to our work from above.

$$\begin{aligned} \mathcal{N}(x^3 + y^3 = 1) &= p - 2 + J(\chi, \chi) + J(\chi^2, \chi^2) \\ &= p - 2 + J(\chi, \chi) + \overline{J(\chi, \chi)} \\ &= p - 2 + 2 \cdot \mathrm{Re}\big(J(\chi, \chi)\big). \end{aligned}$$

Finally, in Theorem 9.3.10, we proved that $J(\chi, \chi) = a + b\omega$, where $a + b\omega$ is primary. So

$$\begin{aligned} a + b\omega &= a + b\left(\frac{-1 + \sqrt{-3}}{2}\right) \\ &= a - \frac{b}{2} - \frac{b\sqrt{-3}}{2}, \end{aligned}$$

so $\mathrm{Re}\big(J(\chi, \chi)\big) = \dfrac{2a - b}{2}$ and $2 \cdot \mathrm{Re}\big(J(\chi, \chi)\big) = 2a - b$. It follows that

$$\mathcal{N}(x^3 + y^3 = 1) = p - 2 + (2a - b).$$

We now take Theorem 9.3.6 one step further and tie it together with the work we have done on $\mathcal{N}(x^3 + y^3 = 1)$.

Theorem 9.3.12 *Suppose that $p \equiv 1 \bmod 3$. Then there are integers A and B such that $4p = A^2 + 27B^2$. If we require that $A \equiv 1 \bmod 3$, then A is uniquely determined, and*

$$N(x^3 + y^3 = 1) = p - 2 + A.$$

Proof: By the discussion preceding this theorem, $J(\chi, \chi) = a + b\omega$, where $a \equiv 2 \bmod 3$ and $b \equiv 0 \bmod 3$. This implies that there are $s, t \in \mathbb{Z}$, such that $a = 3s + 2$ and $b = 3t$. So

$$\begin{aligned} 2a - b &= 2(3s + 2) - 3t \\ &= 6s + 4 - 3t \\ &\equiv 1 \bmod 3. \end{aligned}$$

Set $A = 2a - b$, then $A \equiv 1 \bmod 3$ is uniquely determined. We do not prove uniqueness here, but it can be found in [8]. Thus the number of solutions to $x^3 + y^3 = 1$ is given by $\mathcal{N}(x^3 + y^3 = 1) = p - 2 + A$. ∎

Chapter 10

Cubic Reciprocity

In this chapter, we finally get to explore the idea of cubic reciprocity. We begin Section 1 by defining a new term, rational prime, in an effort to keep track of the various types of primes that we now have. Recall that in Section 5.4, we established some properties and characteristics of the ring $\mathbb{Z}[\omega]$. We also began looking at ways to identify the units and primes in the ring. We will expand on that work, and develop results that we will need to prove the Law of Cubic Reciprocity later. We also prove a theorem that tells us how to determine whether or not an Eisenstein integer is prime in $\mathbb{Z}[\omega]$.

In section 2, we examine a specific factor ring and develop properties about that ring. Some of the concepts used are similar to things we did in the ring theory chapter, but in this special setting.

In the third section, we define cubic residue characters and develop

some properties similar to the properties of the Legendre symbol that we saw previously. We also define something called a primary prime and develop several results about these primes, and end the section by stating the Law of Cubic Reciprocity and proving it in two different ways.

We finish off the chapter by looking at the special case of the cubic character of 2 More specifically, we explore the circumstances under which 2 is a cubic residue.

10.1 Rational Primes

In Chapter 5, we established that $\mathbb{Z}[\omega]$ is a unique factorization domain, and thus that primes and irreducibles are the same thing in $\mathbb{Z}[\omega]$. We want to examine the prime elements in $\mathbb{Z}[\omega]$ in detail, but we need to keep in mind that primes in this setting are not necessarily primes in the integers. For example, 3 is prime in $\mathbb{Z}$, but $3 = (2+\omega)(1-\omega) = (-1-2\omega)(1+2\omega)$ is not prime in $\mathbb{Z}[\omega]$. To help keep the different primes straight, we will define a new term that we will use from here on out.

Our current definition of prime states that if p is a nonzero nonunit element of an integral domain D, then for all $a, b \in D$, $p \mid ab$ implies that either $p \mid a$ or $p \mid b$.

Definition 10.1.1 If p is a prime in $\mathbb{Z}$, then p will be called a *rational prime*.

If $a + b\omega \in \mathbb{Z}[\omega]$ is prime, it will be denoted π unless otherwise specified, and will be referred to simply as *prime*. $\diamondsuit$

In the ring theory chapter, we defined the term associates. Recall that if a and b are elements of a ring and $a = bu$, where u is a unit in the ring, then a and b are associates. We also explored the idea of norm in $\mathbb{Z}[\omega]$, and noted that if $\alpha = a + b\omega \in \mathbb{Z}[\omega]$, then $N(\alpha) = a^2 - ab + b^2$.

Theorem 10.1.2 *Suppose that π is a prime in $\mathbb{Z}[\omega]$. Then there exists a rational prime p, such that either $N(\pi) = p$ or $N(\pi) = p^2$. If $N(\pi) = p^2$, then π and p are associates. If $N(\pi) = p$, π is not associate to a rational prime.*

Note that if π and p are associates, then p is prime in $\mathbb{Z}[\omega]$, since π and p differ only by multiplication of one of the six units in $\mathbb{Z}[\omega]$.

Example 10.1.3 Let $\pi_1 = 2 + \omega$. Recall that by the work done in Example 5.4.9 that this is prime in $\mathbb{Z}[\omega]$.

$$\begin{aligned} N(2+\omega) &= 4 - 2 + 1 && \text{(Definition of norm)} \\ &= 3. && \text{(Arithmetic)} \end{aligned}$$

Let $\pi_2 = 3 + \omega$, which is also prime.

$$\begin{aligned} N(3+\omega) &= 3^2 - 3 + 1 && \text{(Definition of norm)} \\ &= 7. && \text{(Arithmetic)} \end{aligned}$$

Let $\pi_3 = 2$. Since 2 cannot be written as $(a + b\omega)(c + d\omega)$, where $a, b, c, d \in \mathbb{Z}$, 2 is prime in $\mathbb{Z}[\omega]$. Thus

$$N(2) = 4. \qquad \text{(Definition of norm)}$$

In this case, $N(2) = 2^2$, so $\pi_3 = 2$ is associate to $p = 2$. □

Proof: Let $\pi \in \mathbb{Z}[\omega]$ be prime. Then π is not a unit, so $N(\pi) \neq 1$, thus $N(\pi) > 1$. Let $N(\pi) = n$, where $n \in \mathbb{N}$ and $n > 1$. Then $\pi\overline{\pi} = n$ by definition.

Since $n \in \mathbb{N}$, $n = p_1 p_2 \dots p_m$, where each p_i is a rational prime. So $n = p_1 \dots p_m = \pi\overline{\pi}$, which implies that $\pi \mid p_i$, for one of the rational primes p_i, say p. Suppose $p = \pi\gamma$, for $\gamma \in \mathbb{Z}[\omega]$. Then

$$\begin{aligned} N(\pi)N(\gamma) &= N(p) && \text{(Take the norm of both sides)} \\ &= p^2. && \text{(Definition of norm)} \end{aligned}$$

It follows that either $N(\pi) = p^2$ and $N(\gamma) = 1$ or $N(\pi) = p = N(\gamma)$.

If $N(\gamma) = 1$, then γ is a unit, by Theorem 5.4.8, and π and p are associates.

If instead $N(\pi) = p$, suppose that $\pi = uq$, where u is a unit and q is a rational prime. This implies that

$$\begin{aligned} p &= N(\pi) \\ &= N(u)N(q) && \text{(Norm is multiplicative)} \\ &= 1 \cdot q^2 && \text{(Definition of norm)} \end{aligned}$$

which is impossible, since p is a rational prime. Thus p is not associate to a rational prime in this case. ∎

Theorem 10.1.4 *If $\pi \in \mathbb{Z}[\omega]$ is such that $N(\pi) = p$, where p is a rational prime, then π is prime in $\mathbb{Z}[\omega]$.*

Proof: Assume $N(\pi) = p$, for some rational prime p and let $\pi = \alpha\beta$. Then

$$\begin{aligned} p =& N(\pi) \\ =& N(\alpha)N(\beta), && \text{(N is multiplicative)} \end{aligned}$$

which implies without loss of generality that $N(\alpha) = p$ and $N(\beta) = 1$, which in turn implies that π is irreducible, and thus is prime. ∎

Example 10.1.5 Let $\pi = 3$. Then $N(\pi) = 9$, which is not a rational prime, and we know from previous work that 3 is not prime in $\mathbb{Z}[\omega]$.

Let $\pi = 2 + 3\omega$. Then $N(\pi) = 4 - 6 + 9 = 7$, which is a rational prime, so $2 + 3\omega$ is prime in $\mathbb{Z}[\omega]$. □

Theorem 10.1.6 *Suppose that p and q are rational primes. If $q \equiv 2 \bmod 3$, then q is prime in $\mathbb{Z}[\omega]$. If $p \equiv 1 \bmod 3$, then $p = \pi\overline{\pi}$, where π is some prime in $\mathbb{Z}[\omega]$. Finally, $3 = -\omega^2(1-\omega)^2$, where $1 - \omega$ is prime in $\mathbb{Z}[\omega]$.*

Proof: Suppose that $p \neq 3$ is a rational prime that is not prime in $\mathbb{Z}[\omega]$. Then $p = \pi\gamma$ for some $\pi, \gamma \in \mathbb{Z}[\omega]$, where $N(\pi) > 1$ and $N(\gamma) > 1$, which implies that $p^2 = N(p) = N(\pi)N(\gamma)$, so $N(\pi) = p$ and $N(\gamma) = p$.

Let $\pi = a + b\omega$. Then, since $N(\pi) = p$, we have

$$\begin{aligned}
& p = a^2 - ab + b^2 && (N(a + b\omega) = a^2 - ab + ab) \\
\iff & 4p = 4a^2 - 4ab + 4b^2 && \text{(Multiplication Property of Equality)} \\
\iff & 4p = (4a^2 - 4ab + b^2) + 3b^2 && \text{(Split } 4b^2 \text{ into two terms)} \\
\iff & 4p = (2a - b)^2 + 3b^2, && \text{(Factor)}
\end{aligned}$$

which implies that $p \equiv (2a - b)^2 \bmod 3$.

The least residues modulo 3 are 0, 1, and 2, but only 0 and 1 are perfect squares. If $p \equiv 0 \bmod 3$, then $p = 3$ is the only possibility, which contradicts our assumption that $p \neq 3$. Thus, $p \equiv 1 \bmod 3$.

Since the assumption that p is not prime in $\mathbb{Z}[\omega]$ is what led to the result that $p \equiv (2a - b)^2 \bmod 3$, then if $p \equiv 2 \bmod 3$, it follows immediately from the work above that p is in fact prime in $\mathbb{Z}[\omega]$, since 2 is not a perfect square, and thus does not satisfy the congruence.

For the last part of the theorem, recall that $N(a + b\omega) = a^2 - ab + b^2$. If we set $a = 1$ and $b = -1$, then $N(1 - \omega) = 3$. Then using what we know

about norms,

$$
\begin{aligned}
& N(1-\omega) = 3 \\
\Longrightarrow\ & (1-\omega)(1-\overline{\omega}) = 3 && (N(\alpha) = \alpha\overline{\alpha}) \\
\Longrightarrow\ & (1-\omega)(1-\omega^2) = 3 && (\overline{\omega} = \omega^2) \\
\Longrightarrow\ & (1-\omega)(1-\omega)(1+\omega) = 3 && (\text{Factorization of } 1-\omega^2) \\
\Longrightarrow\ & (1-\omega)^2(-\omega^2) = 3, && (-\omega^2 = \omega + 1)
\end{aligned}
$$

which is the desired result. ∎

For the remainder of this chapter, unless otherwise specified, q will represent a positive rational prime, where $q \equiv 2 \bmod 3$ and q is prime in $\mathbb{Z}$. Likewise, π will represent a prime in $\mathbb{Z}[\omega]$, such that $N(\pi) = p$, where p is a rational prime and $p \equiv 1 \bmod 3$.

