A Generalization of Wilson’s Theorem

by
Thomas Jeffery

A Thesis
presented to
The University of Guelph

In partial fulfilment of requirements
for the degree of
Master of Science
in
Mathematics

Guelph, Ontario, Canada
© Thomas Jeffery, November, 2018
Wilson’s theorem states that if $p$ is a prime number then $(p - 1)! \equiv -1 \pmod{p}$. One way of proving Wilson’s theorem is to note that 1 and $p - 1$ are the only self-invertible elements in the product $(p - 1)!$. The other invertible elements are paired off with their inverses leaving only the factors 1 and $p - 1$. Wilson’s theorem is a special case of a more general result that applies to any finite abelian group $G$. In order to apply this general result to a finite abelian group $G$, we are required to know the self-invertible elements of $G$.

In this thesis, we consider several groups formed from polynomials in quotient rings. Knowing the self-invertible elements allows us to state Wilson-like results for these groups. Knowing the order of these groups allows us to state Fermat-like results for these groups.

The required number theoretical background for these results is also included.
# Contents

Abstract ii

1 Introduction 1

2 Classical Theorems in Number Theory 4
   2.1 Wilson’s Theorem and Related Results 4
      2.1.1 Wilson’s Theorem 4
      2.1.2 A Generalization of Wilson’s Theorem 4
      2.1.3 Proof of Wilson’s Theorem 5
      2.1.4 Proof of Generalized Wilson 6
      2.1.5 The Converse of Wilson’s Theorem 7
   2.2 Known Results From Górowski and Lomnicki 8
   2.3 Fermat’s Little Theorem and Related Results 10
      2.3.1 Fermat’s Little Theorem and Euler’s Theorem 10
      2.3.2 Reduced Residues and Primitive Congruence Roots 13
      2.3.3 The Gaussian Factorial Function 15
      2.3.4 A Generalization of Fermat’s Little Theorem and Euler’s Theorem 20
   2.4 Lagrange’s Proof of Wilson’s Theorem 20

3 Quadratic Forms and Quadratic Residues 23
   3.1 Quadratic Congruences 23
   3.2 Binary Quadratic Forms 26
      3.2.1 Known Results Concerning Binary Quadratic Forms 26
      3.2.2 A Connection Between Binary Quadratic Forms and Quadratic Residues 27
      3.2.3 Equivalent Binary Quadratic Forms 28
   3.3 Sums of Two Squares 30
      3.3.1 Representation of An Integer as a Sum of Two Squares 30
      3.3.2 The Number of Ways of Expressing an Integer as a Sum of Two Squares 39
      3.3.3 Properly Representing an Integer As a Sum of Two Squares 40
      3.3.4 The Number of Ways of Properly Representing an Integer as a Sum of Two Squares 41
   3.4 Quadratic Residue Results From Gauss 42
      3.4.1 Properties of Quadratic Residues 42
5 Conclusion

Bibliography
Chapter 1

Introduction

On page 321 in [1], Thomas Koshy calls Wilson’s theorem, Fermat’s little theorem, and Euler’s theorem “Three Classical Milestones” of number theory. Indeed, it would be difficult to find a number theory book that does not include these three results and their respective proofs. All three of these results are essentially group theoretic results. However, number theory books, such as [3] and [1], that do not cover group theory state these results and their proofs without mentioning group theory. It should be noted that proofs of these three classical milestones in these number theory books are in fact group theoretic proofs in disguise. All three of these classical milestones can be written most naturally using the congruence notation introduced by Gauss.

According to Koshy [1], Wilson’s theorem was first conjectured in 1770 by John Wilson, a former student of Edward Waring. Neither Wilson nor Waring were able to prove it. Several years later the first proof was given by Lagrange in [5], who also proved the converse of Wilson’s theorem. The reason why neither Wilson nor Waring could give a proof is probably because they did not have two essential notions known to modern mathematicians. These notions are the notion of a group and the notion of congruence. According to [1], the notion of congruence together with its notation were introduced by Gauss around the year 1800.

Wilson’s theorem states that if \( p \) is prime then \((p - 1)! \equiv -1 \pmod{p}\). Wilson’s theorem answers the question: What do you get when you take the product of all the elements in the finite abelian group \( Z_p^* = \{1, 2, 3, ..., p - 1\} \)? Here we have used the notation \( Z_p^* \) to denote the multiplicative group of reduced residues modulo \( p \) or, in other words, the unit group of \( Z_p = \{0, 1, 2, ..., p - 1\} \). To answer this question, it can be easily shown that 1 and \( p - 1 \) are the only self-invertible group elements. The other factors are paired off with their inverses and thus contribute 1. Thus, \((p - 1)! = \prod_{g \in Z_p^*} g \equiv p - 1 \equiv -1 \pmod{p}\). Wilson’s theorem
In this thesis, we ask the question: What does one get when one takes the product of all polynomials in a certain quotient ring that are invertible modulo the prime $p$? The answer to this question can be written either in terms of quadratic residues modulo the prime $p$ or in terms of primes in residue classes. It is for this reason that this thesis contains known results concerning quadratic residues and primes in residue classes. We also include known results concerning sums of squares and binary quadratic forms as they are closely related to quadratic residues and primes in residue classes.

Fermat’s little theorem states that if $p$ is prime, $a$ is an integer, and $p \nmid a$ then $a^{p-1} \equiv 1 \pmod{p}$. According to Koshy [1], Fermat’s little theorem was first conjectured by Fermat in 1640 and later proved by Euler in 1736. As with Wilson’s theorem, neither Fermat nor Euler had the notions of groups and congruences.

Fermat’s little theorem follows from the fact that when any group element is raised to the power of the order of the group the result is the identity.

In the second chapter of this thesis, we state and prove Wilson’s theorem and Fermat’s little theorem. The proofs we give are from [1]. We then state the following two results that generalize Wilson’s theorem and Fermat’s little theorem:

\textbf{Theorem 1.0.1.} If $G$ is a finite abelian group with identity $1$ then:

$$\prod_{g \in G} g = \begin{cases} a & \text{if } a \text{ and } 1 \text{ are the only self-invertible elements of } G \\ 1 & \text{otherwise} \end{cases}$$

\textbf{Theorem 1.0.2.} If $G$ is a finite group, $n = |G|$ is the order of the group, $1$ is the identity, and $a$ is any group element then:

$$a^n = 1.$$
primes in residue classes, primitive congruence roots, and sums of squares. We also mention several connections between these.

In the fourth and final chapter of this thesis, we apply the results of Górowski and Lomnicki [2] and generalized Fermat to groups of invertible polynomials in a quotient ring. These groups generalize the multiplicative group $\mathbb{Z}_p^*$. In order to apply Górowski and Lomnicki to a group, we require the self-invertible elements in the group. In order to apply generalized Fermat to a group, we require the order of the group. In this thesis, we in some cases rigorously derive these results and in other cases we make conjectures based on numerical evidence. This gives us generalizations of Wilson’s theorem and Fermat’s little theorem. These results are written in terms of number theoretic notions that we mention in the third part of this thesis. In particular, these results are written in terms of quadratic residues, or alternatively, in terms of primes in residue classes.
Chapter 2

Classical Theorems in Number Theory

2.1 Wilson’s Theorem and Related Results

2.1.1 Wilson’s Theorem

Wilson’s theorem is referred to by Thomas Koshy as a classical milestone of number theory ([1] page 321). Wilson’s theorem appears as Theorem 7.1 in Koshy [1] and is as follows:

**Theorem 2.1.1** (Wilson’s Theorem). \( p \) is a prime number then \( (p - 1)! \equiv -1 \pmod{p} \).

In this theorem \((p - 1)!\) can be considered as the product of all group elements in the multiplicative group \( Z_p^* = \{1, 2, 3, \ldots, p - 1\} \). In this thesis we shall generalize this by considering the product of all group elements in a group of invertible polynomials in a quotient ring. The groups that we shall consider are generalizations of \( Z_p^* \).

We refer to Theorem 2.1.1 both as Wilson’s theorem and as Wilson’s theorem in one dimension. We do this because \( Z_p \) can be considered as either a scalar field or as a one dimensional vector space over itself.

2.1.2 A Generalization of Wilson’s Theorem

In Thomas Koshy’s chapter on Wilson’s theorem (see [1] Chapter 7.1), he states and proves the following known result which appears in Koshy [1] as Example 7.2 and is clearly a generalization of Wilson’s theorem:
Theorem 2.1.2 (A Generalization of Wilson’s Theorem). If \( p \) is prime and \( n \) is a natural number, then
\[
\frac{(np)!}{n^p} \equiv (-1)^n \pmod{p}.
\]

Wilson’s theorem follows from this by letting \( n = 1 \).

2.1.3 Proof of Wilson’s Theorem

We now prove these results. The following proofs are directly from Koshy [1] on pages 322-324:

We use the following result which appears in Koshy [1] as Lemma 3.3 and is known as Euclid’s lemma:

**Lemma 2.1.1 (Euclid’s Lemma).** If \( p \) is prime, \( a \) and \( b \) are integers, then if \( p \mid ab \) then \( p \mid a \) or \( p \mid b \).

Before we prove Theorems 2.1.1 and 2.1.2, we first prove a lemma also from [1]. This lemma, which we shall use throughout this paper to classify self-invertible elements in groups, states that in the group \( \mathbb{Z}_p^* = \{1, 2, 3, ..., p - 1\} \) only 1 and \( p - 1 \) are self-invertible. The proof we give is from pages 322-323 of Koshy [1].

**Lemma 2.1.2.** Let \( p \) be a prime and \( a \) an integer. Then \( a \) is self-invertible \((mod \ p)\) if and only if \( a \equiv \pm 1 \pmod{p} \).

**Proof.** Suppose \( a \) is self-invertible \((mod \ p)\). Therefore, \( a^2 \equiv 1 \pmod{p} \). Thus, \( p \mid (a^2 - 1) \). That is: \( p \mid (a - 1)(a + 1) \). So, by Euclid’s lemma (Lemma 2.1.1), \( p \mid (a - 1) \) or \( p \mid (a + 1) \). So, \( a \equiv 1 \pmod{p} \) or \( a \equiv -1 \pmod{p} \). In other words, \( a \equiv \pm 1 \pmod{p} \).

Conversely, if \( a \equiv \pm 1 \pmod{p} \) then clearly, \( a^2 \equiv 1 \pmod{p} \), and so, \( a \) is self-invertible \((mod \ p)\).

This completes the proof.

Note that the previous result may not be true if the prime \( p \) is replaced by an arbitrary integer.

Also, note that as a consequence of Lemma 2.1.2 it follows that if \( p \) is an odd prime then the congruence \( x^2 \equiv 1 \pmod{p} \) has exactly two solutions in \( \mathbb{Z}_p \). These are 1 and \( p - 1 \).

We now follow Koshy, and use this lemma to prove Wilson’s theorem (Theorem 2.1.1):
Proof. If \( p = 2 \) then \((2 - 1)! \equiv -1 \pmod{2}\). The result now follows.

Thus, let us assume that \( p > 2 \). The residues \( 1, 2, 3, \ldots, (p - 1) \) are invertible \( \pmod{p} \) and by Theorem 2.1.2, only 1 and \( (p - 1) \) are self-invertible. Thus, we group the residues that are not self-invertible, that is the residues \( 2, 3, \ldots, (p - 2) \), into pairs \((a, b)\) where \( ab \equiv 1 \pmod{p} \). Thus, \((2)(3)(p - 2) \equiv 1 \pmod{p}\). Therefore, \((p - 1)! = (1)(2)(3)...(p - 2)(p - 1) \equiv (1)(1)(p - 1) \equiv -1 \pmod{p}\) and our result follows.

\[ \square \]

2.1.4 Proof of Generalized Wilson

We now follow Koshy ([1] page 324) by proving Theorem 2.1.2 which we shall call the generalized Wilson’s theorem.