10.2 Residue Class Rings

Suppose α, β, $\gamma \in \mathbb{Z}[\omega]$, where $\gamma \neq 0$ and γ is not a unit. In this setting, $\alpha \equiv \beta \bmod \gamma$ if and only if $\gamma \mid (\alpha - \beta)$, just as it is when we work over the integers.

Recall that in Example 5.4.10, we examined $\dfrac{\mathbb{Z}[\omega]}{(1-\omega)\mathbb{Z}[\omega]}$ and determined that it contains three elements, specifically [0], [1], and [2]. The following theorem generalizes this result for any prime $\pi \in \mathbb{Z}[\omega]$.

Theorem 10.2.1 *Let $\pi \in \mathbb{Z}[\omega]$ be prime. Then $\dfrac{\mathbb{Z}[\omega]}{\pi\mathbb{Z}[\omega]}$ is a finite field with $N(\pi)$ elements.*

Proof: Suppose $\pi \in \mathbb{Z}[\omega]$ is prime. To prove that $\dfrac{\mathbb{Z}[\omega]}{\pi\mathbb{Z}[\omega]}$ is a field, note that π is prime if and only if π is irreducible, since $\mathbb{Z}[\omega]$ is a unique factorization domain. But π is irreducible if and only if $\pi\mathbb{Z}[\omega]$ is maximal, by Proposition 5.3.3, and by Proposition 5.2.17, $\pi\mathbb{Z}[\omega]$ is maximal if and only if $\dfrac{\mathbb{Z}[\omega]}{\pi\mathbb{Z}[\omega]}$ is a field.

Suppose $\pi = q$ is a rational prime, where $q \equiv 2 \bmod 3$. We claim that $\{a + b\omega : 0 \leqslant a, b < q\}$ is a complete set of coset representatives. Let $\mu = m+n\omega \in \mathbb{Z}[\omega]$. Then by the division algorithm for the integers, $m = qs+a$ and $n = qt + b$, where $a, b, s, t \in \mathbb{Z}$ and $0 \leqslant a, b < q$. So

$$\begin{aligned}
& \mu = m + n\omega \\
\iff & \mu = (qs + a) + (qt + b)\omega && \text{(Substitution)} \\
\iff & \mu = q(s + tw) + (a + b\omega) && \text{(Distributive Property)} \\
\iff & \mu \equiv a + b\omega \bmod q, && \text{(Definition of congruent)}
\end{aligned}$$

and we have at most q^2 elements. Suppose that $a+b\omega \equiv a'+b'\omega \bmod q$, where $0 \leqslant a, a', b, b' < q$. Then $q \mid (a-a')+(b-b')\omega$, which implies that $q \mid (a-a')$ and $q \mid (b-b')\omega$, and it follows that $q \mid (b-b')$, since q is a rational prime. But since $0 \leqslant a, a', b, b' < q$, it has to be the case that $a = a'$ and $b = b'$. Thus $\dfrac{\mathbb{Z}[\omega]}{\pi\mathbb{Z}[\omega]}$ has $N(q) = q^2$ elements.

Now suppose that $\pi = a + b\omega$ is not a rational prime. Then there is a rational prime p, such that $p \equiv 1 \bmod 3$ and $N(\pi) = \pi\overline{\pi} = p$. We claim that $\{0, 1, \ldots, p-1\}$ is a complete set of coset representatives of $\dfrac{\mathbb{Z}[\omega]}{\pi\mathbb{Z}[\omega]}$. Since $N(\pi) = a^2 - ab + b^2 = p$, it follows that $p \nmid b$. Let $\mu = m + n\omega$. Since $\gcd(b, p) = 1$, b is a generator modulo p, so there is some $c \in \mathbb{Z}$ such that $cb \equiv n \bmod p$, so $cb = n + kp$ for some k. Now, $c\pi = ac + bc\omega$, so

$$\begin{aligned}
\mu - c\pi &= (m + n\omega) - (ac + bc\omega) && \text{(Substitution)} \\
&= (m - ac) + (n - bc)\omega && \text{(Commutative, Distributive Properties)} \\
&= (m - ac) + (-kp)\omega, \text{ for some } k && (cb = n + kp) \\
&\equiv (m - ac) \bmod p. && \text{(Definition of congruent)}
\end{aligned}$$

Thus we have $\mu - c\pi \equiv (m - ac) \bmod p$, but this implies that there is some j such that $\mu = m + c\pi - ca + jp$. Since $p = \pi\overline{\pi}$, we can rewrite this as $\mu = m - ca + \pi(c + j\overline{\pi})$, and it follows that $\mu \equiv m - ca \bmod \pi$.

Now, note that every element of $\mathbb{Z}[\omega]$ is congruent to a rational integer modulo π. Suppose $l \in \mathbb{Z}$. Then $l = sp + r$, by the division algorithm for the integers, where $0 \leqslant r < p$. This implies that $l \equiv r \bmod p$, and by a similar argument as that used above, $l \equiv r \bmod \pi$. Thus, every $\alpha \in \mathbb{Z}[\omega]$ is congruent to an element in $\{0, 1, \ldots, p-1\}$ modulo π. Furthermore, if $r \equiv r' \bmod \pi$, where $r, r' \in \mathbb{Z}$ and $0 \leqslant r, r' < p$, then $r - r' = \pi\gamma$, for $\gamma \in \mathbb{Z}[\omega]$ and

$$N(r - r') = N(\pi)N(\gamma) \iff (r - r')^2 = p \cdot N(\gamma).$$

This implies that $p \mid (r-r')$, by the definition of divides in $\mathbb{Z}$. But $0 \leqslant r, r' < p$, so $r - r' = 0$, and it follows that $r = r'$. Hence, $\dfrac{\mathbb{Z}[\omega]}{\pi\mathbb{Z}[\omega]}$ has $N(\pi) = p$ elements.

We already showed in Example 5.4.10, that when $\pi = 1 - \omega$, the factor ring $\dfrac{\mathbb{Z}[\omega]}{\pi\mathbb{Z}[\omega]}$ only has the three elements [0], [1], and [2]. Thus the order of $\dfrac{\mathbb{Z}[\omega]}{\pi\mathbb{Z}[\omega]}$ is $N(\pi) = 3$. ∎

10.3 Cubic Residue Character

We know from Theorem 10.2.1 that $\dfrac{\mathbb{Z}[\omega]}{\pi\mathbb{Z}[\omega]}$ has order $N(\pi)$. This means that the order of the multiplicative group $\left(\dfrac{\mathbb{Z}[\omega]}{\pi\mathbb{Z}[\omega]}\right)^*$, for any prime π is $N(\pi) - 1$. The multiplicative group is the group of units under multiplication modulo π, and the only difference in the two sets is that 0 is not an element of the multiplicative group. So if we choose $\alpha \in \left(\dfrac{\mathbb{Z}[\omega]}{\pi\mathbb{Z}[\omega]}\right)^*$, we know from principles of group theory that $\alpha^{N(\pi)-1} \equiv 1 \bmod \pi$. Hence we have an analog of Fermat's Little Theorem that applies in this setting.

Theorem 10.3.1 *Let π be prime. If $\pi \nmid \alpha$, then $\alpha^{N(\pi)-1} \equiv 1 \bmod \pi$.*

Proof: This follows immediately from the discussion above. ∎

Theorem 10.3.2 *Suppose that π is a prime such that $N(\pi) \neq 3$ and $\pi \nmid \alpha$. Then there is a unique integer $m = 0$, 1, or 2 such that*

$$\alpha^{(N(\pi)-1)/3} \equiv \omega^m \bmod \pi.$$

Proof: Let $\alpha \in \left(\frac{\mathbb{Z}[\omega]}{\pi\mathbb{Z}[\omega]}\right)^*$. Since there are $N(\pi) - 1$ elements in this multiplicative group, we know that $\alpha^{N(\pi)-1} \equiv 1 \bmod \pi$.

Note that $[\omega] \in \frac{\mathbb{Z}[\omega]}{\pi\mathbb{Z}[\omega]}$, since elements are of the form $[a + b\omega]$, and if $a = 0$ and $b = 1$, we have $[\omega]$. We know that $\omega^3 = 1$, so $[\omega]^3 = [1]$. Since the set $\{1, \omega, \omega^2\}$ is closed under multiplication, $\left\{[1], [\omega], [\omega]^2\right\}$ is a subgroup of order 3 of our multiplicative group. But this implies that 3 divides the order of the whole group, or that $3 \mid N(\pi) - 1$.

Recall that in a field, the equation $x^3 = 1$ has exactly three solutions. Since $\alpha^{N(\pi)-1} \equiv 1 \bmod \pi$, it is also the case that $\left(\alpha^{(N(\pi)-1)/3}\right)^3 \equiv 1 \bmod \pi$, which implies that $\alpha^{(N(\pi)-1)/3}$ is a solution to $x^3 \equiv 1 \bmod \pi$. But $1^3 \equiv 1 \bmod \pi$, $\omega^3 \equiv 1 \bmod \pi$, and $\left(\omega^2\right)^3 \equiv \left(\omega^3\right)^2 \equiv 1 \bmod \pi$, so the three possibilities for $\alpha^{(N(\pi)-1)/3}$ are 1, ω, or ω^2. Thus m is either 0, 1, or 2, as desired. ∎

For the following theorem, suppose $\mathbb{F}$ denotes any finite field with q elements. Then $\mathbb{F}^*$ is cyclic and contains $q - 1$ elements [8].

Theorem 10.3.3 *Let $\alpha \in \mathbb{F}^*$. Then $x^n = \alpha$ has solutions if and only if $\alpha^{(q-1)/d} = 1$, where $d = \gcd(n, q-1)$. If solutions exist, then there are exactly d of them.*

Proof: This theorem is an application of Theorem 6.0.5, which states that if $\gcd(n, q-1) = d$, then $nx \equiv l \bmod (q-1)$ has exactly d solutions if and only if $d \mid l$.

$\mathbb{F}^*$ is a cyclic group with generator g, containing $q-1$ elements, so $g^{q-1} = 1$. Define a group isomorphism $\varphi : \mathbb{F}^* \to \mathbb{Z}_{q-1}$ by $\varphi(g^l) = l$, where $0 \leqslant l \leqslant q-1$. Set $\alpha = g^l$ and suppose that $\gcd(n, q-1) = d$. Because g has order $p-1$, we know that $(g^l)^{(q-1)/d} = 1$ if and only if $d \mid l$, so by Theorem 6.0.5, $n^n = \alpha$ has solutions if and only $d \mid l$, and if a solution exists, then there are exactly d of them. ∎

Definition 10.3.4 If $N(\pi) \neq 3$, the *cubic residue character of* α *modulo* π is given by

1. $(\alpha/\pi)_3 \equiv \alpha^{(N(\pi)-1)/3} \bmod \pi$, with $(\alpha/\pi)_3$ equal to 1, ω, or ω^2.

2. $(\alpha/\pi)_3 = 0$ if $\pi \mid \alpha$.

This is the cubic analog to the Legendre symbol. ♢

Recall that the Legendre symbol represents the solvability of the congruence $x^2 \equiv a \bmod p$, and is defined to be equal to 0 if $p \mid a$. Also, $(a/p) \equiv a^{(p-1)/2} \bmod p$, with $(a/p) = \pm 1$.

In the quadratic case, the outputs of the Legendre symbol are the two roots of $x^2 = 1$, and in the cubic case, the outputs of the cubic residue character are the three roots of $x^3 = 1$, which are 1, ω, and ω^2. As we will see, the cubic character has many of the same properties that we saw previously for the Legendre symbol.

Theorem 10.3.5 (Properties of the Cubic Residue Character) *Let π be a prime and let $\alpha \in \left(\frac{\mathbb{Z}[\omega]}{\pi\mathbb{Z}[\omega]}\right)^*$. Then*

1. $(\alpha/\pi)_3 \equiv \alpha^{(N(\pi)-1)/3} \bmod \pi$.

2. $(\alpha/\pi)_3 = 1$ *if and only if* $x^3 \equiv \alpha \bmod \pi$ *is solvable. In other words, if and only if* α *is a cubic residue.*

3. $(\alpha\beta/\pi)_3 = (\alpha/\pi)_3(\beta/\pi)_3$.

4. *If* $\alpha \equiv \beta \bmod \pi$, *then* $(\alpha/\pi)_3 = (\beta/\pi)_3$.

Proof: Suppose $\alpha, \beta \in \left(\frac{\mathbb{Z}[\omega]}{\pi\mathbb{Z}[\omega]}\right)^*$ and suppose π is prime.

1. Recall that in Theorem 10.3.3, we saw that $x^n = \alpha$ has exactly d solutions if and only if $\alpha^{(q-1)/d} = 1$. This result follows immediately from that theorem, with $N(\pi) = q$ and $n = 3$, since this is saying $\alpha^{(N(\pi)-1)/d} = 1$ if and only if $x^3 \equiv \alpha \bmod \pi$ is solvable.

2. This follows immediately from Definition 10.3.4.

3.

$$\begin{aligned}
(\alpha\beta/\pi)_3 &\equiv (\alpha\beta)^{(N(\pi)-1)/3} \bmod \pi && \text{(Definition 10.3.4)} \\
&\equiv \alpha^{(N(\pi)-1)/3}\beta^{(N(\pi)-1)/3} \bmod \pi && \text{(Properties of Exponents)} \\
&\equiv (\alpha/\pi)_3(\beta/\pi)_3 \bmod \pi. && \text{(Definition 10.3.4)}
\end{aligned}$$

4. Suppose $\alpha \equiv \beta \bmod \pi$. Then

$$\begin{aligned}
(\alpha/\pi)_3 &\equiv \alpha^{(N(\pi)-1)/3} \bmod \pi && \text{(Definition 10.3.4)} \\
&\equiv \beta^{(N(\pi)-1)/3} \bmod \pi && (\alpha \equiv \beta \bmod \pi) \\
&\equiv (\beta/\pi)_3 \bmod \pi. && \text{(Definition 10.3.4)}
\end{aligned}$$

Thus, each of the properties of the cubic residue character holds. ∎

Theorem 10.3.6 *Suppose π is prime and $\alpha \in \left(\frac{\mathbb{Z}[\omega]}{\pi\mathbb{Z}[\omega]}\right)^*$. Then*

1. $\overline{(\alpha/\pi)}_3 = \left((\alpha/\pi)_3\right)^2 = (\alpha^2/\pi)$.

2. $\overline{(\alpha/\pi)}_3 = (\overline{\alpha}/\overline{\pi})_3$.

In this Theorem, it is important to point out that the bar notation should not be confused with our use of bars in previous chapters to denote partitions and conjugacy classes. When we are working with complex numbers, the bar notation will denote the conjugate of a complex number unless otherwise specified. Note that

$$\begin{aligned}
\overline{\sqrt{-3}} &= \overline{\sqrt{3}i} \\
&= -\sqrt{3}i \\
&= -\sqrt{-3},
\end{aligned}$$

so $\overline{\omega} = \omega^2$. Also, since $\omega^2 + \omega + 1 = 0$, we have $\omega^2 = -1 - \omega$. Thus, if $\alpha = a + b\omega$,

$$\begin{aligned}
\overline{\alpha} &= a + b\overline{\omega} \\
&= a + b\omega^2 && (\overline{\omega} = \omega^2) \\
&= a + b(-1 - \omega) && (\omega^2 = -1 - \omega) \\
&= (a - b) - b\omega. && \text{(Distributive Property)}
\end{aligned}$$

Proof: Assume π is a prime in $\mathbb{Z}[\omega]$ and let $\alpha \in \left(\dfrac{\mathbb{Z}[\omega]}{\pi\mathbb{Z}[\omega]}\right)^*$.

1. Recall that by definition of $(\alpha/\pi)_3$, the possible values it can take are 1, ω, or ω^2. Suppose that $(\alpha/\pi)_3 = \omega$. Then

$$\begin{aligned}
\overline{(\alpha/\pi)_3} &= \overline{\omega} && \text{(Substitution)} \\
&= \omega^2. && (\overline{\omega} = \omega^2)
\end{aligned}$$

   We also have

$$\begin{aligned}
\left((\alpha/\pi)_3\right)^2 &= (\alpha/\pi)_3(\alpha/\pi)_3 \\
&= (\alpha^2/\pi)_3. && \text{(Theorem 10.3.5)}
\end{aligned}$$

   Since $(\alpha/\pi)_3(\alpha/\pi)_3 = \omega^2$ when $(\alpha/\pi)_3 = \omega$, equality holds.

   The proof works exactly the same way for the other two values, in that the conjugate of the value is equal to the value squared, so regardless of the value that $(\alpha/\pi)_3$ takes, we have $\overline{(\alpha/\pi)_3} = \left((\alpha/\pi)_3\right)^2 = (\alpha^2/\pi)$.

2. Observe that $N(\pi) = \pi\overline{\pi} = N(\overline{\pi})$, so

$$\begin{aligned}
(\overline{\alpha}/\overline{\pi})_3 &\equiv \overline{\alpha}^{(N(\overline{\pi})-1)/3} \bmod \overline{\pi} && \text{(Theorem 10.3.5)} \\
&\equiv \overline{\alpha}^{(N(\pi)-1)/3} \bmod \overline{\pi} && (N(\overline{\pi}) = N(\pi)) \\
&\equiv \overline{(\alpha/\pi)_3} \bmod \overline{\pi}. && \text{(Theorem 10.3.6)}
\end{aligned}$$

But the only values that the cubic residue character can take are 1, ω, and ω^2. Since each of these is a least residue modulo $\overline{\pi}$, we have $(\overline{\alpha}/\overline{\pi})_3 = \overline{(\alpha/\pi)_3}$, as desired. ∎

Corollary 10.3.7 *Suppose that q is a rational prime. Then $(\overline{\alpha}/q)_3 = (\alpha^2/q)_3$ and $(n/q)_3 = 1$ if n is an integer relatively prime to q.*

Proof: Let $n \in \mathbb{Z}$ and suppose that q is a rational prime such that $\gcd(n, q) = 1$. Let $\alpha \in \left(\dfrac{\mathbb{Z}[\omega]}{\pi\mathbb{Z}[\omega]}\right)^*$. Since the complex conjugate of an integer is the integer itself, $\overline{q} = q$. Thus

$$\begin{aligned}
(\overline{\alpha}/q)_3 &= (\overline{\alpha}/\overline{q})_3 && (q = \overline{q}) \\
&= \overline{(\alpha/q)_3} && \text{(Theorem 10.3.6)} \\
&= (\alpha^2/q)_3. && \text{(Theorem 10.3.6)}
\end{aligned}$$

Since $\overline{n} = n$ and $\overline{q} = q$,

$$\begin{aligned}
(n/q)_3 &= (\overline{n}/\overline{q})_3 && (n = \overline{n};\ q = \overline{q}) \\
&= \overline{(n/q)_3} && \text{(Theorem 10.3.6)} \\
&= \big((n/q)_3\big)^2. && \text{(Theorem 10.3.6)}
\end{aligned}$$

We know that $q \nmid n$, since n and q are relatively prime, thus $(n/q)_3 \neq 0$. The only other option is that $(n/q)_3 = 1$, which is the desired result. ∎

Definition 10.3.8 If π is a prime in $\mathbb{Z}[\omega]$, then π is called a *primary prime* if $\pi \equiv 2 \bmod 3$. If $\pi = q$ is a rational prime, then $q \equiv 2 \bmod 3$. If $\pi = a + b\omega$, then $a \equiv 2 \bmod 3$ and $b \equiv 0 \bmod 3$. ♢

Theorem 10.3.9 *Let π be prime and suppose that $N(\pi) = p \equiv 1 \bmod 3$. Then exactly one of the associates of π is primary.*

Proof: Assume that $N(\pi) = p \equiv 1 \bmod 3$, where π is prime in $\mathbb{Z}[\omega]$. The six associates of π are π, $\omega\pi$, $\omega^2\pi$, $-\pi$, $-\omega\pi$, and $-\omega^2\pi$. Suppose that $\pi = a + b\omega$. Writing each of the associates in terms of a and b gives us

1. $\pi = a + b\omega$
2. $\omega\pi = -b + (a - b)\omega$
3. $\omega^2\pi = (b - a) - a\omega$
4. $-\pi = -a - b\omega$
5. $-\omega\pi = b + (b - a)\omega$
6. $-\omega^2\pi = (a - b) + a\omega$.

We saw in Theorem 9.3.5 that $p = a^2 - ab + b^2$ when $p \equiv 1 \bmod 3$. We can assume that a and b are not both divisible by 3, since if they are, then

$$\begin{aligned} p &= (3k)^2 - (3k)(3j) + (3j)^2 \\ &= 9k^2 - 9kj + 9j^2 \\ &\equiv 0 \bmod 3. \end{aligned}$$

We can also assume that it is not the case that $a \equiv 1 \bmod 3$ and $b \equiv -1 \bmod 3$, or vice versa, since if that is the case, then $p \equiv 0 \bmod 3$.

These assumptions leave us with six cases to consider. First suppose $a \equiv 0 \bmod 3$. Then either $b \equiv 1 \bmod 3$ or $b \equiv -1 \bmod 3$. Assume $b \equiv 1 \bmod 3$ and note that $N(\pi) = 1^2 \equiv 1 \bmod 3$, so this is a valid value for b. Now we examine each of the six associates modulo 3.

$$\begin{aligned} \pi &= 0 + \omega \\ \omega\pi &= -1 - 1\omega \equiv 2 + 2\omega \bmod 3 \\ \omega^2\pi &= 1 - 0\omega \\ -\pi &= -1\omega \\ -\omega\pi &= 1 + 1\omega \\ -w^2\pi &= -b + 0\omega \equiv 2 + 0\omega \bmod 3 \end{aligned}$$

Of the six, only $-w^2\pi$ is primary when $a \equiv 0 \bmod 3$ and $b \equiv 1 \bmod 3$.

Now suppose $b \equiv -1 \bmod 3$ and note that $N(\pi) \equiv 1 \bmod 3$, so this is also a valid value for b. Examination of the six associates yields the following.

$$\pi = 2\omega$$

$$\omega\pi = -2 - 2\omega \equiv 1 + \omega \bmod 3$$

$$\omega^2\pi = 2 - 0\omega$$

$$-\pi = -2\omega \equiv \omega \bmod 3$$

$$-\omega\pi = 2 + 2\omega$$

$$-\omega^2\pi = -2 + 0\omega \equiv 1 \bmod 3$$

Of these six, only $\omega^2\pi$ is primary when $a \equiv 0 \bmod 3$ and $b \equiv 2 \bmod 3$.

The other four cases are handled in exactly the same way. If we assume $a \equiv 1 \bmod 3$, then either $b \equiv 0 \bmod 3$ or $b \equiv 1 \bmod 3$. Of these possibilities, $-\pi$ is primary when $b \equiv 0 \bmod 3$ and $\omega\pi$ is primary when $b \equiv 1 \bmod 3$. If instead we assume that $a \equiv -1 \bmod 3$, then $b \equiv 0 \bmod 3$ or $b \equiv -1 \bmod 3$. In these two cases, π is primary when $b \equiv 0 \bmod 3$ and $-\omega\pi$ is primary when $b \equiv -1 \bmod 3$.

In each case, exactly one of the six associates is primary, which is exactly the result we need. ∎

For ease of notation, we are going to use χ to represent cubic residue characters in general. χ will come along with all of the properties that we previously proved about multiplicative characters. If we are specifically working

modulo π, then the notation χ_π will be used. In other words, $\chi_\pi(\alpha) = (\alpha/\pi)_3$. When we are working in general, χ will just represent a generic cubic character.

Suppose π is a prime such that $N(\pi) = p \equiv 1 \bmod 3$. We know that $\dfrac{\mathbb{Z}[\omega]}{\pi\mathbb{Z}[\omega]}$ is a finite field of characteristic p, so it contains a copy of $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$. Both fields have p elements, thus an isomorphism exists between them. This isomorphism is defined by sending the coset of n in $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$ to the coset of n in $\dfrac{\mathbb{Z}[\omega]}{\pi\mathbb{Z}[\omega]}$, and allows us to work with χ_π as a cubic character in the field $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$. Thus we are able to work with the Gauss sums $g_a(\chi_\pi)$ and the Jacobi sums $J(\chi_\pi, \chi_\pi)$.