We first note that by Wilson’s theorem (Theorem 2.1.1), if \( a \equiv 0 \pmod{p} \) then \((1 + a)(2 + a)(3 + a)...(p - 1 + a) \equiv -1 \pmod{p}\). In other words, the product of the \( p - 1 \) integers between any two consecutive multiples of \( p \) is congruent to \(-1\) modulo \( p \). If we choose \( a = 0 \), which is clearly a multiple of \( p \) then we get:

\[ (1 + 0)(2 + 0)(3 + 0)...(p - 1 + 0) \equiv -1 \pmod{p}. \]

If we choose \( a = p \) then we get:

\[ (1 + p)(2 + p)(3 + p)...(p - 1 + p) \equiv -1 \pmod{p}. \]

Now, keep choosing multiples of \( p \) until we reach \( a = (n - 1)p \), where \( n \) is any natural number:

\[ (1 + (n - 1)p)(2 + (n - 1)p)(3 + (n - 1)p)...(p - 1 + (n - 1)p) \equiv -1 \pmod{p}. \]

We now have \( n \) products, each of which is congruent to \(-1\) modulo \( p \). We now take the product of these \( n \) products. The product of these \( n \) products is clearly congruent to \((-1)^n\) modulo \( p \). That is:

\[ \prod_{r=0}^{n-1} (1 + rp)(2 + rp)(3 + rp)...(p - 1 + rp) \equiv (-1)^n \pmod{p}. \]

This new product of products is formed by taking the product of the natural numbers
between 1 and \( np \) that are not multiples of \( p \). Indeed, if we had included any multiples of \( p \) then this product of products would be congruent to 0 modulo \( p \). Thus, another way to write this product of products, is to take the product of the natural numbers between 1 and \( np \) then divide by the multiples of \( p \). In this way we eliminate the unwanted multiples of \( p \) from the product.

Thus, we have:

\[
\prod_{r=0}^{n-1}(1 + rp)(2 + rp)(3 + rp)\ldots(p - 1 + rp) = \frac{(1)(2)(3)\ldots(np)}{(p)(2p)(3p)\ldots(np)}.
\]

But

\[
\frac{(1)(2)(3)\ldots(np)}{(p)(2p)(3p)\ldots(np)} = \frac{(np)!}{n!p^n}.
\]

Thus we have established the following key result:

\[
\frac{(np)!}{n!p^n} \equiv (-1)^n \pmod{p}.
\]

Therefore, Theorem 2.1.2 now follows.

### 2.1.5 The Converse of Wilson’s Theorem

Recall that Wilson’s theorem (Theorem 2.1.1) states that if \( p \) is prime then \((p - 1)! \equiv -1 \pmod{p}\). It turns out that the converse of this is also true. The converse of Wilson’s theorem, which is stated and proved as Theorem 7.2 in Koshy [1], and was first proved by Lagrange, is as follows:

**Theorem 2.1.3** (The Converse of Wilson’s Theorem). *Let \( p \) be a positive integer. If \((p - 1)! \equiv -1 \pmod{p}\) then \( p \) is prime.*

The following contradiction proof is from pages 324-325 in Koshy [1]:

**Proof.** We proceed by contradiction as follows:

Suppose that \((p - 1)! \equiv -1 \pmod{p}\) and that \( p \) is composite. Thus, we can write \( p = ab \), where \( 1 < a < p \) and \( 1 < b < p \).

Now \( a|p \) and \( p |((p - 1)! + 1) \). Thus, \( a|((p - 1)! + 1) \).

Since \( a \) is strictly between 1 and \( p \) it follows that \( a \in \{2, 3, \ldots, p - 1\} \). So, \( a|(p - 1)! \) and \( a|((p - 1)! + 1) \).
From this, it follows that $a | ((p - 1)! + 1 - (p - 1)!)$. Therefore, $a | 1$ which contradicts $a > 1$.

Thus, $p$ is prime.

With this result (Theorem 2.1.3) and Wilson’s theorem (Theorem 2.1.1) we have the following result:

Theorem 2.1.4. If $p$ is a positive integer then $(p - 1)! \equiv -1 \pmod{p}$ if and only if $p$ is prime.

Theorem 2.1.4 gives us a way to test the primality of a positive integer. However, because the quantity $(p - 1)!$ is extremely large unless $p$ is small, this primality test is never used in practice.

## 2.2 Known Results From Górowski and Łomnicki

Let $G$ be any finite abelian group.

In [2], Górowski and Łomnicki consider the product: $\prod_{g \in G} g$ and they show that this product depends on the set of group elements in $G$ that have order 2.

Now, the self-invertible elements in a group $G$ are the identity element and the elements of order 2.

In this thesis we denote the set of self-invertible elements in the group $G$ by $S(G)$. With this notation we have the following:

Theorem 2.2.1. If $G$ is an abelian group, then $S(G)$ is a subgroup of $G$.

Proof. Consider an abelian group $G$ with identity 1. We show that $S(G)$ contains the identity, is closed under the binary operation of $G$, and is closed under inverses. Clearly $1 \in S(G)$. If $a, b \in S(G)$, then $(ab)^2 = (ab)(ab) = a(ba)b = a(ab)b = a^2b^2 = 1$. Thus, $ab \in S(G)$. If $a \in S(G)$ then $(a^{-1})^2 = (a^2)^{-1} = 1$. Thus, $a^{-1} \in S(G)$.

This completes the proof.

Note that if $G$ is not abelian then $S(G)$ may not be a subgroup. To see this, consider $G$ to be the symmetric group on 3 elements. Then $|G| = 6$ and $|S(G)| = 4$. By Lagrange’s
theorem, the order of a subgroup divides the order of the group. Thus, \( S(G) \) is not a subgroup.

The main result in Górowski and Lomnicki [2] can be written in terms of self-invertible group elements as follows:

**Theorem 2.2.2.** If \( G \) is a finite abelian group with identity 1 then:

\[
\prod_{g \in G} g = \begin{cases} 
  a & \text{if \( a \) and 1 are the only self-invertible elements of \( G \)} \\
  1 & \text{otherwise}
\end{cases}
\]

If we let \( |S(G)| \) denote the number of self-invertible elements in the group \( G \) (i.e. the order of \( S(G) \), the subgroup of self-invertible elements in \( G \)), then the following follows immediately from the previous result:

**Theorem 2.2.3.** If \( G \) is a finite abelian group with identity 1 then:

\[
\prod_{g \in G} g = 1 \iff (|S(G)| \neq 2).
\]

Every Wilson-like result in this thesis follows from Theorem 2.2.2 in some way or another. The Wilson-like results that appear in Chapter 4 involve products over groups formed from polynomials in a quotient ring, matrices, and determinants.

Consider the group of reduced residues modulo a prime \( p \). That is consider the residues \( Z_p^* = \{1, 2, 3, ..., p-1\} \). By Theorem 2.1.2, 1 and \( p - 1 \) are the only self-invertible elements in the group \( Z_p^* \). In other words, \( p - 1 \) is the unique element in \( Z_p^* \) of order 2. Thus, by Górowski and Lomnicki (Theorem 2.2.2) we have:

\[
\prod_{g \in G} g = \prod_{i=1}^{p-1} i = (p - 1)! \equiv p - 1 \equiv -1 \; (mod \; p).
\]

Thus, we have proved Wilson’s theorem (Theorem 2.1.1) as a corollary to Theorem 2.2.2. Deriving results that are generalizations of Theorem 2.1.1 and special cases of Theorem 2.2.2 is the main goal of this thesis.
2.3 Fermat’s Little Theorem and Related Results

2.3.1 Fermat’s Little Theorem and Euler’s Theorem

We now mention two important results known as Fermat’s little theorem and Euler’s theorem. These results appear as Theorems 7.3 and 7.1 in Koshy [1]. In [1], Thomas Koshy calls Wilson’s theorem, Fermat’s little theorem, and Euler’s theorem “Three classical Milestones” of number theory. Thus, Fermat’s little theorem and Euler’s theorem are definitely worth mentioning. As another reason for mentioning these two results, note that they are similar to Wilson’s theorem. To see this similarity, note that given a finite abelian group $G$, Wilson’s theorem considers the following product:

$$\prod_{g \in G} g.$$ 

Whereas, given a finite group $G$ and a group element $a$, Fermat’s little theorem and Euler’s theorem consider the product:

$$\prod_{g \in G} a.$$ 

This can be written as:

$$\prod_{g \in G} a = a^{|G|},$$

where we have written $|G|$ to denote the order of the group $G$.

We follow Koshy by proving Euler’s theorem without mentioning group theory. Note, however, that this proof is a group theoretic proof in disguise. The proof we give of Euler’s theorem together with the proof of the required lemma is from pages 343-345 in [1].

Finally, we mention a group theoretic result which generalizes both Fermat’s little theorem and Euler’s theorem and applies to any finite group.

Fermat’s little theorem, which is sometimes called Fermat’s theorem, is as follows:

**Theorem 2.3.1 (Fermat’s Little Theorem).** If $p$ is prime, $a$ is an integer, and $p \nmid a$ then:

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

Note, that we can combine Wilson’s theorem (Theorem 2.1.1) and Fermat’s little theorem...
(Theorem 2.3.1), to give the following result which follows from both of them:

**Theorem 2.3.2.** If $p$ is prime, $a$ is an integer, and $p 
mid a$ then:

$$a^{p-1} + (p-1)! \equiv 0 \pmod{p}.$$  

We write $\gcd(a, b)$ to denote the greatest common divisor of the integers $a$ and $b$. If $\gcd(a, b) = 1$ then we say that $a$ and $b$ are relatively prime.

We write $\phi(m)$ to mean the Euler phi function that is defined to be the number of positive integers less than or equal to $m$ and relatively prime to $m$.

We define the notion of least residue of an integer as follows: Note that every integer $n$ is congruent modulo $m$ to a unique integer in the set $\{0, 1, 2, \ldots, m-1\}$. We call this integer the least residue of $n$ modulo $m$.

Now, Fermat’s little theorem can be generalized to give the following result known as Euler’s theorem:

**Theorem 2.3.3** (Euler’s Theorem). If $m$ is a positive integer, $a$ is an integer, and $\gcd(a, m) = 1$ then:

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$  

To prove this we first establish the following which appears as Lemma 7.6 in [1]:

**Lemma 2.3.1.** Suppose $m$ is a positive integer, $a$ is an integer, and $\gcd(a, m) = 1$. Let $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ be the set of positive integers $\leq m$ and relatively prime to $m$. Then the least residues of: $ar_1$, $ar_2$, $ar_3$, $\ldots$, $ar_{\phi(m)}$ modulo $m$ are a permutation of: $r_1$, $r_2$, $r_3$, $\ldots$, $r_{\phi(m)}$.

We now prove this lemma as follows: The proof we give is from pages 343-344 in [1].

**Proof.** We will show that the function $f$ defined as:

$$f(i) = \text{the least residue of } a \cdot i \pmod{m}$$

is a bijection from the set $\{r_1, r_2, r_3, \ldots, r_{\phi(m)}\}$ to itself.

Now, $\gcd(a, m) = 1$ and $\gcd(r_i, m) = 1$, for all $i \in \{r_1, r_2, r_3, \ldots, r_{\phi(m)}\}$. Thus, $\gcd(ar_i, m) = 1$, for all $i \in \{r_1, r_2, r_3, \ldots, r_{\phi(m)}\}$. Therefore, $\gcd(f(r_i), m) = 1$, for all $i \in \{r_1, r_2, r_3, \ldots, r_{\phi(m)}\}$. Thus, $f$ maps the set $r_i \in \{r_1, r_2, r_3, \ldots, r_{\phi(m)}\}$ to itself.
We now show that $f$ is one to one as follows: Suppose that $f(r_i) = f(r_j)$.
Thus,

$$ar_i \equiv ar_j \pmod{m}.$$ 

Since $\gcd(a, m) = 1$, we now have:

$$r_i \equiv r_j \pmod{m}.$$ 

It now follows, since $1 \leq r_i, r_j \leq m$, that $r_i = r_j$.
Thus, $f$ is a one to one function from the set $r_i \in \{r_1, r_2, r_3, ..., r_{\phi(m)}\}$ to itself, which means that $f$ is onto.

Therefore, $f$ is a permutation.
This completes the proof.

We now use Lemma 2.3.1 to prove Euler’s theorem as follows: Again, the proof we give is from pages 344-345 in [1].

**Proof.** By Lemma 2.3.1, the integers: $ar_1, ar_2, ar_3, ..., ar_{\phi(m)}$ are congruent modulo $m$ to $r_1, r_2, r_3, ..., r_{\phi(m)}$ in some order.
Thus,

$$ar_1 \cdot ar_2 \cdot ar_3 \cdot ... \cdot ar_{\phi(m)} \equiv r_1 \cdot r_2 \cdot r_3 \cdot ... \cdot r_{\phi(m)} \pmod{m}.$$ 

This implies that:

$$a^{\phi(m)} r_1 r_2 r_3 ... r_{\phi(m)} \equiv r_1 r_2 r_3 ... r_{\phi(m)} \pmod{m}.$$ 

Now, $\gcd(r_i, m) = 1$ for all $r_i \in \{r_1, r_2, r_3, ..., r_{\phi(m)}\}$. Thus, $\gcd(r_1 r_2 r_3 ... r_{\phi(m)}, m) = 1$. Therefore,

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$ 

This completes the proof.

Fermat’s little theorem follows immediately from Euler’s theorem by choosing $m = p$ to be prime and noting that $\phi(p) = p - 1$. 

12
2.3.2 Reduced Residues and Primitive Congruence Roots

In this section we mention the group theoretic notion of reduced residues and their connection to Fermat’s little theorem and Euler’s theorem. We first mention complete residue systems. A complete residue system modulo an integer \( m \) is a set of integers \( S \) with the following two properties:

1. No two integers in \( S \) are congruent modulo \( m \).
2. Every integer is congruent modulo \( m \) to an integer in \( S \).

Note that the set \( S = \{0, 1, 2, ..., m - 1\} \) clearly satisfies these two properties and is therefore a complete residue system modulo \( m \). We call this set the set of least residues modulo \( m \). Also, note that every complete residue system modulo \( m \) contains exactly \( m \) integers.

We define \( Z_m \), the set of complete residues modulo \( m \) as follows:

\[
Z_m = \{(0), (1), (2), ..., (m - 1)\}
\]

where \((a) = \{x \in Z \mid x \equiv a \ (mod \ m)\}\) is the residue class containing the integer \( a \). In this thesis we will often write the residue class \((a)\) as just \( a \) when it is clear from the context that we are considering residue classes and not integers.

We now define the related notion of a reduced residue system. A reduced residue system modulo an integer \( m \) is a set of integers \( S \) with the following three properties:

1. No two integers in \( S \) are congruent modulo \( m \).
2. Every integer in \( S \) is relatively prime to \( m \).
3. Every integer that is relatively prime to \( m \) is congruent modulo \( m \) to an integer in \( S \).

Note that every reduced residue system modulo \( m \) contains exactly \( \phi(m) \) integers. Also, note that the set of integers \( \{r_1, r_2, r_3, ..., r_{\phi(m)}\} \) that we defined in the previous section is a reduced residue system modulo \( m \).

We define the set of reduced residues modulo \( m \) as follows:

\[
\{(a) \mid (a) \in Z_m, \ gcd(a, m) = 1\}.
\]

The following result appears in [1], [3], and [4] and follows from the elementary properties of greatest common divisors and linear Diophantine equations:
Theorem 2.3.4. \( \gcd(a, m) = 1 \) if and only if there exists an integer \( x \) such that \( ax \equiv 1 \pmod{m} \).

From this theorem it is clear that the set of reduced residues modulo \( m \) form a multiplicative group. This follows since by the previous result, all reduced residues are invertible. If we choose \( m = p \) to be prime, then the only element in \( \mathbb{Z}_p \) that is not invertible is the zero residue (0). Thus, the group of reduced residues modulo \( p \) is \( \mathbb{Z}_p^* = \{1, 2, \ldots, (p-1)\} \). Also, Theorem 2.3.4 explains why many algebra books refer to the group of reduced residues modulo \( m \) as the group of units modulo \( m \).

Now, the congruence that appears in Theorem 2.3.4 can be written in terms of residue classes as: \( (a)(x) = (1) \). By Euler’s theorem this equation in \( \mathbb{Z}_m \) has solution \( x = (a^{\phi(m) - 1}) \). Therefore, Theorem 2.3.4 also follows from Euler’s theorem.

We now define the notion of the order of a group element \( a \) in a group \( G \) as follows:

We define the order of \( a \) by \( e = \text{ord}(a) \) to be the least positive integer \( e \) such that \( a^e \) is the identity in \( G \). From this definition it follows immediately that the order of the group element \( a \) is the order of the cyclic subgroup generated by \( a \). In other words, \( \text{ord}(a) = | \langle a \rangle | \), where \( \langle a \rangle = \{a^n | n \in \mathbb{Z}\} \). If \( G \) is the group of reduced residues modulo \( m \) then we shall write the order of \( a \) as \( \text{ord}_mA \).

By Euler’s theorem \( \text{ord}_mA \) exists and is well defined. Also, from Euler’s theorem it is clear that \( \text{ord}_mA \leq \phi(m) \).

Now, the order of the group of reduced residues modulo \( m \) is \( \phi(m) \). It can be shown, either by elementary methods or by group theoretic methods, (see [1]) that for each reduced residue \( a \), \( \text{ord}_mA \) divides \( \phi(m) \), which is the order of the group of reduced residues. Thus, we have the following which appears in Koshy [1] as Corollary 10.1:

**Theorem 2.3.5.** If \( \gcd(a, m) = 1 \) then \( \text{ord}_mA \) divides \( \phi(m) \).

We also have the following result which generalizes Theorem 2.3.5 and can be found in any book on algebra:

**Theorem 2.3.6.** The order of a group element divides the order of the group.

This follows from the well-known result from algebra that states that the order of a subgroup divides the order of the group.

We now return to the group of reduced residues modulo \( m \). Let \( g \) be relatively prime to \( m \). Now, it may happen that \( \text{ord}_mg = \phi(m) \). In this case we say that \( g \) is a primitive congruence root modulo \( m \).
We now state without proof some important results in the theory of primitive congruence roots. The first of these is a consequence of Lagrange’s theorem, which we mention in the next section. These results are stated and proved in each of [1], [3], and [4]. In particular, the following three results appear as Theorem 2.36, Theorem 2.41, and Definition 2.7 in [4].

**Theorem 2.3.7.** If $p$ is prime then there exist exactly $\phi(p - 1)$ primitive congruence roots modulo $p$.

**Theorem 2.3.8.** The positive integer $m$ has a primitive congruence root if and only if $m = 1, 2, 4, p^\alpha$, or $2p^\alpha$, where $p$ is an odd prime and $\alpha$ is a positive integer.

**Theorem 2.3.9.** If $m$ is a positive integer with primitive congruence root $g$ then:

$$g^1, g^2, ..., g^{\phi(m)}$$

form a reduced residue system modulo $m$.

From Theorem 2.3.9, we can show the following which appears as Corollary 10.4 in [1]:

**Theorem 2.3.10.** If a positive integer $m$ has a primitive congruence root then it has exactly $\phi(\phi(m))$ primitive congruence roots.

Also, from Theorem 2.3.9, it follows that if $m$ has a congruence root $g$, then the group of reduced residues modulo $m$ is equal to:

$$\langle g \rangle = \{g^1, g^2, ..., g^{\phi(m)} \} = \{g^n \mid n \in \mathbb{Z} \}.$$  

Thus we have the following two results which follow immediately from Theorems 2.3.8 and 2.3.9:

**Theorem 2.3.11.** If $m$ is a positive integer with primitive congruence root $g$ then the group of reduced residues modulo $m$ is a cyclic group and $g$ is a generator of this group.

**Theorem 2.3.12.** The group of reduced residues modulo $m$ is a cyclic group if and only if $m = 1, 2, 4, p^\alpha$, or $2p^\alpha$, where $p$ is an odd prime and $\alpha$ is a positive integer.

### 2.3.3 The Gaussian Factorial Function

We now briefly mention the Gaussian factorial function $n_m!$, which is a generalization of the factorial function $n!$. The Gaussian factorial function is studied in [6]. Note that the Gaussian factorial is one of many different versions of the factorial function.
We define the Gaussian factorial $n_m!$ to be the product of all positive integers $i \leq n$ that are relatively prime to $m$. In other words:

$$n_m! = \prod_{i \leq n, \gcd(i, m) = 1} i.$$ 

Clearly $n_1! = n!$. Thus, $n_m!$ generalizes $n!$.

We now consider the special case of the Gaussian factorial function where $m = n$. Thus, we consider $n_n!$. Now, the Gaussian factorial $n_n!$ removes factors in $n!$ that are not relatively prime to $n$. By Theorem 2.3.4 the Gaussian factorial removes factors in $n!$ that are not invertible modulo $n$.

Therefore, the factors in $n_n!$ are reduced residues modulo $n$. Thus, they form a well-known finite abelian group of order $\phi(n)$. We can apply Górowski and Lomnicki [2] to give a new proof of the following known result:

**Theorem 2.3.13.** If $n \geq 2$ is an integer then

$$n_n! \equiv \begin{cases} -1 \pmod{n} & \text{if } n = 2, 4, p^\alpha, \text{ or } 2p^\alpha \\ 1 \pmod{n} & \text{otherwise} \end{cases}$$

where $p$ is an odd prime and $\alpha$ is a positive integer.

Theorem 2.3.13 is from [6] and was first proved by Gauss.

If we choose $n$ to be the prime $p$ in Theorem 2.3.13 then we have the following, which is another way of writing Wilson’s theorem:

**Theorem 2.3.14.** If $p$ is prime then $p_p! \equiv -1 \pmod{p}.

Thus, Theorem 2.3.13 is a generalization of Wilson’s theorem.

Note that since $-1$ is self-invertible and relatively prime to every $n$ it follows immediately from Theorem 2.2.2 that $n_n! \equiv \pm \pmod{n}$. This agrees with Theorem 2.3.13.

We now use Theorem 2.2.2 to give a new proof of Theorem 2.3.13. We use the following three results which appear as Corollary 2.42, Corollary 2.44, and Theorem 2.20 in Niven, Zuckerman, and Montgomery [4]:

**Theorem 2.3.15.** Let $n = 1, 2, 4, p^\alpha, \text{ or } 2p^\alpha$, where $p$ is an odd prime. If $\gcd(a, n) = 1$ then the congruence $x^m \equiv a \pmod{n}$ has $\gcd(m, \phi(n))$ solutions or no solutions, according as
\[ a^{\phi(n)/\gcd(m,\phi(n))} \equiv 1 \pmod{n} \]

or not.

**Theorem 2.3.16.** Let \( \alpha \geq 3 \) and let \( a \) be odd. If \( m \) is odd, then the congruence \( x^m \equiv a \pmod{2^\alpha} \) has exactly one solution. If \( m \) is even, then choose \( \beta \) so that \( \gcd(m, 2^{\alpha-2}) = 2^\beta \). The congruence \( x^m \equiv a \pmod{2^\alpha} \) has \( 2\beta+1 \) solutions or no solutions according as \( a \equiv 1 \pmod{2^{\beta+2}} \) or not.