Before we look at these specific Gauss and Jacobi sums, we want to revisit some of the general results that we established previously. Recall that in Theorem 9.3.8, we proved that if $p \equiv 1 \bmod n$ and χ is a character of order $n > 2$, then $\big(g(\chi)\big)^n = \chi(-1)pJ(\chi,\chi)J(\chi,\chi^2)\dots J(\chi,\chi^{n-2})$. We then looked at the specific case of $n = 3$ and showed that $\big(g(\chi)\big)^3 = pJ(\chi,\chi)$ in Corollary 9.3.9. Finally, in Theorem 9.3.10, we showed that if $p \equiv 1 \bmod 3$ and χ is a cubic character, then if we set $J(\chi,\chi) = a + b\omega$, we see that $a \equiv 2 \bmod 3$ and $b \equiv 0 \bmod 3$. This result implies that $J(\chi,\chi) = a + b\omega$ is primary when $p \equiv 1 \bmod 3$.

Lemma 10.3.10 *If p is a rational prime and $p-1 \nmid k$, for some nonnegative $k \in \mathbb{Z}$, then*

$$\sum_{i=1}^{p-1} i^k \equiv 0 \bmod p.$$

Proof: Let p be a rational prime and k a nonnegative integer such that $p-1 \nmid k$. Then

$$\sum_{i=1}^{p-1} i^k = 1^k + 2^k + \cdots + (p-1)^k.$$

Observe that each of the i in the sum is an element of the cyclic group $\mathbb{Z}_p^*$. Let g be a generator of $\mathbb{Z}_p^*$ and note that $\{1, 2, \ldots, p-1\}$ is a permutation of $\{g, g^2, \ldots, g^{p-1}\}$ modulo p. This implies that we can rewrite the sum as

$$\begin{aligned}
\sum_{i=1}^{p-1} i^k &\equiv \sum_{i=1}^{p-1} \left(g^i\right)^k \bmod p && (g \text{ generates } \mathbb{Z}_p^*) \\
&\equiv \sum_{i=1}^{p-1} g^{ki} \bmod p && (\text{Properties of exponents}) \\
&\equiv \sum_{i=1}^{p-1} g^i \bmod p && (ki \text{ modulo } p \text{ is a permutation of } \{1, 2, \ldots, p-1\}) \\
&\equiv \sum_{i=0}^{p-2} g^i \bmod p && (\text{Reindex the sum; } g^{p-1} \equiv g^0 \equiv 1 \bmod p) \\
&\equiv \left(1 - g^{p-1}\right)\left(1 - g\right)^{-1} \bmod p && (\text{Sum of finite geometric series}) \\
&\equiv 0 \bmod p,
\end{aligned}$$

since $g^{p-1} \equiv 1 \bmod p$. ∎

Lemma 10.3.11 *Let π be primary. Then $J(\chi_\pi, \chi_\pi) = \pi$.*

Proof: Let $\pi \in \mathbb{Z}[\omega]$ and assume that π is primary. Let $J(\chi_\pi, \chi_\pi) = \pi'$. We know from Theorem 9.3.10 that π' is primary, and it is easy to see that $\overline{\pi}'$ is as well. We also know that $N(\pi) = \pi\overline{\pi} = p$, and by Corollary 9.3.4, we have $|J(\chi_\pi, \chi_\pi)| = \sqrt{p}$ and $|J(\chi_{\overline{\pi}}, \chi_{\overline{\pi}})| = \sqrt{p}$. Thus we can surmise that

$\pi'\overline{\pi}' = |\pi'|^2 = |J(\chi_\pi, \chi_\pi)|^2 = p$, so we have $\pi\overline{\pi} = p = \pi'\overline{\pi}'$. This implies that either π and π' or π and $\overline{\pi}'$ are associates. But π is primary, so by Theorem 10.3.9, either $\pi = \pi'$ or $\pi = \overline{\pi}'$. Our goal is to show that the second case does not occur.

From the definition of Jacobi sum, we have

$$\begin{aligned}
J(\chi_\pi, \chi_\pi) &= \sum_{x+y=1} \chi_\pi(x)\chi_\pi(y) && \text{(Definition of Jacobi Sum)} \\
&= \sum_{x=0}^{p-1} \chi_\pi(x)\chi_\pi(1-x) && (y = 1-x) \\
&\equiv \sum_{x=0}^{p-1} (x/\pi)_3 \cdot (1 - x/\pi)_3 \bmod \pi && (\chi_\pi(x) = (x/\pi)_3) \\
&\equiv \sum_{x=0}^{p-1} x^{(N(\pi)-1)/3} \cdot (1-x)^{(N(\pi)-1)/3} \bmod \pi && \text{(Theorem 10.3.5)} \\
&\equiv \sum_{x=0}^{p-1} x^{(p-1)/3} \cdot (1-x)^{(p-1)/3} \bmod \pi. && (N(\pi) = p)
\end{aligned}$$

We can simplify our work above by making a couple of observations. First, notice that when $x = 0$, both of the factors in the sum are equal to 0, so we can start indexing at $x = 1$. We also have $N(\pi) = p \equiv 1 \bmod 3$, so let $p = 3t + 1$

for some t. Then $\dfrac{p-1}{3} = t$ for some t. Making these changes yields

$$\begin{aligned}
J(\chi_\pi, \chi_\pi) &\equiv \sum_{x=1}^{p-1} x^{(p-1)/3} \cdot (1-x)^{(p-1)/3} \bmod \pi \\
&\equiv \sum_{x=1}^{p-1} x^t \cdot (1-x)^t \bmod \pi, \text{ for some } t && ((p-1)/3 = t) \\
&\equiv \sum_{x=1}^{p-1} \big(x(1-x)\big)^t \bmod \pi, \text{ for some } t && \text{(Properties of exponents)} \\
&\equiv \sum_{x=1}^{p-1} (x - x^2)^t \bmod \pi, \text{ for some } t && \text{(Distributive Property)} \\
&\equiv \sum_{x=1}^{p-1} \sum_{k=0}^{t} \binom{t}{k} x^{t-k} (-x^2)^k \bmod \pi, \text{ for some } t \\
& && \text{(Binomial Expansion Theorem)} \\
&\equiv \sum_{x=1}^{p-1} \sum_{k=0}^{t} \binom{t}{k} (-1)^k x^{t-k} x^{2k} \bmod \pi, \text{ for some } t \\
& && \text{(Properties of exponents)} \\
&\equiv \sum_{x=1}^{p-1} \sum_{k=0}^{t} \binom{t}{k} (-1)^k x^{t+k} \bmod \pi, \text{ for some } t \\
& && \text{(Properties of exponents)} \\
&\equiv \sum_{x=1}^{p-1} x^t + \sum_{x=1}^{p-1} -t x^{t+1} + \cdots + \sum_{x=1}^{p-1} (-1)^t x^{2t} \bmod \pi, \text{ for some } t. \\
& && \text{(Expand inner sum)}
\end{aligned}$$

Thus we have

$$J(\chi_\pi, \chi_\pi) \equiv \sum_{x=1}^{p-1} x^t + \sum_{x=1}^{p-1} -t x^{t+1} + \cdots + \sum_{x=1}^{p-1} (-1)^t x^{2t} \bmod \pi, \text{ for some } t.$$

Now we want to apply Lemma 10.3.10, so we examine the right hand side of the equation modulo p. Each of the sums in the equation is of the form

$C\sum_{x=1}^{p-1} x^k$ for some constant C and some nonnegative exponent k. Furthermore, notice that $(p-1) \nmid k$ for any of the exponents k. By Lemma 10.3.10, each of the sums is congruent to 0 modulo p.

Now, recall that $\pi\overline{\pi} = p$ and observe that if $\alpha \equiv \beta \bmod p$, that is equivalent to saying $\alpha = \beta + \gamma p$ for some γ. But if we substitute $\pi\overline{\pi}$ for p, then we have $\alpha = \beta + \gamma\pi\overline{\pi}$, which implies that $\alpha \equiv \beta \bmod \pi$. Thus

$$\sum_{x=1}^{p-1} x^t + \sum_{x=1}^{p-1} -tx^{t+1} + \cdots + \sum_{x=1}^{p-1} (-1)^t x^{2t} \equiv 0 \bmod p$$

implies that

$$J(\chi_\pi, \chi_\pi) = \sum_{x=1}^{p-1} x^t + \sum_{x=1}^{p-1} -tx^{t+1} + \cdots + \sum_{x=1}^{p-1} (-1)^t x^{2t} \equiv 0 \bmod \pi.$$

But $J(\chi_\pi, \chi_\pi) = \pi'$, so we have $\pi' \equiv 0 \bmod \pi$. However, both π and π' are primary, and by Theorem 10.3.9, exactly one of the associates of π can be primary, so it must be the case that $\pi = \pi'$, and the result follows. ∎

The next lemma takes Corollary 10.3.7 one step further and proves that for a specific type of rational prime, every integer is a cubic residue.

Lemma 10.3.12 *If $q \equiv 2 \bmod 3$ is a rational prime, then every integer is a cubic residue modulo q.*

Proof: Assume that $q \equiv 2 \bmod 3$ is a rational prime. Then define $\varphi : \mathbb{Z}_q^* \to \mathbb{Z}_q^*$ by $\varphi(k) = k^3$. This φ is a group homomorphism, and by the Fundamental Homomorphism Theorem, $\dfrac{\mathbb{Z}_q^*}{\ker(\varphi)} \cong \mathrm{Im}(\varphi)$.

Now, $k \in \ker(\varphi)$ if and only if $k^3 = 1$. But we know that $\mathbb{Z}_q^*$ is a cyclic group of order $q-1$, and $3 \nmid q-1$, so $k^3 = 1$ implies that $k = 1$. Thus $\ker(\varphi)$ is trivial.

Note that

$$|\mathrm{Im}(\varphi)| = \left|\frac{\mathbb{Z}_q^*}{\ker(\varphi)}\right| = \frac{\left|\mathbb{Z}_q^*\right|}{1} = \left|\mathbb{Z}_q^*\right|,$$

which implies that φ is onto. It follows that every element of $\mathbb{Z}_q^*$ is a perfect cube. ∎

Corollary 10.3.13 *Let π be primary. Then $\big(g(\chi_\pi)\big)^3 = p\pi$.*

Proof: Assume $\pi \in \mathbb{Z}[\omega]$ is primary. By Corollary 9.3.9, we know that $\big(g(\chi_\pi)\big)^3 = pJ(\chi_\pi, \chi_\pi)$. But by Lemma 10.3.11, $J(\chi_\pi, \chi_\pi) = \pi$. Putting the two results together yields

$$\big(g(\chi_\pi)\big)^3 = pJ(\chi_\pi, \chi_\pi) = p\pi,$$

as desired. ∎

Lemma 10.3.14 *If α and β are primary elements of $\mathbb{Z}[\omega]$, then $-\alpha\beta$ is also primary.*

Proof: Let $\alpha = a + b\omega, \beta = c + d\omega \in \mathbb{Z}[\omega]$ be primary. Then both α and β are congruent to 2 modulo 3, so let $\alpha = 3t + 2$ and $\beta = 3s + 2$ for some

$s, t \in \mathbb{Z}$. The product of the two elements is

$$\begin{aligned}\alpha\beta &= (3t+2)(3s+2) \\ &= 9st + 6t + 6s + 4 \\ &\equiv 1 \bmod 3,\end{aligned}$$

but if we consider instead $-\alpha\beta$, then $-\alpha\beta \equiv -1 \bmod 3 \equiv 2 \bmod 3$. Thus when α and β are primary, the opposite of their product is also primary. ∎

Corollary 10.3.15 *Assume that $\gamma_1, \gamma_2, \ldots, \gamma_k$ are all primary elements of $\mathbb{Z}[\omega]$. Then $(-1)^{k-1}\gamma_1\gamma_2\ldots\gamma_k$ is also primary.*

Proof: We use induction on k. The base case is $k = 2$, and it holds by Lemma 10.3.14. Assume that the result holds for some k and consider the product of $k+1$ primitive elements, $\gamma_1\gamma_2\ldots\gamma_k\gamma_{k+1}$. By the inductive assumption, we know that $(-1)^{k-1}\gamma_1\gamma_2\ldots\gamma_k$ is primitive. We also know that γ_{k+1} is primitive. Thus by Lemma 10.3.14, $(-1)(-1)^{k-1}\gamma_1\ldots\gamma_{k+1} = (-1)^k\gamma_1\ldots\gamma_{k+1}$ is also primary, so the result holds for all $k \in \mathbb{N}$. ∎

The previous lemma and its corollary enable us to use the fact that $\mathbb{Z}[\omega]$ is a unique factorization domain to formulate the following definition.