**Theorem 2.3.17.** Let \( f(x) \) be a fixed polynomial with integral coefficients. Let \( N(n) \) denote the number of solutions in \( \mathbb{Z}_n \) of the congruence \( f(x) \equiv 0 \pmod{n} \). If \( n = n_1n_2 \) where \( \gcd(n_1, n_2) = 1 \) then \( N(n) = N(n_1)N(n_2) \).

Note that if we choose \( n = p \) to be an odd prime, \( m = 2 \), and \( p \nmid a \) in Theorem 2.3.15 then it follows that the quadratic congruence \( x^2 \equiv a \pmod{p} \) has two solutions or no solutions according as:

\[ a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \]

or not.

This consequence of Theorem 2.3.15 is known as Euler’s criterion, a result we mention again in our section on quadratic residues.

Note that Theorem 2.3.17 applies to any polynomial congruence. In what follows we consider the polynomial congruence \( x^2 \equiv 1 \pmod{n} \). This congruence has the trivial solution \( x = 1 \). Thus, if we let \( N(n) \) be the number of \( x \in \mathbb{Z}_n \) such that \( x^2 \equiv 1 \pmod{n} \) then for every \( n \), \( N(n) \geq 1 \). From this remark and from Theorem 2.3.17, it follows that if \( \gcd(n_1, n_2) = 1 \) then \( N(n_1n_2) \geq N(n_1) \).

Thus, we have the following lemma:

**Lemma 2.3.2.** Let \( N(n) \) denote the number of solutions of the congruence \( x^2 \equiv 1 \pmod{n} \). Then if \( \gcd(n_1, n_2) = 1 \) then \( N(n_1n_2) \geq N(n_1) \).

We now use Theorem 2.2.2 due to Górowski and Lomnicki in addition to Theorems 2.3.15, 2.3.16, 2.3.17, and Lemma 2.3.2 to prove Theorem 2.3.13 as follows:

**Proof.** If \( n = 2 \) the result follows. Thus, we assume that \( n > 2 \).

The product \( n_n! \) is the product of all group elements in the group of reduced residues modulo \( n \). Now both 1 and \(-1\) are self-invertible group elements. By Theorem 2.2.2, the
product \( n_n! \) is congruent to \(-1\) modulo \( p \) if 1 and \(-1\) are the only self-invertible group elements and \( n_n! \) is congruent to 1 modulo \( p \) if the group contains self-invertible elements other than 1 and \(-1\).

Now the self-invertible elements in the group of reduced residues modulo \( n \) are precisely the solutions of the congruence:

\[
x^2 \equiv 1 \pmod{n}.
\]

Since \( n > 2 \) this congruence has at least two distinct solutions in the group of reduced residues modulo \( n \). These are 1 and \(-1\). Therefore, by Theorem 2.2.2, the product \( n_n! \) is congruent to \(-1\) modulo \( n \) if the congruence \( x^2 \equiv 1 \pmod{n} \) has only two solutions (these being 1 and \(-1\)) and the product \( n_n! \) is congruent to 1 modulo \( n \) if the congruence \( x^2 \equiv 1 \pmod{n} \) has more than 2 solutions.

Suppose that \( n \) is an integer of the form \( n = 4, p^a \), or \( 2p^a \) where \( p \) is an odd prime. We now Choose \( a = 1 \) and \( m = 2 \) in Theorem 2.3.15. Clearly \( \gcd(a, n) = \gcd(1, n) = 1 \). Thus, by Theorem 2.3.15, the congruence \( x^2 \equiv 1 \pmod{n} \) has exactly \( \gcd(2, \phi(n)) \) solutions. Now, \( n > 2 \). Thus, \( \phi(n) \) is even. Therefore, \( \gcd(2, \phi(n)) = 2 \). It now follows that the congruence \( x^2 \equiv 1 \pmod{n} \) has exactly 2 solutions in \( Z_n \). These are 1 and \(-1\). By Theorem 2.2.2 we have:

\[
n_n! \equiv -1 \pmod{n}.
\]

We now suppose that \( n > 2 \) is an integer not of the form \( n = 4, p^a \), or \( 2p^a \) where \( p \) is an odd prime. Thus, \( n \) either has at least two odd prime factors, is 4 times a power of an odd prime, or is divisible by 8. We consider each of these three cases separately as follows: First let \( n \) have at least two distinct odd prime factors say \( p \) and \( q \). Let \( p^a \) and \( q^b \) be the highest powers of \( p \) and \( q \) that divide \( n \). Each of the congruences:

\[
x^2 \equiv 1 \pmod{p^a}
\]

and

\[
x^2 \equiv 1 \pmod{q^b}
\]

have at least 2 solutions. Thus, by Theorem 2.3.17, the congruence:

\[
x^2 \equiv 1 \pmod{p^aq^b}
\]
has at least 4 solutions. It now follows from Lemma 2.3.2 that the congruence \( x^2 \equiv 1 \pmod{n} \) has at least 4 distinct solutions, each of which is a self-invertible element in the group of reduced residues modulo \( n \). By Theorem 2.2.2 we have:

\[
n_n! \equiv 1 \pmod{n}.
\]

Secondly let \( n \) be 4 times a power of an odd prime. Let this odd prime be \( p \) and let \( p^a \) be the highest power of \( p \) that divides \( n \). The congruence:

\[
x^2 \equiv 1 \pmod{p^a}
\]

has at least 2 solutions. The congruence:

\[
x^2 \equiv 1 \pmod{4}
\]

has exactly 2 solutions. Therefore, by Theorem 2.3.17, the congruence:

\[
x^2 \equiv 1 \pmod{4p^a}
\]

has at least 4 solutions Thus, by Lemma 2.3.2, the congruence:

\[
x^2 \equiv 1 \pmod{n}
\]

has at least 4 solutions, each of which is a self-invertible element in the group of reduced residues modulo \( n \). By Theorem 2.2.2 we have:

\[
n_n! \equiv 1 \pmod{n}.
\]

In the third case, let \( n \) be divisible by 8. Let \( 2^\alpha \), where \( \alpha \geq 3 \), be the highest power of 2 that divides \( n \). We now choose \( a = 1 \) and \( m = 2 \) in Theorem 2.3.16. We choose \( \beta = 1 \). This choice of \( \beta \) satisfies \( \gcd(2, 2^\alpha - 2) = 2^\beta \). Thus, by Theorem 2.3.16, the congruence \( x^2 \equiv 1 \pmod{2^\alpha} \) has \( 2^{\beta+1} = 2^{1+1} = 4 \) solutions. Thus, by Lemma 2.3.2, the congruence \( x^2 \equiv 1 \pmod{n} \) has at least 4 solutions each of which is a self-invertible element in the group of reduced residues modulo \( n \). By Theorem 2.2.2 we have:

\[
n_n! \equiv 1 \pmod{n}.
\]
This completes the proof. □

Note that in light of Theorem 2.3.8 this result due to Gauss can be written in terms of primitive congruence roots as follows:

**Theorem 2.3.18.** If \( n \geq 2 \) is an integer then

\[
\begin{align*}
n_n! & \equiv \begin{cases} 
-1 \pmod{n} & \text{if } n \text{ has a primitive congruence root} \\
1 \pmod{n} & \text{otherwise}
\end{cases}
\end{align*}
\]

### 2.3.4 A Generalization of Fermat’s Little Theorem and Euler’s Theorem

Note that both Fermat’s little theorem and Euler’s theorem are special cases of the following more general result which is found in any book on algebra:

**Theorem 2.3.19.** If \( G \) is a finite group, \( n = |G| \) is the order of the group, \( a \) is any group element, and 1 is the identity then:

\[ a^n = 1. \]

This follows immediately from the well-known fact (due to Lagrange) that the order of a subgroup divides the order of the group. For the special case of this result where it is assumed that the group \( G \) is abelian, this follows from the well-known fact that when you multiply each element in a group by a fixed group element you permute the group. Note, that Fermat’s little theorem (Theorem 2.3.1) and Euler’s theorem (Theorem 2.3.3) follow immediately from this result by considering the group \( G \) to be the group of reduced residues modulo \( p \) (i.e. \( Z_p^* \)) in the case of Fermat’s little theorem and the group of reduced residues modulo \( m \) in the case of Euler’s theorem.

### 2.4 Lagrange’s Proof of Wilson’s Theorem

We now give an additional proof of Wilson’s theorem (Theorem 2.1.1). This proof is due to Lagrange, appears in [5], and is the first published proof of Wilson’s theorem. The proof is an easy application of Fermat’s little theorem (Theorem 2.3.1) and Lagrange’s theorem and
appears in Chapter 10.3 in Koshy [1] and in Chapter 7.6 in Hardy and Wright [3] in their chapters on primitive congruence roots, where they use a corollary of Lagrange’s theorem to prove the existence of primitive congruence roots of a prime. The existence of primitive congruence roots of a prime $p$ is given in Theorem 2.3.7 in the last section which states that there are exactly $\phi(p-1)$ such primitive congruence roots.

We use the following result which appears as Theorem 10.5 in [1] and Theorem 107 in [3] and is known as Lagrange’s theorem:

**Theorem 2.4.1** (Lagrange’s Theorem). Let $f(x) = c_nx^n + ... + c_1x + c_0$ be a polynomial with integral coefficients and with degree $n \geq 1$. Then the congruence $f(x) \equiv 0 \pmod{p}$ has at most $n$ roots in $\mathbb{Z}_p$.

The proof of this follows by induction on $n$ and appears in Koshy [1] and in Hardy and Wright [3].

Note that the following two results are consequences of Lagrange’s theorem:

**Theorem 2.4.2.** Let $f(x) = c_nx^n + ... + c_1x + c_0$ be a polynomial with integral coefficients and with degree $n \geq 1$. If the congruence $f(x) \equiv 0 \pmod{p}$ has more than $n$ roots in $\mathbb{Z}_p$ then $f(x)$ is the zero polynomial modulo $p$.

**Theorem 2.4.3.** If $f(x) = c_nx^n + ... + c_1x + c_0 \in \mathbb{Z}[x]$ has roots $a_1, ..., a_n$ in $\mathbb{Z}_p$, then:

$$f(x) \equiv c_n(x - a_1)(x - a_2)...(x - a_n) \pmod{p}.$$ 

Theorems 2.4.2 and 2.4.3 are Theorems 107 and 108 from [3]. Either one of Theorems 2.4.2 and 2.4.3 can be used to prove Wilson’s theorem.

We now follow Lagrange by proving Wilson’s theorem using Fermat’s little theorem (Theorem 2.3.1) and either Theorem 2.4.2 or 2.4.3 as follows:

**Proof.** Consider the polynomial $f(x) = (x-1)(x-2)...(x-p+1)-x^{p-1}+1$. Thus, $f(x) \in \mathbb{Z}[x]$ and $f(x)$ has degree $p-2$. By Fermat’s little theorem, the congruence $x^{p-1} - 1 \equiv 0 \pmod{p}$ has $p-1$ solutions in $\mathbb{Z}_p$. These solutions are: 1, 2, ..., $p-1$. Thus, by 2.4.3 we have:

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

Thus, $f(x)$ is the zero polynomial modulo $p$. It now follows that every coefficient of $f(x)$, including the constant term, is congruent to 0 modulo $p$. The constant term in $f(x)$ is $(-1)(-2)...(-p+1)+1$. 

21
Thus,
\[ (-1)(-2)...(-p + 1) + 1 = (p - 1)!(-1)^{p-1} + 1 \equiv 0 \ (mod \ p). \]

It now follows that \((p - 1)! \equiv (-1)^p \ (mod \ p)\).