Definition 10.3.16 *If γ is primary, then we can write $\gamma = (-1)^{k-1}\gamma_1\gamma_2\ldots\gamma_k$, where the γ_i are not necessarily distinct primary primes.* ♢

Definition 10.3.17 *Let $\alpha, \beta \in \mathbb{Z}[\omega]$ and assume that $\beta \not\equiv 0 \bmod (1-\omega)$. Assume also that $\beta = \beta_1\beta_2\ldots\beta_k$ is the prime factorization of β, where the β_i are not necessarily distinct primes of $\mathbb{Z}[\omega]$. Then*

$$\left[\frac{\alpha}{\beta}\right]_3 = \begin{cases} 1, & \text{if } \beta \text{ is a unit of } \mathbb{Z}[\omega] \\ (\alpha/\beta_1)_3(\alpha/\beta_2)_3\ldots(\alpha/\beta_k)_3, & \text{if } \beta \text{ is a nonunit.} \end{cases}$$

(Note that this is essentially the cubic analog to the Jacobi symbol.) $\diamondsuit$

Theorem 10.3.18 (The Law of Cubic Reciprocity) *Suppose π_1 and π_2 are relatively prime primary elements of $\mathbb{Z}[\omega]$, where $N(\pi_1), N(\pi_2) \neq 3$ and $N(\pi_1) \neq N(\pi_2)$. Then*

$$(\pi_2/\pi_1)_3 = (\pi_1/\pi_2)_3.$$

Before we prove this theorem, a couple of notes are in order. We have six units in $\mathbb{Z}[\omega]$, ± 1, $\pm\omega$, and $\pm\omega^2$, and this theorem doesn't specifically address how to deal with them, so we will look briefly at the cubic character of the units. Recall that $(-1)^3 = -1$, so $x^3 \equiv -1 \bmod \pi$ always has a solution. Thus $(-1/\pi)_3 = 1$ for all primes $\pi \in \mathbb{Z}[\omega]$. To evaluate $(\omega/\pi)_3$, we turn to Property 1 of the cubic residue character which indicates that

$$(\omega/\pi)_3 = \omega^{(N(\pi)-1)/3}.$$

Thus

$$(\omega/\pi)_3 = \begin{cases} 1, & N(\pi) \equiv 1 \bmod 9 \\ \omega, & N(\pi) \equiv 4 \bmod 9 \\ \omega^2, & N(\pi) \equiv 7 \bmod 9. \end{cases}$$

Proof: Assume that π_1 and π_2 are relatively prime primary elements in $\mathbb{Z}[\omega]$, such that $N(\pi_1), N(\pi_2) \neq 3$ and $N(\pi_1) \neq N(\pi_2)$. We need to consider three cases. Specifically, both π_1 and π_2 are rational, exactly one of π_1 or π_2 is rational and the other is complex, and both π_1 and π_2 are complex.

Suppose that π_1 and π_2 are distinct and are both rational. If one or both are not prime, we can apply Definition 10.3.17 to the non-prime denominators. To handle the non-prime numerators, Property 3 of cubic residue characters says that $(\alpha\beta/\pi)_3 = (\alpha/\pi)_3(\beta/\pi)_3$. Thus it is sufficient to prove the result for two rational primes. If π_1 and π_2 are both primary rational primes, then by Corollary 10.3.7, $(\pi_1/\pi_2)_3 = 1$ and $(\pi_2/\pi_1)_3 = 1$, so $(\pi_1/\pi_2)_3 = (\pi_2/\pi_1)_3$.

Suppose without loss of generality that π_1 is a rational prime and π_2 is a complex prime. By Theorem 10.1.6, $\pi_1 = q \equiv 2 \bmod 3$ and $\pi_2 = \pi$, where $N(\pi) = p$. Then by Corollary 10.3.13, we have

$$\begin{aligned} & \big(g_1(\chi_\pi)\big)^3 = p\pi && \text{(Corollary 10.3.13)} \\ \iff & \Big(\big(g_1(\chi_\pi)\big)^3\Big)^{(q^2-1)/3} = (p\pi)^{(q^2-1)/3} && \text{(Power Rule)} \\ \iff & \big(g_1(\chi_\pi)\big)^{q^2-1} = (p\pi)^{(q^2-1)/3}. && \text{(Properties of exponents)} \end{aligned}$$

Now if we consider this last equation modulo q, we have

$$\begin{aligned}
\big(g_1(\chi_\pi)\big)^{q^2-1} &\equiv (p\pi/q)_3 \bmod q && \text{(Theorem 10.3.5)} \\
&\equiv (p/q)_3(\pi/q)_3 \bmod q && \text{(Theorem 10.3.5)} \\
&\equiv 1 \cdot (\pi/q)_3 \bmod q. && \text{(Corollary 10.3.7)}
\end{aligned}$$

So

$$\big(g_1(\chi_\pi)\big)^{q^2-1} \equiv (\pi/q)_3 \bmod q \iff \big(g_1(\chi_\pi)\big)^{q^2} \equiv (\pi/q)_3 \cdot g_1(\chi_\pi) \bmod q.$$

Now, by definition of Gauss sums, we have

$$\begin{aligned}
\big(g_1(\chi_\pi)\big)^{q^2} &= \left(\sum_{t=0}^{p-1} \chi_\pi(t) \cdot \zeta^t\right)^{q^2} \\
&\equiv \sum_{t=0}^{p-1} \big(\chi_\pi(t)\big)^{q^2} \cdot \zeta^{q^2 t} \bmod q.
\end{aligned}$$

But $q \equiv 2 \bmod 3$, so $q^2 \equiv 1 \bmod 3$, and we can write $q^2 = 3k + 1$, for some k. We also know that $\chi_\pi(t)$ is a cubic character. We can apply these two ideas to our work above, which yields

$$\begin{aligned}
\big(g_1(\chi_\pi)\big)^{q^2} &\equiv \sum_{t=0}^{p-1} \big(\chi_\pi(t)\big)^{3k+1} \cdot \zeta^{q^2 t} \bmod q \\
&\equiv \sum_{t=0}^{p-1} \chi_\pi(t) \cdot \zeta^{q^2 t} \bmod q && (\chi_\pi(t) \text{ is a cubic character}) \\
&\equiv g_{q^2}(\chi_\pi) \bmod q. && \text{(Definition of Gauss Sum)}
\end{aligned}$$

Manipulating the right hand side of this last congruence yields

$$\begin{aligned}
g_{q^2}(\chi_\pi) &= \chi_\pi(q^{-2}) \cdot g_1(\chi_\pi) && \text{(Theorem 9.2.2)} \\
&= \chi_\pi(q^{-1}) \cdot \chi_\pi(q^{-1}) \cdot g_1(\chi_\pi) && (\chi \text{ is multiplicative}) \\
&= \overline{\chi_\pi(q)} \cdot \chi_\pi(q^{-1}) \cdot g_1(\chi_\pi) && \text{(Theorem 7.3.2)} \\
&= \chi_\pi(q^2) \cdot \chi_\pi(q^{-1}) \cdot g_1(\chi_\pi) && \text{(Theorem 10.3.6)} \\
&= \chi_\pi(q^2 \cdot q^{-1}) \cdot g_1(\chi_\pi) && (\chi \text{ is multiplicative}) \\
&= \chi_\pi(q) \cdot g_1(\chi_\pi). && (q^2 \cdot q^{-1} = q)
\end{aligned}$$

So now we have

$$\big(g(\chi_\pi)\big)^{q^2} \equiv \chi_q(\pi) \cdot g_1(\chi_\pi) \bmod q \text{ and}$$

$$\big(g(\chi_\pi)\big)^{q^2} \equiv g_{q^2}(\chi_\pi) \bmod q \equiv \chi_\pi(q) \cdot g_1(\chi_\pi) \bmod q,$$

and combining the two results yields $\chi_q(\pi) \cdot g_1(\chi_\pi) \equiv \chi_\pi(q) \cdot g_1(\chi_\pi) \bmod q$.

If we multiply both sides of this last congruence by $g_1\big(\overline{\chi}_\pi\big)$, then

$$\begin{aligned}
&\chi_q(\pi) \cdot g_1(\chi_\pi) \cdot g_1\big(\overline{\chi}_\pi\big) \equiv \chi_\pi(q) \cdot g_1(\chi_\pi) \cdot g_1\big(\overline{\chi}_\pi\big) \bmod q \\
\iff &\chi_q(\pi) \cdot p \equiv \chi_\pi(q) \cdot p \bmod q && \text{(Theorem 9.2.3)} \\
\iff &\chi_q(\pi) \equiv \chi_\pi(q) \bmod q. && \text{(Theorem 4.3.20)}
\end{aligned}$$

It follows that $\chi_q(\pi) = \chi_\pi(q)$, as desired.

Suppose finally that π_1 and π_2 are both primary complex primes. Assume that $N(\pi_1) = p_1 \equiv 1 \bmod 3$ and $N(\pi_2) = p_2 \equiv 1 \bmod 3$. Let $\gamma_1 = \overline{\pi}_1$

and $\gamma_2 = \overline{\pi}_2$. Then γ_1 and γ_2 are also primary, $p_1 = \pi_1\gamma_1$, and $p_2 = \pi_2\gamma_2$. So we have

$$\begin{aligned}
&\big(g_1(\chi_{\gamma_1})\big)^3 = p_1\gamma_1 && \text{(Corollary 10.3.13)}\\
\Longrightarrow &\Big(\big(g_1(\chi_{\gamma_1})\big)^3\Big)^{(N(\pi_2)-1)/3} = (p_1\gamma_1)^{(N(\pi_2)-1)/3} && \text{(Power Rule)}\\
\Longleftrightarrow &\big(g_1(\chi_{\gamma_1})\big)^{N(\pi_2)-1} = (p_1\gamma_1)^{(N(\pi_2)-1)/3} && \text{(Properties of exponents)}\\
\Longleftrightarrow &\big(g_1(\chi_{\gamma_1})\big)^{p_2-1} = (p_1\gamma_1)^{(N(\pi_2)-1)/3} && (N(\pi_2) = p_2)\\
\Longleftrightarrow &\big(g_1(\chi_{\gamma_1})\big)^{p_2-1} \equiv (p_1\gamma_1/\pi_2)_3 \bmod \pi_2 && \text{(Theorem 10.3.5)}\\
\Longleftrightarrow &\big(g_1(\chi_{\gamma_1})\big)^{p_2-1} \equiv \chi_{\pi_2}(p_1\gamma_1) \bmod \pi_2.
\end{aligned}$$

Thus we have

$$\big(g_1(\chi_{\gamma_1})\big)^{p_2-1} \equiv \chi_{\pi_2}(p_1\gamma_1) \bmod \pi_2 \iff \big(g_1(\chi_{\gamma_1})\big)^{p_2} \equiv g_1(\chi_{\gamma_1})\chi_{\pi_2}(p_1\gamma_1) \bmod \pi_2.$$

By the definition of Gauss sum,

$$\begin{aligned}
\big(g_1(\chi_{\gamma_1})\big)^{p_2} &= \left(\sum_{t=0}^{p_2-1} \chi_{\gamma_1}(t)\zeta^t\right)^{p_2}\\
&\equiv \sum_{t=0}^{p_2-1} \big(\chi_{\gamma_1}(t)\big)^{p_2}\zeta^{p_2 t} \bmod \pi_2.
\end{aligned}$$

But $p_2 \equiv 1 \bmod 3$, so $p_2 = 3k+1$, for some $k \in \mathbb{Z}$. Also, $\chi_{\gamma_1}(t)$ is a cube root of 1, so

$$\begin{aligned}
\big(g_1(\chi_{\gamma_1})\big)^{p_2} &\equiv \big(\chi_{\gamma_1}(t)\big)^{3k+1}\zeta^{p_2 t} \bmod \pi_2 && \text{(Definition of Gauss Sum)}\\
&\equiv \sum_{t=0}^{p_2-1} \chi_{\gamma_1}(t)\zeta^{p_2 t} \bmod \pi_2 && (\chi_{\gamma_1}(t) \text{ is a cubic character})\\
&\equiv g_{p_2}(\chi_{\gamma_1}) \bmod \pi_2.
\end{aligned}$$