Wilson’s theorem now follows.

\[ \square \]

Note, that in the previous proof of Wilson’s theorem, instead of using Theorem 2.4.3 we could have shown that \(f(x) \in \mathbb{Z}[x]\) has degree \(p - 2\) and the congruence \(f(x) \equiv 0 \ (mod \ p)\) has \(p - 1\) solutions in \(\mathbb{Z}_p\). We could have then used Theorem 2.4.2 to conclude that \(f(x)\) is the zero polynomial modulo \(p\). As with before, Wilson’s theorem now follows.
Chapter 3

Quadratic Forms and Quadratic Residues

3.1 Quadratic Congruences

We follow Koshy [1] by considering the quadratic congruence:

\[ Ax^2 + Bx + C \equiv 0 \pmod{p}, \]

where \( p \nmid A \) and \( p \) is an odd prime.

If we multiply by 4A and complete the square, then we arrive at the following congruence:

\[ (2Ax + B)^2 \equiv B^2 - 4AC \pmod{p}. \]

Note, that since \( p \) is an odd prime, we can work backwards from the congruence:

\[ (2Ax + B)^2 \equiv B^2 - 4AC \pmod{p}. \]

To return to the congruence:

\[ Ax^2 + Bx + C \equiv 0 \pmod{p}. \]

Thus, the following are equivalent:

\[ Ax^2 + Bx + C \equiv 0 \pmod{p} \]
and

$$(2Ax + B)^2 \equiv B^2 - 4AC \pmod{p}.$$ 

If we choose $y \equiv 2Ax + B$ and $b \equiv B^2 - 4AC$ then our original congruence is now equivalent to a congruence of the following form:

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

It is for this reason that we study the congruence $y^2 \equiv b \pmod{p}$.

In particular, for the (simplified) quadratic congruence $y^2 \equiv b \pmod{p}$, we would like to know are there solutions and, if there are, how many solutions?

If $p$ is prime, $b$ is an integer, and $p \nmid b$ then we shall say that $b$ is a quadratic residue if there exists an integer $y$ such that $y^2 \equiv b \pmod{p}$. We shall say that $b$ is a quadratic nonresidue if there is no such integer $y$ such that $y^2 \equiv b \pmod{p}$. If $p|b$ then we shall say that $b$ is neither a quadratic residue nor a quadratic nonresidue. In this thesis, we refer to the question of whether $b$ is a quadratic residue, a quadratic nonresidue, or neither as the quadratic nature of $b$ modulo the prime $p$.

Note, that the quadratic residues are analogous to integers that are perfect squares.

We shall follow Gauss by referring to quadratic residues simply as residues when there is no confusion between quadratic residues and linear residues.

Now that we have introduced terminology to answer the question of whether or not the congruence $y^2 \equiv b \pmod{p}$ and thus also the equivalent congruence $Ax^2 + Bx + C \equiv 0 \pmod{p}$ have solutions, we shall now address the question of how many solutions.

This question is answered by the following, which is stated and proved as Lemma 11.1 in Koshy [1]:

**Theorem 3.1.1.** Let $p$ be an odd prime, $a$ be an integer, and $p \nmid a$. Then the congruence $x^2 \equiv a \pmod{p}$ has either no solutions or two noncongruent solutions.

**Proof.** Suppose there exists a solution say $\alpha$. Thus, $\alpha^2 \equiv a \pmod{p}$. It is easy to see that $\beta = p - \alpha$ is a second solution.

Now suppose that these two solutions are congruent modulo $p$. This implies that

$$\alpha \equiv p - \alpha \pmod{p}.$$ 

Since $p$ is odd this means that $\alpha \equiv 0 \pmod{p}$. Therefore, since $\alpha^2 \equiv a \pmod{p}$ we have
\( a \equiv 0 \pmod{p} \) which contradicts the assumption \( p \nmid a \). We therefore have shown that there exists 2 noncongruent modulo \( p \) solutions.

Now, suppose that \( \gamma \) is third solution.

Thus,

\[
\gamma^2 \equiv \alpha^2 \pmod{p}.
\]

This is equivalent by Euclid’s lemma (Lemma 2.1.1) to

\[
\gamma \equiv \pm \alpha \pmod{p}.
\]

Thus, it follows that \( \gamma \equiv \alpha \) or \( \gamma \equiv \beta \) modulo \( p \). Therefore, if there is a solution then there are exactly 2 noncongruent solutions modulo \( p \).

This completes the proof.

Now, in Theorem 3.1.1, we assumed that \( p \nmid a \). If \( p \mid a \) then the congruence has exactly one solution \( x \equiv 0 \pmod{p} \).

Thus the congruence \( x^2 \equiv a \pmod{p} \) has either no solution, one solution, or 2 noncongruent mod \( p \) solutions. This also follows from Lagrange’s theorem (Theorem 2.4.1) which we mentioned in the last section.

Note, that since the congruences:

\[
Ax^2 + Bx + C \equiv 0 \pmod{p}
\]

and

\[
(2Ax + B)^2 \equiv B^2 - 4AC \pmod{p}
\]

are equivalent, then by the previous theorem (Theorem 3.1.1), we have the following:

**Theorem 3.1.2.** Let \( p \) be an odd prime, let \( p \nmid A \) then the congruence \( Ax^2 + Bx + C \equiv 0 \pmod{p} \) has either no solution, one solution, or two noncongruent mod \( p \) solutions. Which of these depends on the quadratic nature of \( B^2 - 4AC \) modulo the prime \( p \).

Again, this result can also be proved by using Lagrange’s theorem (Theorem 2.4.1).
3.2 Binary Quadratic Forms

3.2.1 Known Results Concerning Binary Quadratic Forms

In this section, we briefly mention several results from the theory of binary quadratic forms. All the results and proofs in this section are from Niven, Zuckerman, and Montgomery [4] in their chapter on quadratic reciprocity and quadratic forms. These results are relevant in light of Theorem 3.2.2 which gives a connection between binary quadratic forms and quadratic residues. (As the reader will see, quadratic residues are essential to this thesis).

A binary quadratic form is a function of the form:

$$f(x, y) = ax^2 + bxy + cy^2.$$  

Here, $a$, $b$, and $c$ are integers.

We say the form $f(x, y) = ax^2 + bxy + cy^2$ is indefinite if it assumes both positive and negative values. We say this form is positive semidefinite if $f(x, y) \geq 0$, for all integers $x$, $y$. We say this form is negative semidefinite if $f(x, y) \leq 0$, for all integers $x$, $y$. We say this form is positive definite if it is positive semidefinite and $f(x, y) = 0$ if and only if $x = y = 0$. We say this form is negative definite if it is negative semidefinite and $f(x, y) = 0$ if and only if $x = y = 0$.

The discriminant of this binary quadratic form is the quantity:

$$d = b^2 - 4ac.$$  

Note the similarities between the discriminant of a binary quadratic form and the quantity $B^2 - 4AC$ encountered in the previous section.

The discriminant is useful because it tells us whether a quadratic form is definite or indefinite according to the following result which appears as Theorem 3.11 in Niven, Zuckerman, and Montgomery [4]:

**Theorem 3.2.1.** Let $f(x, y)$ be a binary quadratic form where $a$, $b$, and $c$ are integers and $d = b^2 - 4ac$ is the discriminant. If $d > 0$ then $f(x, y)$ is indefinite. If $d = 0$ then $f(x, y)$ is semidefinite and not definite. If $d < 0$ then $a$ and $c$ have the same sign and $f(x, y)$ is positive definite if $a > 0$ and $f(x, y)$ is negative definite if $a < 0$.

We say that the binary quadratic form $f(x, y)$ represents the integer $n$ if there exist integers $x_1$ and $y_1$ such that $n = f(x_1, y_1)$. 

26
We say that the binary quadratic form \( f(x, y) \) represents the integer \( n \) properly if there exist integers \( x_1 \) and \( y_1 \) such that \( n = f(x_1, y_1) \) and \( \gcd(x_1, y_1) = 1 \) (i.e. \( x_1 \) and \( y_1 \) are relatively prime).

In the next section we state and prove a key result, which provides a connection between binary quadratic forms and quadratic residues, whose proof is from Niven, Zuckerman, and Montgomery.

### 3.2.2 A Connection Between Binary Quadratic Forms and Quadratic Residues

The following result appears as Theorem 3.13 in [4].

**Theorem 3.2.2.** If \( n \) and \( d \) are integers and \( n \neq 0 \) then there exists a binary quadratic form with discriminant \( d \) that represents \( n \) properly if and only if there exists an integer \( x \) such that \( x^2 \equiv d \pmod{4|n|} \).

This result makes sense intuitively since the equation \( n = ax^2 + bxy + cy^2 \) is equivalent to \( 4an = (2ax + by)^2 - dy^2 \) which leads us to consider the quadratic nature of \( d \) modulo \( 4|n| \).

We now give a rigorous proof of this result from Niven, Zuckerman, and Montgomery. For this proof we require the following two lemmas, the first of which is a special case of a well-known result known as the Chinese remainder theorem.

**Lemma 3.2.1.** If \( m_1 \) and \( m_2 \) are relatively prime positive integers and \( a_1 \) and \( a_2 \) are integers then there exists an integer \( x \) such that \( x \equiv a_1 \pmod{m_1} \) and \( x \equiv a_2 \pmod{m_2} \).

For a proof of this see Koshy [1] or Hardy and Wright [3].

**Lemma 3.2.2.** If \( N \) is an integer, \( x_0 \), and \( y_0 \) are relatively prime integers then there exist relatively prime integers \( m_1 \) and \( m_2 \) such that \( m_1 \) and \( y_0 \) are relatively prime, \( m_2 \) and \( x_0 \) are relatively prime, and \( N = m_1 m_2 \).

**Proof.** To prove this lemma, let \( x_0 = p_1^{a_1} \cdots p_k^{a_k} \) and \( y_0 = q_1^{b_1} \cdots q_m^{b_m} \) be the prime factorizations of \( x_0 \) and \( y_0 \). Write \( N \) as \( N = p_1^{a_1} \cdots p_k^{a_k} q_1^{b_1} \cdots q_m^{b_m} r_1^{c_1} \cdots r_n^{c_n} \).

We now choose \( m_1 = p_1^{a_1} \cdots p_k^{a_k} r_1^{c_1} \cdots r_n^{c_n} \) and \( m_2 = q_1^{b_1} \cdots q_m^{b_m} \). The result now follows.

We now prove Theorem 3.2.2 as follows. The proof we give is from [4] on page 153:
Proof. Suppose that the integer $b$ is a solution of the congruence $x^2 \equiv d \pmod{4|n|}$. Thus, there exists an integer $c$ such that $b^2 = d + 4nc$. Now consider the binary quadratic form $f(x, y) = nx^2 + bxy + cy^2$. Clearly, $f(1, 0) = n$ and $gcd(1, 0) = 1$. Therefore, this binary quadratic form represents $n$ properly.

Conversely, suppose there exists a binary form, say $f(x, y) = ax^2 + bxy + cy^2$, with discriminant $d = b^2 - 4ac$ that represents $n \neq 0$ properly. Thus, there exists relatively prime integers, say $x_0$ and $y_0$, such that $n = f(x_0, y_0) = ax_0^2 + bx_0y_0 + cy_0^2$. If we apply Lemma 3.2.2 to $N = 4|n|$ then there exist relatively prime integers, say $m_1$ and $m_2$ such that $m_1$ and $y_0$ are relatively prime, $m_2$ and $x_0$ are relatively prime, and $4|n| = m_1m_2$.

Now, for any binary quadratic form $f(x, y) = ax^2 + bxy + cy^2$ with discriminant $d = b^2 - 4ac$, we can write:

$$4af(x, y) = (2ax + by)^2 - dy^2.$$  

Therefore, $4an = (2ax + by)^2 - dy^2$. Since $4|n| = m_1m_2$, we have:

$$(2ax_0 + by_0)^2 \equiv dy_0^2 \pmod{m_1}.$$  

Now $gcd(m_1, y_0) = 1$. Thus, by Theorem 2.3.4, there exists an integer $y_0$ such that $y_0y_0 \equiv 1 \pmod{m_1}$.

From this, it follows that $(2ax_0 + by_0)^2y_0^2 \equiv d \pmod{m_1}$.

It now follows that $u = u_1 = (2ax_0 + by_0)y_0$ is a solution of the congruence: $u^2 \equiv d \pmod{m_1}$. In a similar manner, we can show that there exists a solution $u = u_2$ of the congruence $u^2 \equiv d \pmod{m_2}$.

Thus, by Lemma 3.2.1, there exists an integer $x$ such that $x \equiv u_1 \pmod{m_1}$ and $x \equiv u_2 \pmod{m_2}$. Therefore, $x^2 \equiv u_1^2 \equiv d \pmod{m_1}$ and $x^2 \equiv u_2^2 \equiv d \pmod{m_2}$. Since, $gcd(m_1, m_2) = 1$, we have that there exists an integer $x$ such that $x^2 \equiv d \pmod{m_1m_2}$. The result now follows, since $m_1m_2 = 4|n|$.

\[\square\]

### 3.2.3 Equivalent Binary Quadratic Forms

We now define the notion of equivalent forms as follows: The definition we give is from Chapter 3.5 from Niven, Zuckerman, and Montgomery [4].

We say that the binary quadratic forms $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y) = Ax^2 + Bxy + Cy^2$ are equivalent and write $f \sim g$ if there exists $M = [m_{ij}] \in SL_2(\mathbb{Z})$ such
that \( g(x, y) = f(m_{11}x + m_{12}y, m_{21}x + m_{22}y) \), where \( SL_2(Z) \) is the special linear group of \( 2 \times 2 \) matrices over \( Z \). That is, \( SL_2(Z) \) is the set of \( 2 \times 2 \) matrices with integer entries and determinant 1. Note that in [4] Niven, Zuckerman, and Montgomery call \( SL_2(Z) \) the modular group and denote it by \( \Gamma \).

Niven, Zuckerman, and Montgomery write the relation \( \sim \) between binary quadratic forms in terms of matrices. From this it is straightforward to show that this defines an equivalence relation. We also have the following which appears as Theorem 3.17 in [4]:

**Theorem 3.2.3.** If \( f \) and \( g \) are equivalent binary quadratic forms then the discriminants of \( f \) and \( g \) are equal and if \( n \) is an integer, then there is a one to one correspondence between representations of \( n \) by \( f \) and representations of \( n \) by \( g \). Also, there is a one to one correspondence between proper representations of \( n \) by \( f \) and proper representations of \( n \) by \( g \).

We now define the notion of a reduced form as follows: Again, the definition we give is from Chapter 3.5 from [4].

If \( f \) is a binary quadratic form such that the discriminant of \( f \) is not a perfect square, then we say \( f \) is a reduced form if:

\[
-|a| < b \leq |a| < |c|
\]

or if

\[
0 \leq b \leq |a| = |c|.
\]

Niven, Zuckerman, and Montgomery give a method involving matrices in \( SL_2(Z) \) to replace the form \( f \) whose discriminant \( d \) is not a perfect square with a reduced form whose discriminant is also \( d \). Thus, we have the following result which appears as Theorem 3.18 in [4]:

**Theorem 3.2.4.** If \( d \) is a fixed integer which is not a perfect square then every equivalence class of binary quadratic forms of discriminant \( d \) contains at least one reduced form.

The following result from Niven, Zuckerman, and Montgomery places conditions on reduced positive definite forms and appears as Theorem 3.19 in [4]:

**Theorem 3.2.5.** If \( f(x, y) = ax^2 + bxy + cy^2 \) is a reduced positive definite form with discriminant \( d \) then \( 0 < a \leq \sqrt{-d/3} \).
From this the following is immediate:

**Theorem 3.2.6.** The binary quadratic form $x^2 + y^2$, which represents a sum of two squares, is the only reduced form with discriminant $d = -4$.

This is a fact that we shall make use of in the following section on sums of two squares. In this thesis, we shall encounter the following 3 binary quadratic forms:

$$x^2 + y^2,$$

$$2x^2 - 2xy + y^2,$$

and

$$x^2 - xy + y^2.$$

3.3 Sums of Two Squares

3.3.1 Representation of An Integer as a Sum of Two Squares

In this section we state and prove known results that tell us exactly which integers are sums of two squares. We then briefly address the question: “Given an integer how many ways can it be written as a sum of two squares?” We do not address the question: “Given an integer how can we write it as a sum of two squares?”

These results are relevant for two reasons. One reason is that the sum of squares: $x^2 + y^2$ is in fact, a binary quadratic form. Thus, the question of whether an integer $n$ can be written as a sum of two squares is now a question of whether $n$ can be represented by this quadratic form which is now, by Theorem 3.2.2, a question of quadratic residues.

Another reason is the connection between the sums of two squares results proved in this section and the quadratic nature of $-1$ modulo a prime $p$. As we shall see, the question of the quadratic nature of $-1$ modulo an odd prime $p$ is essentially a question of which reduced residue class in $Z_4$ that $p$ belongs to.

This connection is apparent in the following two results from Niven, Zuckerman, and Montgomery [4] which appear in [4] as Theorem 2.12 and Lemma 2.13:
Theorem 3.3.1. Let $p$ be prime. Then there exists an integer $x$ such that $x^2 \equiv -1 \pmod{p}$ if and only if $p = 2$ or $p \equiv 1 \pmod{4}$.

Theorem 3.3.2. If $p$ is prime and $p = 2$ or $p \equiv 1 \pmod{4}$ then $p$ is a sum of two squares.

Thus, the sum of squares problem is now a quadratic residue problem. In particular, the problem of expressing a prime $p$ as a sum of two squares is now a question of the quadratic nature of $-1$ modulo $p$. As we mentioned already, quadratic residues are essential to this thesis.

In the section on quadratic residues we shall interpret Theorem 3.3.1 in terms of quadratic residues and the Legendre symbol and give three different proofs.

In the present section, we give 3 different proofs of Theorem 3.3.2 each of which makes use of Theorem 3.3.1. These three proofs are from [1], [4], and [3].

Note that, according to page 54 of Niven, Zuckerman, and Montgomery [4], Theorem 3.3.2 was “first stated in 1632 by Albert Girard, on the basis of numerical evidence. The first proof was given by Fermat in 1654.”

We provide two proofs of the following, which follows from Theorem 3.3.2, completely answers the question of which positive integers are a sum of two squares, and is known as Fermat’s two squares theorem. One proof is from [1] the other is from [4].

Theorem 3.3.3 (Fermat’s Two Squares Theorem). A natural number $n$ can be written as a sum of two squares if and only if the exponent of each prime factor of $n$ congruent to $3$ modulo $4$ in the canonical decomposition of $n$ is even.

We now give three proofs of Theorem 3.3.2 each of which uses Theorem 3.3.1 as promised. Note, that if $p = 2$ then Theorem 3.3.2 is clearly true, since $2 = 1^2 + 1^2$. Thus, in each of these proofs we assume that $p \equiv 1 \pmod{4}$.

The first proof is from Koshy [1], the second proof is from Niven, Zuckerman, and Montgomery [4], and the third proof is from Hardy and Wright [3].

We first require the following which appears in [1] as Lemma 13.9:

Lemma 3.3.1. If $p$ is prime and $p \equiv 1 \pmod{4}$ then there exist positive integers $x$ and $y$ such that $x^2 + y^2 = kp$ for some natural number $k$ with $k < p$.

Proof. Since $p \equiv 1 \pmod{4}$, by Theorem 3.3.1 there exists a positive integer $a$ such that $a^2 \equiv -1 \pmod{p}$ and $a < p$. Thus, there exists a positive integer $k$ such that $a^2 + 1 = kp$. Now choose $x = a$ and $y = 1$. Therefore, there exist positive integers $x$ and $y$ such that $x^2 + y^2 = kp$. 

31
Now, $a \leq p - 1$. Thus,

$$kp = a^2 + 1 \leq (p - 1)^2 + 1 = p^2 - 2(p - 1) < p^2.$$ 

Thus, $k < p$. \qedhere

We also require the following result which appears as Lemma 13.8 from [1] and is due to Diophantus:

**Theorem 3.3.4.** The product of two sums of squares is a sum of two squares. In particular, we have:

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2.$$  

**Proof.** To prove this, we consider the complex numbers $z = a + ib$ and $w = d + ic$. The result now follows by noting that $|z|^2|w|^2 = |zw|^2$. \qedhere

We now follow Koshy by proving Theorem 3.3.2 as follows:

The proof we now give is from pages 604-605 from Koshy [1].

**Proof.** Let $p$ be a prime and $p \equiv 1 \pmod{4}$. By Lemma 3.3.1 and the well-ordering principle, there exists a positive integer $m$ such that $mp$ is a sum of two squares, say $mp = x^2 + y^2$, $m < p$, and $m$ is the least such positive integer. We now prove by contradiction that $m = 1$. Suppose $m > 1$.

Choose $r$ and $s$ to be integers such that:

$$r \equiv x \pmod{m},$$

$$s \equiv y \pmod{m},$$

and

$$-\frac{m}{2} < r, s \leq \frac{m}{2}.$$ 

Thus,

$$r^2 + s^2 \equiv x^2 + y^2 = mp \equiv 0 \pmod{m}.$$
Therefore, there exists a nonnegative integer $n$ such that $nm = r^2 + s^2$.

With this, we have $(r^2 + s^2)(x^2 + y^2) = (mn)(mp) = m^2np$. Now, by Theorem 3.3.4,

$$(r^2 + s^2)(x^2 + y^2) = (rx + sy)^2 + (ry - sx)^2.$$ 

Thus,

$$(rx + sy)^2 + (ry - sx)^2 = m^2np.$$ 

Now,

$$rx + sy \equiv x^2 + y^2 \equiv 0 \pmod{m}$$ 

and

$$ry - sx \equiv xy - yx \equiv 0 \pmod{m}.$$ 

This implies that $\frac{rx+sy}{m}$ and $\frac{ry-sx}{m}$ are integers, and therefore,

$$np = \left(\frac{rx + sy}{m}\right)^2 + \left(\frac{ry - sx}{m}\right)^2.$$ 

Thus, $np$ is a sum of two squares. Now, $nm = r^2 + s^2 \leq (\frac{m}{2})^2 + (\frac{m}{2})^2 = \frac{m^2}{2} < m^2$.

Therefore, $n < m$.

Now, $n$ is a nonnegative integer. If $n = 0$, then, $r^2 + s^2 = 0$. Thus, $r = s = 0$ and $x \equiv y \equiv 0 \pmod{m}$. Which means that $m|x$ and $m|y$ and therefore, $m^2|(x^2 + y^2)$. That is, $m^2|mp$. Thus, $m|p$. Since $m > 1$ and $m < p$. This is of course impossible. We thus conclude that $n \neq 0$, which means that $n$ is a positive integer.

Thus, there exists a positive integer $n$ such that $np$ is a sum of two squares, $n < p$, and $n < m$. This is a contradiction, since we assumed $m$ to be the least positive integer such that $mp$ is a sum of two squares and $m < p$. Therefore, $m = 1$.

□

We now give a second proof of Theorem 3.3.2. This proof is from pages 54-55 from Niven, Zuckerman, and Montgomery [4].

**Proof.** Let $p$ be a prime number and $p \equiv 1 \pmod{4}$.

By Theorem 3.3.1, there exists an integer $x$ that satisfies:
With this choice of \( x \), define the function \( f \) as follows:

\[
f(u, v) = u + xv.
\]

Define the positive integer \( N \) by \( N = \lfloor \sqrt{p} \rfloor \). Now, \( \sqrt{p} \) is not an integer. Thus, \( N < \sqrt{p} < N + 1 \).