By Theorem 9.2.2, we have

$$\begin{aligned}
g_{p_2}(\chi_{\gamma_1}) &= \chi_{\gamma_1}\left(p_2^{-1}\right) \cdot g_1(\chi_{\gamma_1}) \\
&= \overline{\chi_{\gamma_1}(p_2)} \cdot g_1(\chi_{\gamma_1}) && \text{(Theorem 7.3.2)} \\
&= \overline{(p_2/\gamma_1)_3} \cdot g_1(\chi_{\gamma_1}) && \text{(Definition of } \chi_{\gamma_1}(p_2)\text{)} \\
&= \left(p_2^2/\gamma_1\right)_3 \cdot g_1(\chi_{\gamma_1}) && \text{(Theorem 10.3.6)} \\
&= \chi_{\gamma_1}\left(p_2^2\right) \cdot g_1(\chi_{\gamma_1}). && \text{(Definition of } \chi_{\gamma_1}\left(p_2^2\right)\text{)}
\end{aligned}$$

So now we have

$$\left(g_1(\chi_{\gamma_1})\right)^{p_2} \equiv g_1(\chi_{\gamma_1}) \cdot \chi_{\pi_2}(p_1\gamma_1) \bmod \pi_2$$

and

$$\left(g_1(\chi_{\gamma_1})\right)^{p_2} \equiv g_1(\chi_{\gamma_1}) \cdot \chi_{\gamma_1}\left(p_2^2\right) \bmod \pi_2,$$

and combining the two results yields

$$\begin{aligned}
& g_1(\chi_{\gamma_1}) \cdot \chi_{\pi_2}(p_1\gamma_1) \equiv g_1(\chi_{\gamma_1}) \cdot \chi_{\gamma_1}\left(p_2^2\right) \bmod \pi_2 \\
\iff & g_1(\chi_{\gamma_1}) \cdot g_1\left(\overline{\chi_{\gamma_1}}\right) \cdot \chi_{\pi_2}(p_1\gamma_1) \equiv g_1(\chi_{\gamma_1}) \cdot g_1\left(\overline{\chi_{\gamma_1}}\right) \cdot \chi_{\gamma_1}\left(p_2^2\right) \bmod \pi_2 \\
\iff & p_1 \cdot \chi_{\pi_2}(p_1\gamma_1) \equiv p_1 \cdot \chi_{\gamma_1}(p_2^2) \bmod \pi_2 \\
\iff & \chi_{\pi_2}(p_1\gamma_1) \equiv \chi_{\gamma_1}\left(p_2^2\right) \bmod \pi_2.
\end{aligned}$$

By a symmetric argument, $\chi_{\pi_1}(p_2\pi_2) \equiv \chi_{\pi_2}(p_1^2) \bmod \pi_1$. So now we have

$$\chi_{\pi_2}(p_1\gamma_1) \equiv \chi_{\gamma_1}\left(p_2^2\right) \bmod \pi_2 \tag{10.1}$$

and

$$\chi_{\pi_1}(p_2\pi_2) \equiv \chi_{\pi_2}\left(p_1^2\right) \bmod \pi_1. \tag{10.2}$$

Note that the values of the characters in Congruences (10.1) and (10.2) are in $\{1, \omega, \omega^2\}$, so congruence modulo π_2 and π_1 respectively implies that we have equality, therefore we can drop the modulus.

By Theorem 10.3.6,

$$\begin{aligned}
\chi_{\gamma_1}\left(p_2^2\right) &= \overline{\chi_{\gamma_1}(p_2)} \\
&= \chi_{\overline{\gamma_1}}(\overline{p_2}) && \text{(Theorem 10.3.6)} \\
&= \chi_{\pi_1}(p_2),
\end{aligned}$$

because $\gamma_1 = \overline{\pi_1} \Rightarrow \overline{\gamma_1} = \pi_1$ and $\overline{p_2} = p_2$. Thus, if we start with Equation (10.1) and multiply both sides of the equation by $\chi_{\pi_1}(\pi_2)$, we have

$$\begin{aligned}
\chi_{\pi_1}(\pi_2) \cdot \chi_{\pi_2}(p_1\gamma_1) &= \chi_{\pi_1}(\pi_2) \cdot \chi_{\gamma_1}\left(p_2^2\right) \\
&= \chi_{\pi_1}(\pi_2) \cdot \chi_{\pi_1}(p_2) && \left(\chi_{\gamma_1}\left(p_2^2\right) = \chi_{\pi_1}(p_2)\right) \\
&= \chi_{\pi_1}(p_2\pi_2) && (\chi_{\pi_1} \text{ is multiplicative}) \\
&= \chi_{\pi_2}\left(p_1^2\right) && \text{(Equation (10.2))} \\
&= \chi_{\pi_2}(p_1 \cdot \pi_1\gamma_1) && (p_1 = \gamma_1\pi_1) \\
&= \chi_{\pi_2}(\pi_1) \cdot \chi_{\pi_2}(p_1\gamma_1). && (\chi_{\pi_2} \text{ is multiplicative})
\end{aligned}$$

Thus,

$$\chi_{\pi_1}(\pi_2)\chi_{\pi_2}(p_1\gamma_1) = \chi_{\pi_2}(\pi_1)\chi_{\pi_2}(p_1\gamma_1).$$

Since by definition of cubic characters, $\chi_{\pi_2}(p_1\gamma_1) \neq 0$, we can cancel the common factor, and we have

$$\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1),$$

as desired. ∎

Theorem 10.3.19 (Supplement to the Cubic Reciprocity Law) *Let π be a primary prime. Then* $\left(\frac{1-\omega}{\pi}\right)_3 = \omega^{2m}$.

Proof: We need to consider two cases. First, assume that $\pi = q$ is a rational primary prime. Let $q = 3m - 1$ and observe that

$$\begin{aligned}
(1-\omega)^2 &= (1-\omega)(1-\omega) \\
&= 1 - 2\omega + \omega^2 && \text{(Distributive Property)} \\
&= 1 - 2\omega - 1 - \omega && (\omega^2 = -1 - \omega) \\
&= -3\omega. && \text{(Arithmetic)}
\end{aligned}$$

Thus,

$$\begin{aligned}
\big(\chi_q(1-\omega)\big)^2 &= \chi_q\big((1-\omega)^2\big) && \text{(Theorem 10.3.6)}\\
&= \chi_q(-3\omega) && ((1-\omega)^2 = -3\omega)\\
&= \big(-3\omega/q\big)_3 && \text{(Definition of } \chi_q)\\
&= \big(-3/q\big)_3\big(\omega/q\big)_3 && \text{(Theorem 10.3.5)}\\
&= \big(\omega/q\big)_3 && \text{(Corollary 10.3.7)}\\
&= \omega^{(N(q)-1)/3} && \text{(Theorem 10.3.5)}\\
&= \omega^{(q^2-1)/3}. && (N(q) = q^2)
\end{aligned}$$

So we have

$$\big(\chi_q(1-\omega)\big)^2 = \omega^{(q^2-1)/3}.$$

Squaring both sides of this equation yields

$$\big(\chi_q(1-\omega)\big)^4 = \big(\omega^{(q^2-1)/3}\big)^2 = \omega^{2(q^2-1)/3}.$$

Now, $q^2 - 1 = 9m^2 - 6m$, so

$$\begin{aligned}
\frac{2(q^2-1)}{3} &= \frac{2(9m^2-6m)}{3}\\
&= 6m^2 - 4m\\
&\equiv -4m \bmod 3\\
&\equiv 2m \bmod 3.
\end{aligned}$$

We will need part of this result later in the proof, so we label it to make notation easier.

$$6m^2 - 4m \equiv 2m \bmod 3 \tag{10.3}$$

Also, note that

$$\big(\chi_q(1-\omega)\big)^4 = \big(\chi_q(1-\omega)\big)^3 \cdot \chi_q(1-\omega).$$

But by definition, $\chi_q(\alpha) = 1, \omega,$ or ω^2, for any appropriate α, and $1^3 = 1$, $\omega^3 = 1$, and $(\omega^2)^3 = (\omega^3)^2 = 1^2 = 1$, so $\big(\chi_q(1-\omega)\big)^4 = \chi_q(1-\omega)$. Thus,

$$\big(\chi_q(1-\omega)\big)^4 = \omega^{2(q^2-1)/3} \iff \chi_q(1-\omega) = \omega^{2m},$$

as desired.

Now suppose that $\pi = a + b\omega$ is a primary complex prime. Then $a \equiv 2 \equiv -1 \bmod 3$ and $b \equiv 0 \bmod 3$, so let $a = 3m - 1$ and $b = 3n$, for some $m, n \in \mathbb{Z}$. Note that since $a \equiv 2 \bmod 3$, a is primary by definition. If a is not prime, then by Corollary 10.3.15, we can factor a into the product $a = (-1)^{k-1} a_1 a_2 \dots a_k$, where each a_i is a primary prime. Thus, we can assume without loss of generality that a is a primary rational prime. By a similar argument, we can also assume that $a + b$ is a primary rational prime. Notice also that $b \neq 0$, since π is a complex prime, so a and $a+b$ and a and $a+b\omega$ are relatively prime. Likewise, b and $a + b$ are also relatively prime since $a \neq 0$.

We need to perform a few computations that will be helpful in this proof. First, note that

$$\begin{aligned}\frac{N(a)-1}{3} &= \frac{(3m-1)^2-1}{3} && (a = 3m-1)\\ &= \frac{9m^2-6m+1-1}{3}\\ &= 3m^2-2m\\ &\equiv m \bmod 3.\end{aligned}$$

To make notation easier when we proceed with the proof, we label this result.

$$\frac{N(a)-1}{3} \equiv m \bmod 3. \tag{10.4}$$

Second,

$$a + b\omega \equiv b\omega \bmod a. \tag{10.5}$$

Next,

$$\begin{aligned}& a + b\omega \equiv 0 \bmod \pi\\ \Longrightarrow\ & a - a\omega + a\omega + b\omega \equiv 0 \bmod \pi && (-a\omega + a\omega = 0)\\ \Longrightarrow\ & a - a\omega \equiv -(a+b)\omega \bmod \pi.\end{aligned}$$

$$a - a\omega \equiv -(a+b)\omega \bmod \pi \tag{10.6}$$

Since $N(\pi) = p$,

$$p = a^2 - ab + b^2 \qquad \text{(Definition of } N(\pi)\text{)}$$

$$\iff (3m-1)^2 - (3m-1)(3n) + (3n)^2 = p \qquad (a = 3m-1,\ b = 3n)$$

$$\iff 9m^2 - 6m + 1 - 9mn + 3n + 9n^2 = p \qquad \text{(Distributive Property)}$$

$$\iff \frac{p-1}{3} = 3m^2 - 2m - 3mn + n + 3n^2$$

$$\iff \frac{p-1}{3} \equiv -2m + n \bmod 3.$$

$$\frac{p-1}{3} \equiv -2m + n \bmod 3 \tag{10.7}$$

Recall that since $(-1)^3 = 1$, for any $\gamma \in \mathbb{Z}[\omega]$,

$$\left(\frac{-1}{\gamma}\right)_3 = 1. \tag{10.8}$$

Finally, we compute $a + b\omega$ modulo $a + b$.

$$a + b\omega \equiv bw - b \bmod (a+b)$$

$$\equiv -b(1-\omega) \bmod (a+b).$$

$$a + b\omega \equiv -b(1-\omega) \bmod (a+b) \tag{10.9}$$

For each of notation in the justification of the computations to come, we abbreviate cubic residue characters as CRC. So for example, if we are referring to Property 3 of cubic residue characters, then we will use "Property 3 of CRC" as the reason for the computation. We also temporarily abbreviate the Law of Cubic Reciprocity as "LCR".