Let us now consider ordered pairs of integers \( (u, v) \), where \( 0 \leq u \leq N \) and \( 0 \leq v \leq N \). Thus, there exists \((N + 1)^2\) of these ordered pairs. Now, \( N + 1 > \sqrt{p} \). Thus, the number of these ordered pairs is \( > p \). We now consider the function \( f(u, v) \) (mod \( p \)). Since the number of ordered pairs is greater than the number of residue classes, by the pigeonhole principle, there exist distinct pairs \( (u_1, v_1) \) and \( (u_2, v_2) \) such that \( 0 \leq u_1, u_2, v_1, v_2 \leq N \) and \( f(u_1, v_1) \equiv f(u_2, v_2) \) (mod \( p \)).

We thus, have the following congruence:

\[
u_1 + xv_1 \equiv u_2 + xv_2 \pmod{p}.
\]

This gives us:

\[
(u_1 - u_2) \equiv -x(v_1 - v_2) \pmod{p}.
\]

Now, choose \( a = u_1 - u_2 \) and \( b = v_1 - v_2 \).

We now have the following congruence:

\[
a \equiv -xb \pmod{p}.
\]

Squaring both sides gives:

\[
a^2 \equiv x^2b^2 \equiv -b^2 \pmod{p}.
\]

This implies that \( p | (a^2 + b^2) \). Now \( (u_1, v_1) \neq (u_2, v_2) \). Thus, \( a^2 + b^2 > 0 \). Since \( a = u_1 - u_2 \), \( 0 \leq u_1 \leq N \), and \( 0 \leq u_2 \leq N \) we have \(-N \leq a \leq N \). However, \( N < \sqrt{p} \). Therefore, \( |a| < \sqrt{p} \). Similarly, \( |b| < \sqrt{p} \). Thus, \( a^2 < p \) and \( b^2 < p \).

This gives \( 0 < a^2 + b^2 < 2p \) and \( p | (a^2 + b^2) \). Now, the only multiple of \( p \) in the open interval \( (0, 2p) \) is \( p \) itself. Thus, we conclude that \( p = a^2 + b^2 \).
We now give a third proof of 3.3.2. We use the following result whose proof involves Farey fractions, appears in [3] as Theorem 36, appears in [4] as Theorem 6.8, and can be used to prove a weaker version of Hurwitz’s theorem:

**Theorem 3.3.5.** If $x$ is a real number and $n$ a positive integer, then there exists a rational number $a/b$ such that

$$|x - \frac{a}{b}| \leq \frac{1}{b(n+1)}$$

and

$$0 < b \leq n.$$  


We now follow Hardy and Wright [3] by giving a third proof of Theorem 3.3.2 as follows: This proof is from pages 396-397 from Hardy and Wright [3].

**Proof.** Let $p$ be prime and $p \equiv 1 \pmod{4}$.

Thus, by Theorem 3.3.1, there exists an integer $l$ such that:

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

We now let $n = \lfloor \sqrt{p} \rfloor$ and $x = -l/p$. With these choices for $n$ and $x$ we apply Theorem 3.3.5. Thus, by Theorem 3.3.5, there exists integers $a$ and $b$ such that:

$$\left| -\frac{l}{p} - \frac{a}{b} \right| \leq \frac{1}{b(n+1)} < \frac{1}{b\sqrt{p}}$$

and

$$0 < b < \sqrt{p}.$$  

Thus,

$$\left| \frac{lb + pa}{pb} \right| < \frac{1}{b\sqrt{p}}.$$  

We now choose $c = lb + pa$.

Thus,
$|c| < \sqrt{p}$.

These imply the following:

$0 < b^2 + c^2 < 2p$.

Now $c \equiv lb \pmod{p}$. Thus,

$b^2 + c^2 \equiv b^2 + l^2 b^2 \equiv b^2(1 + l^2) \equiv 0 \pmod{p}$.

We now have $p | (b^2 + c^2)$ and $0 < b^2 + c^2 < 2p$. Since $p$ is the only multiple of $p$ in the open interval $(0, 2p)$ it follows that $p = b^2 + c^2$.

We now follow Koshy, by using Theorem 3.3.2 to prove Theorem 3.3.3:

We first require the following two results which appear as Lemma 13.6 and Lemma 13.7 in [1]:

**Theorem 3.3.6.** If $n \equiv 3 \pmod{4}$ then $n$ is not a sum of two squares.

**Proof.** Note that for any integer $x$, $x^2 \equiv 0$ or $1 \pmod{4}$. Thus, $x^2 + y^2 \equiv 0, 1$, or $2 \pmod{4}$. In particular, $x^2 + y^2 \not\equiv 3 \pmod{4}$.

**Theorem 3.3.7.** If $n$ is a positive integer that is a sum of two squares then for every positive integer $k$, $k^2 n$ is a sum of two squares.

The proof of this is trivial thus we omit it.

We now follow Koshy, by proving Theorem 3.3.3 as follows: The proof we give is from pages 605-606 in [1].

**Proof.** We begin with the forward direction. Suppose that $n = x^2 + y^2$ and the canonical decomposition of $n$ contains the prime $p \equiv 3 \pmod{4}$ with odd exponent $2i + 1$. Thus $p^{2i+1}$ is the highest power of $p$ that divides $n$.

Let $d = \gcd(x, y)$ be the greatest common divisor of $x$ and $y$. Let $r = x/d$, $s = y/d$, and $m = n/d^2$. Thus, $r^2 + s^2 = m$ and $\gcd(r, s) = 1$.

Let $p^j$ be the highest power of $p$ that divides $d$. Now, $m = n/d^2$. Thus, $p^{2i+1-2j} | m$. 

36
If $2i - 2j + 1 \leq 0$ then $2i + 2 \leq 2j$ and since $p^{2j}|d^2$ and $d^2|n$, this implies that $p^{2i+2}|n$. However, $p^{2i+1}$ is, by our assumption, the highest power of $p$ that divides $n$. Thus, we have a contraction. Thus, $2i - 2j + 1 > 0$. Which of course means that $2i - 2j + 1 \geq 1$. Since $p^{2i+1-2j}|m$, we have, $p|m$.

Now let us suppose that $p|r$. Since $p|m$ and $r^2 + s^2 = m$ we have $p|s$. This contradicts $gcd(r, s) = 1$. Thus, $p \nmid r$.

Therefore, by Theorem 2.3.4, there exists an integer $\tilde{r}$ such that $r\tilde{r} \equiv 1 (mod p)$.

Now, $p|m$ and $r^2 + s^2 = m$. Thus, $r^2 + s^2 \equiv 0 (mod p)$, which is the same as $-r^2 \equiv s^2 (mod p)$.

Thus,

$$(s\tilde{r})^2 \equiv -1 (mod p).$$

By Theorem 3.3.1, $p \not\equiv 3 (mod 4)$. This is a contradiction. Thus, $n$ is not a sum of two squares.

Conversely, if the exponent of each prime factor congruent to 3 modulo 4 in the canonical decomposition of $n$ is even, then we can write $n$ as $n = a^2b$, where $b$ is a product of distinct primes $\not\equiv 3 (mod 4)$. In other words, $b$ is a product of distinct primes $p$ such that $p \equiv 1 (mod 4)$ or $p = 2$. Thus, by Theorem 3.3.4 and Theorem 3.3.2, $b$ is a sum of two squares and by Theorem 3.3.7 so is $n$.

We now follow Niven, Zuckerman, and Montgomery [4] in proving Theorem 3.3.3 from Theorem 3.3.2. We first prove the following required lemma whose proof is on page 55 of [4]:

**Lemma 3.3.2.** If $q$ is a prime, $q|(a^2 + b^2)$, and $q \equiv 3 (mod 4)$ then $q|a$ and $q|b$.

**Proof.** We prove the contrapositive. Let $q$ be prime and $q|(a^2 + b^2)$. We prove that if $q \nmid a$ or $q \nmid b$ then $p \not\equiv 3 (mod 4)$.

Let $q \nmid a$ (if $q \nmid b$ then interchange $a$ and $b$). By Theorem 2.3.4, we can choose $\bar{a}$ such that $\bar{a}a \equiv 1 (mod q)$.

Now $a^2 \equiv -b^2 (mod q)$.

Thus, $(b\bar{a})^2 \equiv -1 (mod q)$. By Theorem 3.3.1, $q \not\equiv 3 (mod 4)$.

We now follow Niven, Zuckerman, and Montgomery in giving a second proof of Theorem 3.3.3 as follows:
The proof that follows is from page 56 in [4]. We shall prove the forward direction only. The converse direction given in Niven, Zuckerman, and Montgomery [4] is essentially the same as in the previous proof from Koshy [1].

**Proof.** We shall prove that if \( n \) is a sum of two squares then the exponent of each prime factor of \( n \) congruent to 3 modulo 4 in the canonical decomposition is even.

Let us write \( n \) as a canonical decomposition as follows:

\[
  n = 2^\alpha \prod_{p \equiv 1 \pmod{4}} p^\beta \prod_{q \equiv 3 \pmod{4}} q^\gamma.
\]

We shall show that if \( n = a^2 + b^2 \) then every \( \gamma \) is even.

We proceed by contradiction. Suppose that \( n = a^2 + b^2 \) and that \( \gamma \) is odd. Say \( \gamma = 2k+1 \). Thus, \( q^{2k+1} \) is the highest power of \( q \) that divides \( n = a^2 + b^2 \). Therefore,

\[
  q^{2k+1} | (a^2 + b^2).
\]

And so

\[
  q | \left( \left( \frac{a}{q^k} \right)^2 + \left( \frac{b}{q^k} \right)^2 \right).
\]

From the previous result, it follows that:

\[
  q | \frac{a}{q^k}
\]

and

\[
  q | \frac{b}{q^k}.
\]

It now follows that

\[
  q^{k+1} | a
\]

and

\[
  q^{k+1} | b.
\]

Thus,
This contradicts our assumption that $q^{2k+1}$ is the highest power of $q$ that divides $a^2 + b^2$. Thus, we have established a contradiction. Thus, each $\gamma$ is even.

3.3.2 The Number of Ways of Expressing an Integer as a Sum of Two Squares

Now that we have completely answered the question: “Which integers $n$ are a sum of two squares?” We now turn our attention to the question: “How many ways can $n$ be expressed as a sum of two squares?”.

All the results in this section are from Niven, Zuckerman, and Montgomery [4].

We follow Niven, Zuckerman, and Montgomery by defining the function $R(n)$ to be the number of ordered pairs of integer $(x, y)$ such that $n = x^2 + y^2$.

Note, that the representations $n = x^2 + y^2$ and $n = (-x)^2 + y^2$ are distinct and counted twice by the function $R(n)$. Also, note that the representations $n = x^2 + y^2$ and $n = y^2 + x^2$ are also distinct and counted twice, since $R(n)$ counts ordered pairs of integers $(x, y)$.

Niven, Zuckerman, and Montgomery state and prove the following, which is Theorem 3.22 in [4]:

**Theorem 3.3.8.** Write the positive integer $n$ as:

$$n = 2^\alpha \prod_{p \equiv 1 \pmod{4}} p^{\beta} \prod_{q \equiv 3 \pmod{4}} q^\gamma.$$

If all $\gamma$ are even then:

$$R(n) = 4 \prod_{p \equiv 1 \pmod{4}} (\beta + 1).$$

Otherwise:

$$R(n) = 0.$$ 

Note that Fermat’s two squares theorem (Theorem 3.3.3) follows immediately from Theorem 3.3.8.
3.3.3 Properly Representing an Integer As a Sum of Two Squares

We have thus considered the problem of representing an integer as a sum of two squares. We now turn our attention to the problem of properly representing an integer as a sum of two squares. That is, given a positive integer \( n \) can we find relatively prime integers \( x_1 \) and \( y_1 \) such that \( n = x_1^2 + y_1^2 \)?