Now we are in a position to examine $\left(\frac{1-\omega}{\pi}\right)_3$.

$$\begin{aligned}
\left(\frac{1-\omega}{a+b\omega}\right)_3 &= \left(\frac{b}{a}\right)_3 \left(\frac{1-\omega}{a+b\omega}\right)_3 && ((b/a)_3 = 1 \text{ by Lemma 10.3.12}) \\
&= \left(\frac{b\omega^3}{a}\right)_3 \left(\frac{1-\omega}{a+b\omega}\right)_3 && (\omega^3 = 1) \\
&= \left(\frac{\omega^2}{a}\right)_3 \left(\frac{b\omega}{a}\right)_3 \left(\frac{1-\omega}{a+b\omega}\right)_3 && (\text{Property 3 of CRC}) \\
&= \left(\frac{\omega}{a}\right)_3^2 \left(\frac{a+b\omega}{a}\right)_3 \left(\frac{1-\omega}{a+b\omega}\right)_3 && (\text{Theorem 10.3.6; 10.5}) \\
&= \omega^{2(N(a)-1)/3} \left(\frac{a}{a+b\omega}\right)_3 \left(\frac{1-\omega}{a+b\omega}\right)_3 \\
& && (\text{Property 1 of CRC; LCR}) \\
&= \omega^{2m} \left(\frac{a-a\omega}{a+b\omega}\right)_3 && (10.4; \text{ Property 3 of CRC}) \\
&= \omega^{2m} \left(\frac{-(a+b)\omega}{a+b\omega}\right)_3 && (10.6) \\
&= \omega^{2m} \left(\frac{-1}{a+b\omega}\right)_3 \left(\frac{\omega}{a+b\omega}\right)_3 \left(\frac{a+b}{a+b\omega}\right)_3 && (\text{Property 3 of CRC}) \\
&= \omega^{2m} \cdot (1) \cdot \omega^{(N(\pi)-1)/3} \left(\frac{a+b}{a+b\omega}\right)_3 && (10.8; \text{ Property 1 of CRC}) \\
&= \omega^{2m} \cdot \omega^{-2m+n} \left(\frac{a+b\omega}{a+b}\right)_3 && (10.7; \text{ LCR}) \\
&= \omega^n \left(\frac{-b(1-\omega)}{a+b}\right)_3 && (10.9) \\
&= \omega^n \left(\frac{-1}{a+b}\right)_3 \left(\frac{b}{a+b}\right)_3 \left(\frac{1-\omega}{a+b}\right)_3 && (\text{Property 3 of CRC}) \\
&= \omega^n \cdot (1) \cdot (1) \left(\frac{1-\omega}{a+b}\right)_3 . && (10.8; \text{ Lemma 10.3.12})
\end{aligned}$$

Now, we need to work on $\left(\frac{1-\omega}{a+b}\right)_3$. First note that

$$\begin{aligned}
2 \cdot \frac{N(a+b)-1}{3} &= \frac{2\big((3m-1+3n)^2-1\big)}{3} \\
&= \frac{2(9m^2-6m+18mn+1-6n+9n^2-1)}{3} \\
&= 2\left(3m^2-2m+6mn-2n+3n^2\right) \\
&= 6m^2-4m+12mn-4n+6n^2 \\
&\equiv 2(m+n) \bmod 3.
\end{aligned}$$

Also, any cubic character has order 3, so

$$\begin{aligned}
\left(\frac{1-\omega}{a+b}\right)_3 &= 1 \cdot \left(\frac{1-\omega}{a+b}\right)_3 \\
&= \left(\frac{1-\omega}{a+b}\right)_3^3 \left(\frac{1-\omega}{a+b}\right)_3 \\
&= \left(\frac{1-\omega}{a+b}\right)_3^4 \\
&= \left(\frac{(1-\omega)^2}{a+b}\right)_3^2 && \text{(Theorem 10.3.6)} \\
&= \left(\frac{-3\omega}{a+b}\right)_3^2 \\
&= \left(\frac{-1}{a+b}\right)_3^2 \left(\frac{3}{a+b}\right)_3^2 \left(\frac{\omega}{a+b}\right)_3^2 && \text{(Property 3 of CRC)} \\
&= (1)^2 \cdot (1)^2 \cdot \left(\omega^{(N(a+b)-1)/3}\right)^2 \\
& && \text{(10.8; Lemma 10.3.12; Property 1 of CRC)} \\
&= \omega^{2(m+n)}.
\end{aligned}$$

Now returning to our calculations, we have

$$\begin{aligned}\left(\frac{1-\omega}{a+b\omega}\right)_3 &= \omega^n \left(\frac{1-\omega}{a+b}\right)_3 \\ &= \omega^n \cdot \omega^{2(m+n)} \\ &= \omega^{2m+3n} \\ &= \omega^{2m},\end{aligned}$$

since $2m + 3n \equiv 2m \bmod 3$. ∎

We want to look at an example of cubic reciprocity at work, but before we begin the example, we need to revisit some concepts that we haven't seen for a while. Recall that in Example 5.4.4, we showed that there is a division algorithm for the elements of $\mathbb{Z}\omega]$. This means that given $\alpha, \beta \in \mathbb{Z}[\omega]$, we can express α as $\alpha = \beta\gamma + \rho$, where γ and ρ are unique and $N(\rho)$ is either 0 or is less than $N(\beta)$. But the more subtle consequence is that if $\alpha = \beta\gamma + \rho$, then $\alpha \equiv \rho \bmod \beta$, and we need to be able to do modular arithmetic in this setting to utilize all of the properties of cubic residue characters.

We offer a quick recap of the division algorithm for $\mathbb{Z}[\omega]$ before we begin our example. Suppose $\alpha = a + b\omega, \beta = c + d\omega \neq 0 \in \mathbb{Z}[\omega]$. Our goal is to find the particular γ and ρ such that $\alpha = \beta\gamma + \rho$. The first step is to represent $\dfrac{\alpha}{\beta} = \dfrac{ac - ac + bd}{c^2 - cd + d^2} + \dfrac{bc - ad}{c^2 - cd + d^2}\omega$. In other words, we said that this is $\dfrac{\alpha}{\beta} = r + s\omega$. The second step is to approximate r and s and then choose integers t and u so that they are as close as possible to the approximate values

of r and s respectively. Then $\gamma = t + u\omega$ and $\rho = \alpha - \beta\gamma$. We solve for ρ and check to be sure that the norm of ρ is either 0 or is smaller than the norm of β. If it is, then we have $\alpha = \beta\gamma + \rho$.

Example 10.3.20 Consider $x^3 \equiv (-9+4)\omega \bmod (2-9\omega)$. We want to explore the solvability of this congruence. If a solution exists, then the cubic residue character $\left(\frac{-9+4\omega}{2-9\omega}\right)_3$ will be equal to 1. Before we start our computations, note that $N(-9+4\omega) = 133$, so $-9+4\omega$ is not prime in $\mathbb{Z}[\omega]$. On the other hand, $N(2-9\omega) = 103$, and $2-9\omega \equiv 2 \bmod 3$, so $2-9\omega$ is prime, and is in fact primary.

Step one is to use the division algorithm with so that we can start applying properties of the cubic residue character.

$$\begin{aligned}\frac{-9+4\omega}{2-9\omega} &= \frac{-18-81-36}{103} + \frac{8-81}{103}\omega \qquad \text{(Division algorithm in } \mathbb{Z}[\omega]\text{)} \\ &= \frac{-135}{103} - \frac{73}{103}\omega\end{aligned}$$

Thus we have $r = \frac{-135}{103} \approx -1.31$ and $s = \frac{-73}{103} \approx -0.709$. Let $t = -1$ and $u = -1$. Then $\gamma = -1 - \omega$ and

$$\begin{aligned}\rho &= (-9+4\omega) - (2-9\omega)(-1-\omega) && (\rho = \alpha - \beta\gamma) \\ &= -9 + 4\omega + 2 + 2\omega - 9\omega + 9(1+\omega) && \text{(Distributive Property)} \\ &= 2 + 6\omega.\end{aligned}$$

$N(\rho) = 28$ and $N(\beta) = 103$, so $-9+4\omega \equiv 2+6\omega \bmod (2-9\omega)$.

Now we can begin to evaluate the cubic residue character.

$$\left(\frac{-9+4\omega}{2-9\omega}\right)_3 = \left(\frac{2+6\omega}{2-9\omega}\right)_3 \qquad \text{(Property 4 of cubic residue characters)}$$

$$= \left(\frac{2}{2-9\omega}\right)_3 \left(\frac{1+3\omega}{2-9\omega}\right)_3$$

(Property 3 of cubic residue characters)

$$= \left(\frac{2-9\omega}{2}\right)_3 \left(\frac{1+3\omega}{2-9\omega}\right)_3$$

(Theorem 10.1.6; Law of Cubic Reciprocity)

At this point, note that $2-9\omega$ is a primary prime and 2 is a rational primary prime, but while $1+3\omega$ is prime, it is not primary. Before we try to do anything with $1+3\omega$, we need to reduce $2-9\omega$ modulo 2. The division algorithm for $\mathbb{Z}[\omega]$ yields

$$\frac{2-9\omega}{2+0\omega} = \frac{4}{4} - \frac{9}{2}\omega,$$

so $r=1$ and $s=-4.5$. We choose $t=1$ and $u=-5$, so $\gamma = 1-5\omega$. Then

$$\rho = (2-9\omega) - (2)(1-5\omega) \qquad (\rho = \alpha - \beta\gamma)$$

$$= \omega.$$

$N(\rho)=1$ and $N(\beta)=103$, so $2-9\omega \equiv \omega \bmod 2$. Incidentally, note that in this case we have $s=-4.5$, and we chose $u=-5$, but if one chooses $u=-4$ instead, then we would get $\rho=-\omega$, so it would work equally well, as they differ only by a unit.

Before we return to manipulating the cubic residue character, we examine $1+3\omega$. It is a prime and is congruent to 1 modulo 3, so by Theorem 10.3.9,

we know that exactly one of its six associates is primary. It can easily be seen that $-1-3\omega$ is primary, so we know that if we multiply $1+3\omega$ by -1, we will have a primary prime to work with. However, we must do this in such a way that we do not change the value of the equation we are working on. We know that we can multiply the equation by 1 and not change it, so observe that since $(-1)^3 = -1$, -1 is always a cubic residue. Thus the particular value of 1 that we choose to multiply by is going to be the cubic residue character $\left(\frac{-1}{2-9\omega}\right)_3 = 1$. So returning to our computations, we have

$$\begin{aligned}
\left(\frac{-9+4\omega}{2-9\omega}\right)_3 &= \left(\frac{\omega}{2}\right)_3 \left(\frac{1+3\omega}{2-9\omega}\right)_3 \quad \text{(Property 4 of cubic residue characters)} \\
&= \omega^{(N(2)-1)/3} \left(\frac{-1}{2-9\omega}\right)_3 \left(\frac{1+3\omega}{2-9\omega}\right)_3 \\
&\qquad \text{(Property 1 of cubic residue characters; Multiplication by 1)} \\
&= \omega \left(\frac{-1-3\omega}{2-9\omega}\right)_3 \quad \text{(Property 3 of cubic residue characters)} \\
&= \omega \left(\frac{2-9\omega}{-1-3\omega}\right)_3 \quad \text{(Law of Cubic Reciprocity)}
\end{aligned}$$

Now we want to reduce $2-9\omega$ modulo $(-1-3\omega)$, so we look to the division algorithm for assistance again.

$$\frac{2-9\omega}{-1-3\omega} = \frac{31}{7} + \frac{15}{7}\omega,$$

so $r = \frac{31}{7} \approx 4.43$ and $s = \frac{15}{7} \approx 2.14$. Let $t = 4$ and $s = 2$, then $\gamma = 4 + 2\omega$

and

$$\rho = (2 - 9\omega) - (-1 - 3\omega)(4 + 2\omega) \qquad (\rho = \alpha - \beta\gamma)$$

$$= -\omega.$$

$N(-\omega) = 1$ and $N(\beta) = 7$, so $2 - 9\omega \equiv -\omega \bmod (-1 - 3\omega)$. Thus our computation is now

$$\left(\frac{-9 + 4\omega}{2 - 9\omega}\right)_3 = \omega \left(\frac{-\omega}{-1 - 3\omega}\right)_3 \qquad \text{(Property 4 of cubic residue characters)}$$

$$= \omega \cdot \omega^{(N(-1-3\omega)-1)/3} \qquad \text{(Property 1 of cubic residue characters)}$$

$$= \omega \cdot \omega^2$$

$$= 1.$$

Recall that Property 2 of cubic residue characters states that $(\alpha/\pi)_3 = 1$ if and only if $x^3 \equiv \alpha \bmod \pi$ is solvable, so it follows that the congruence $x^3 \equiv -9 + 4\omega \bmod (2 - 9\omega)$ has a solution. □

10.4 The Cubic Character of 2

We want to explore the cubic character of 2, since it is a special prime.

Theorem 10.4.1 *Let π be primary. Then $x^3 \equiv 2 \bmod \pi$ is solvable if and only if $\pi \equiv 1 \bmod 2$, or in other words, if $\pi = a + b\omega$, where $a \equiv 1 \bmod 2$ and $b \equiv 0 \bmod 2$.*

Proof: If $\pi = q$ is a primary rational prime, then by Lemma 10.3.12, every integer is a cubic residue modulo q. Thus it is sufficient to prove that the result holds for a primary prime π.

Suppose that $\pi = a + b\omega$ is a primary prime. By the Law of Cubic Reciprocity, $(2/\pi)_3 = (\pi/2)_3$. Now,

$$\begin{aligned} \pi^{(N(2)-1)/3} &= \pi^{(4-1)/3} && (N(2) = 2^2 = 4) \\ &= \pi \\ &\equiv (\pi/2)_3 \bmod 2. && \text{(Theorem 10.3.5)} \end{aligned}$$

But $(\pi/2)_3 = 1$ if and only if $x^3 \equiv \pi \bmod 2$ is solvable, by Theorem 10.3.5. However, $x^3 \equiv \pi \bmod 2$ is solvable if and only if $\pi \equiv 1 \bmod 2$. Thus $(\pi/2)_3 = 1$ if and only if $\pi \equiv 1 \bmod 2$, and since $(\pi/2)_3 = (2/\pi)_3$, it follows that $(2/\pi)_3 = 1$ if and only if $\pi \equiv 1 \bmod 2$ as well. Therefore, $x^3 \equiv 2 \bmod \pi$ is solvable if and only if $\pi \equiv 1 \bmod 2$. ∎

Theorem 10.4.2 *If $p \equiv 1 \bmod 3$, then $x^3 \equiv 2 \bmod p$ is solvable if and only if there are integers C and D such that $p = C^2 + 27D^2$.*

Proof: Let $\pi = a + b\omega$ and $N(\pi) = p = a^2 - ab + b^2$. Suppose that $x^3 \equiv 2 \bmod p$ is solvable. Then $x^3 \equiv 2 \bmod \pi$ is also solvable, so $\pi \equiv 1 \bmod 2$, by Theorem 10.4.1, which implies that $a \equiv 1 \bmod 2$ and $b \equiv 0 \bmod 2$. From work in Chapter 9, we know that $4p = (2a - b)^2 + 3b^2$. Set $A = 2a - b$ and $B = \dfrac{b}{3}$. Then $4p = A^2 + 27B^2$, and by Theorem 9.3.6, we know that A and

B are unique integers up to sign. Now, since $b \equiv 0 \bmod 2$, it must be the case that b is even. But B is an integer, so b is also a multiple of 3. Let $b = (2m)(3n)$. Then $\frac{6mn}{3} = 2mn$, for integers m and n, and it follows that B is also even. But $4 \mid (A^2 + 27B^2)$, so A is also even. Now let $C = \frac{A}{2}$ and $D = \frac{B}{2}$. Then $p = C^2 + 27D^2$, as desired.

Suppose now that $p = C^2 + 27D^2$, for integers C and D. Then

$$\begin{aligned} 4p &= 4C^2 + 4 \cdot 27D^2 \\ &= (2C)^2 + 27(2D)^2. \end{aligned}$$

By the uniqueness argument of Theorem 9.3.6, $B = \pm 2D$, which implies that B is even. But if B is even, then b is also even. So we have $b \equiv 0 \bmod 2$, so $\pi \equiv 1 \bmod 2$, since π is not a multiple of 2. Thus $x^3 \equiv 2 \bmod \pi$ is solvable.

We know that $\frac{\mathbb{Z}[\omega]}{\pi\mathbb{Z}[\omega]}$ contains $N(\pi) = p$ elements. By Theorem 10.2.1, there is some integer a such that $a^3 \equiv 2 \bmod \pi$. This means that $\pi \mid (a^3 - 2)$. But then $\overline{\pi} \mid (a^3 - 2)$ as well, and $\pi\overline{\pi} = p \mid (a^3 - 2)^2$, so $p \mid (a^3 - 2)$. It follows that $a^3 \equiv 2 \bmod p$, as desired. ∎

10.5 Where do we go from here?

We have spent a lot of time developing the concepts of quadratic and cubic reciprocity. They have some similarities, in that each of them plays a key role in determining whether or not solutions to quadratic and cubic congruences exist

respectively. Both of them also have a special symbol, the Legendre symbol for quadratics and the cubic residue character for cubics. The properties for the symbols are similar, although they aren't quite identical. One big difference that we saw when we defined the cubic residue character, is that its outputs are not as overtly helpful as the outputs for the Legendre symbol. When we evaluate a Legendre symbol, we either come up with 1, which means that our congruence has a solution, or we get -1, which means we do not have a solution. In contrast, the outputs for the cubic residue character can be 1, ω, or ω^2, and only the output of 1 really tells us anything useful. But even that difference is not all that monumental, in the scheme of things. The most obvious difference, at least to this author, is the amount of work that is involved in working with the cubic reciprocity examples verses their quadratic counterparts. Everything in the cubic setting seems to be magnified by some large power, and nothing is as "simple" to compute there, as it is when working in the ordinary integers. For example, the division algorithm in $\mathbb{Z}$ is pretty straightforward, and we have all been using it for many years. But the division algorithm in $\mathbb{Z}[\omega]$ is just flat out weird, and it can get rather time consuming, especially when one has to use it repeatedly. It is also quite an exercise just to think about notions of primeness in $\mathbb{Z}[\omega]$, whereas it's almost trivial to think about primeness in the integers, because we have been exposed to that idea for a very long time.

One idea that we developed in the quadratic reciprocity chapter is the Jacobi symbol. It allows us to deal with the congruence $x^2 \equiv a \bmod n$, where n is not prime. This symbol came along with its own set of properties, and it greatly expanded the set of congruences we could examine. We also had some discussion about how using the Jacobi symbol to evaluate the solvability of $x^2 \equiv a \bmod n$ is akin to breaking the congruence into a system of congruences. In order for the initial congruence to have a solution, each of the congruences in the system must necessarily be solvable. This discussion came up because of the ambiguity of the output of the Jacobi symbol. An output of 1 doesn't really tell us anything at all, as we saw when we evaluated $[2/63]$. The symbol gave us a result of 1, but we showed that $x^2 \equiv 2 \bmod 63$ is in fact not solvable. So while the Jacobi symbol was helpful and gave us more tools to work with, we had to use caution not to get carried away with assumptions about what its outputs meant in terms of solvability. There is a similar notion for the cubic congruences, although we just barely touched on it. In the books we used as references, this idea was not very developed, so we did not spend a lot of time on it, but Definition 10.3.17 presents the basic idea.

Another difference between quadratic and cubic reciprocity comes with the theorems themselves. In the Law of Quadratic Reciprocity, it is required that we have distinct odd primes, p and q. In the Law of Cubic Reciprocity, however, it is only necessary that π_1 and π_2 be relatively prime to do the actual

"flipping" within the symbol.

Some of the ideas are pretty similar and some are very different, but both reciprocities are interesting, at least to this author. There are higher order reciprocity laws as well. Biquadratic, or quartic, reciprocity takes place in the ring of Gaussian integers, $\mathbb{Z}[i]$. It is noted in [8] that "the basic idea is the same as in the cubic case, although the details are more extensive". So perhaps there is a similar magnification in the amount of work required between cubic and quartic reciprocities as there is between quadratic and cubic reciprocities. Interestingly enough, the cases for rational primes and complex primes in biquadratic reciprocity are split completely apart, and in fact are handled in separate sections of [8]. The rational primes come along with their own definitions and theorems and it looks like the Law of Biquadratic Reciprocity is actually different depending on which primes one is working with. Many generalizations have arisen from quadratic reciprocity, including Eisenstein reciprocity, Artin reciprocity, and Kummer reciprocity [20]. These three reciprocities seem to involve computations on various ideals, rather than numbers. There are many others, and in fact, they are too numerous to mention individually. So it seems that the answer to the question "where do we go from here?" is not particularly easy to answer, as there are many directions one can go for further studies in reciprocity.

Bibliography

[1] B. C. BERNDT, R. J. EVANS, and K. S. WILLIAMS *Gauss and Jacobi Sums.* John Wiley & Sons, Inc., New York, 1998.

[2] U. DUDLEY *Elementary Number Theory, 2nd Edition.* W. H. Freeman and Company, New York, 1978.

[3] D. S. DUMMIT and R. M. FOOTE *Abstract Algebra, 3rd Edition.* John Wiley & Sons, Inc., Hoboken, NJ, 2004.

[4] G. EISENSTEIN. Nachtrag zum kubischen Reciprocitätssatze. *J. Reine und Agnew. Math.,* 28 (1844), 28-35.

[5] EUCLID *The Thirteen Books of the Elements, Vol 2.* Translated by Sir Thomas L. Heath. Dover Publishers Inc, New York, 1956

[6] J. B. FRALEIGH *A First Course in Abstract Algebra, 7th Edition.* Addison Wesley, Boston, 2003.

[7] J. R. GOLDMAN *The Queen of Mathematics: A Historically Motivated Guide to Number Theory.* A K Peters, Ltd., Wellesley, MA, 1998.

[8] K. IRELAND and M. ROSEN *A Classical Introduction to Modern Number Theory, 2nd Edition.* Springer, New York, 1990.

[9] Franz Lemmermeyer's Chronology and Bibliography of Proofs of the Quadratic Reciprocity Law. `http://www.rzuser.uni-heidelberg.de/~hb3/fchrono.html`. May 7, 2012.

[10] K. H. ROSEN *Elementary Number Theory and its Applications, 5th Edition.* Addison Wesley, Boston 2005.

[11] D. SMITH, M. EGGEN, and R. ST. ANDRE *A Transition to Advanced Mathematics, 5th Edition.* Brooks/Cole, Pacific Grove, 2001.

[12] B. SURY. Cyclotomy and Cyclotomic Polynomials. *Resonance.* Volume 4, Number 12 (1999), 41-53.

[13] Wikipedia. `http://en.wikipedia.org/wiki/Kronecker_delta`. May 4, 2012.

[14] Wikipedia. `http://en.wikipedia.org/wiki/Cubic_reciprocity`. May 7, 2012.

[15] Wikipedia. http://en.wikipedia.org/wiki/Diffusion_(acoustics). May 18, 2012.

[16] Wikipedia. http://en.wikipedia.org/wiki/Miller-Rabin_primality_test. May 18, 2012.

[17] Wikipedia. http://en.wikipedia.org/wiki/Paley_graph. May 18, 2012.

[18] Wikipedia. http://en.wikipedia.org/wiki/Quadratic_reciprocity. May 7, 2012.

[19] Wikipedia. http://en.wikipedia.org/wiki/Quadratic_residue. May 18, 2012.

[20] Wikipedia. http://en.wikipedia.org/wiki/Reciprocity_law. June 7, 2012.

[21] Wikipedia. http://en.wikipedia.org/wiki/Solovay-Strassen_primality_test. May 18, 2012.

VITA

Author: Suzanne M. Rousseau

Place of Birth: Salem, Oregon

Education:

Eastern Washington University

Lewis-Clark State College

Degrees Awarded:

Bachelor of Science, 2009, Lewis-Clark State College

Honors and Awards:

Graduate Instructorship, Mathematics Department, 2009-2012, Eastern Washington University

Graduated Magna Cum Laude, Lewis-Clark State College, 2009

Publications:

Towards Accurate Basalt Lava Flow Bedding Attitude Measurements From Aerial LIDAR Data, Lapwai Drainage Basin, Idaho, USA. 2010 Geological Society of America Abstracts with Programs, Volume 42, Number 5, page 283.