As with the previous section, all results in this section are taken directly from Niven, Zuckerman, and Montgomery [4].

We use results from the previous section on properly representing an integer by the binary quadratic form \( x^2 + y^2 \) to prove Theorem 3.3.9 by following Niven, Zuckerman, and Montgomery.

We use the following, which is Theorem 2.23 in [4]:

**Lemma 3.3.3** (Hensel’s Lemma). Let \( f(x) \) be a fixed polynomial with integer coefficients. If \( f(a) \equiv 0 \) \( (\text{mod } p^n) \) and \( f'(a) \not\equiv 0 \) \( (\text{mod } p) \) then \( \exists! \ t \) \( (\text{mod } p) \) such that \( f(a + tp^n) \equiv 0 \) \( (\text{mod } p^{n+1}) \).

We now prove the following by applying Theorem 3.2.2 to the binary quadratic form \( x^2 + y^2 \):

**Theorem 3.3.9.** The positive integer \( n \) is properly representable as a sum of two squares if and only if \( n \) is either a product of primes of the form \( 4m + 1 \) or twice a product of primes of the form \( 4m + 1 \).

The proof we now give is from page 164 from [4].

*Proof.* It follows from Theorem 3.2.6, that the binary quadratic form \( x^2 + y^2 \) is the only reduced form whose discriminant is \( d = -4 \).

From Theorem 3.2.2, it follows that a positive integer \( n \) can be properly represented by the binary quadratic form \( x^2 + y^2 \) if and only if the quadratic congruence:

\[
x^2 \equiv -4 \pmod{4n}
\]

has a solution.

Note that \( x^2 \equiv -4 \pmod{8} \) has a solution. However, \( x^2 \equiv -4 \pmod{16} \) has no solution. Thus, \( n \) may be divisible by 2 and not 4.

If \( p \) is a prime of the form \( 4m + 1 \) then by Theorem 3.3.1 there exists an integer \( x \) such that \( x^2 \equiv -1 \pmod{p} \), or equivalently, \( x^2 + 4 \equiv 0 \pmod{p} \).
Now, let \( f(x) = x^2 + 4 \). Thus, the congruence \( f(x) \equiv 0 \pmod{p} \) has a solution say \( x_1 \) that satisfies \( f'(x_1) = 2x_1 \not\equiv 0 \pmod{p} \).

Therefore, by Hensel’s lemma (Theorem 3.3.3), the congruence \( f(x) \equiv 0 \pmod{p^\beta} \) has a solution for each \( \beta \geq 1 \). Thus, the positive integer \( n \) may be divisible by any power of any prime of the form \( p = 4m + 1 \).

Also, by Theorem 3.3.1, if \( p \) is a prime of the form \( p = 4m + 3 \) then the congruence \( x^2 \equiv -1 \pmod{p} \) has no solution. Thus, the congruence \( x^2 \equiv -4 \pmod{p} \) has no solution. Therefore, \( n \) is not divisible by any power of any prime of the form \( p = 4m + 3 \).

This completes the proof.

\[ \square \]

### 3.3.4 The Number of Ways of Properly Representing an Integer as a Sum of Two Squares

We now turn our attention to the number of ways in which a positive integer \( n \) can be properly represented as a sum of two squares.

As with the previous two sections, all results in this section are taken directly from Niven, Zuckerman, and Montgomery [4].

Let \( r(n) \) denote the number of proper representations of \( n \). That is, \( r(n) \) is the number of ordered pairs of relatively prime integers \((x, y)\) such that \( n = x^2 + y^2 \). Note that, as with \( R(n) \), the representations \( n = x^2 + y^2 \) and \( n = (-x)^2 + y^2 \) are distinct and counted twice by the function \( r(n) \). Also, note, that the representations \( n = x^2 + y^2 \) and \( n = y^2 + x^2 \) are also distinct and counted twice since \( r(n) \) counts ordered pairs of integers \((x, y)\).

So, for example, \( r(2) = 4 \) since \( 2 = 1^2 + 1^2 = (-1)^2 + 1^2 = 1^2 + (-1)^2 = (-1)^2 + (-1)^2 \) and \( r(5) = 8 \) since \( 5 = 2^2 + 1^2 = (-2)^2 + 1^2 = 2^2 + (-1)^2 = (-2)^2 + (-1)^2 = 1^2 + 2^2 = (-1)^2 + 2^2 = 1^2 + (-2)^2 = (-1)^2 + (-2)^2 \).

We now have the following, which is Theorem 3.22 from [4].

**Theorem 3.3.10.** Write the positive integer \( n \) as follows:

\[
    n = 2^\alpha \prod_{p \equiv 1 \pmod{4}} p^{\beta} \prod_{q \equiv 3 \pmod{4}} q^{\gamma}.
\]

If \( \alpha = 0 \) or \( \alpha = 1 \) and every \( \gamma = 0 \) then \( r(n) = 2^{\alpha+2} \) where
\[ t = \sum_{p \equiv 1 \ (mod\ 4), p | n} (1). \]

Otherwise, \( r(n) = 0. \)

Note that Theorem 3.3.9 follows immediately from Theorem 3.3.10.

### 3.4 Quadratic Residue Results From Gauss

All results and proofs in this section (with the exception of one proof of Theorem 3.4.5) are taken directly from pages 626-641 of Gauss’ Disquisitiones Arithmeticae in God Created The Integers [7].

#### 3.4.1 Properties of Quadratic Residues

In this section, we state and prove some results due to Gauss concerning quadratic residues. In Gauss’ paper [7] he considers quadratic residues relative to a prime modulus and then generalizes by considering quadratic residues relative to a composite modulus.

In this section, we only mention results due to Gauss that apply to quadratic residues relative to a prime modulus. We do this because these results are all that we really need in this thesis.

The quadratic nature of an integer relative to a prime modulus is easily determined either by the results in this section, the law of quadratic reciprocity, or the generalized law of quadratic reciprocity. Also, if \( a \not\equiv 0 \ (mod\ p) \) then by Theorem 3.1.1 the congruence: \( x^2 \equiv a \ (mod\ p) \) has two noncongruent solutions or no solutions depending on the quadratic nature of \( a \) modulo \( p \). A major difference between Gauss and other authors, like Koshy for example, is that Gauss considers the integer 0 (and thus everything congruent to 0) to be a quadratic residue while other authors define 0 to be neither a residue nor a nonresidue. Defining 0 to be a quadratic residue makes some sense algebraically, since the congruence: \( x^2 \equiv 0 \ (mod\ p) \) clearly has the single solution \( x = 0 \). However, defining 0 to be neither a residue nor a nonresidue means that the number of residues and the number of nonresidues relative to the prime modulus \( p \) are equal and that the congruence: \( x^2 \equiv a \ (mod\ p) \) has two noncongruent solutions or no solutions depending on whether \( a \) is a residue or a nonresidue. The proofs of the results that follow in this section do not use the law of quadratic reciprocity. The truth of the law of quadratic reciprocity, which Gauss calls the fundamental theorem,
is suggested by the results in this section. Some of the results in this section are in fact special cases of the law of quadratic reciprocity. We will have more to say about the law of quadratic reciprocity in the next section when we introduce the Legendre symbol. Also, in this section when we use the word residue, we of course mean a quadratic residue.

Our first result tells us that the number of residues is equal to the number of nonresidues:

**Theorem 3.4.1.** If $p$ is prime then of the numbers $1, 2, 3, ..., p − 1$, a total of $\frac{p-1}{2}$ will be residues and the other $\frac{p-1}{2}$ will be nonresidues.

The proof of this result follows from Theorem 3.1.1 that states that if $a \not\equiv 0 \pmod{p}$ then the congruence $x^2 \equiv a \pmod{p}$ has two noncongruent solutions or no solutions. Theorem 3.4.1 implies that if an integer in the set $1, 2, 3, ..., p−1$ is randomly chosen then there is a fifty percent chance that it will be a residue and a fifty percent chance that it will be a nonresidue. From the results in this section and the next section, we can show that if it is assumed that primes are asymptotically equally distributed among reduced residue classes, then if we first choose a fixed integer $a$ in $\mathbb{Z}$ and we then randomly choose a prime $p$ then there is (asymptotically) a fifty percent chance that $a$ is a residue of $p$.

**Theorem 3.4.2.** The product of two residues of a prime $p$ is a residue; the product of a residue and a nonresidue is a nonresidue; and the product of two nonresidues is a residue.

*Proof.* Suppose that $a$ and $b$ are residues. Then there exist integers $x$ and $y$ such that $x^2 \equiv a$ and $y^2 \equiv b \pmod{p}$.

Therefore, $(xy)^2 \equiv ab \pmod{p}$ and thus, the product $ab$ is a residue of $p$.

Now suppose that $a$ is a residue and $b$ is a nonresidue. Then there exists an integer $x$ such that $x^2 \equiv a \pmod{p}$.

We now proceed by contradiction. Let us suppose that the product $ab$ is a residue. Then there exists an integer $z$ such that $z^2 \equiv ab \pmod{p}$. Let $t \equiv zx^{-1} \pmod{p}$. Then $x^2t^2 \equiv z^2 \equiv ab \pmod{p}$ and $x^2 \equiv a \pmod{p}$. Therefore, $t^2 \equiv b \pmod{p}$ and $b$ is a residue, which is a contradiction. Therefore, the product $ab$ is a nonresidue.

Now let us suppose that $a$ and $b$ are two nonresidues. Let $k = \frac{p-1}{2}$, let $R = \{r_1, ..., r_k\}$ denote the residues in $\mathbb{Z}_p^* = \{1, 2, 3, ..., p-1\}$, and let $N = \{n_1, ..., n_k\}$ denote the nonresidues in $\mathbb{Z}_p^*$. Thus, $a, b \in N$.

We already know that the product of a residue and a nonresidue is a nonresidue. Therefore, $a-r_i$ is a nonresidue for all $i$ such that $1 \leq i \leq k$ and since $a$ is invertible these nonresidues are noncongruent modulo $p$. The number of nonresidues is $k$. Therefore, $N = \{a-r_1, ..., a-r_k\}$.
Now $a$ is invertible modulo $p$. Thus, if $ab \in N$ then $ab = a \cdot r$, and so $b = r$, but it was assumed that $b$ is a nonresidue. Thus, $ab \not\in N$ which means that $ab \in R$. Therefore, $ab$ is a residue.

In the next section we shall give another proof of Theorem 3.4.2 that uses the Legendre symbol.

The next result is now known as Euler’s criterion and can be proved as in Koshy [1] or Hardy and Wright [3] by using Fermat’s little theorem (Theorem 2.3.1) and the existence part of Theorem 2.3.7, which states that every prime has a primitive congruence root:

**Theorem 3.4.3** (Euler’s Criterion). If $a$ is an integer not divisible by an odd prime $p$ then $a$ is a residue of $p$ if $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ and $a$ is a nonresidue of $p$ if $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

Note that Euler’s criterion follows immediately from 2.3.15. In the sections that follow, we shall use the Legendre symbol to restate Euler’s criterion and eventually prove it as a consequence of Wilson’s theorem.

### 3.4.2 The Quadratic Nature of $-1$ modulo a Prime

We begin our analysis of quadratic residues by investigating the quadratic nature of the integers $\pm 1$ modulo a prime $p$. We then consider the quadratic nature of the integers $\pm 2$, $\pm 3$, and $\pm 5$. Note that the integer $+1$ is trivially a residue of every prime. Thus, we begin with the integer $-1$.

We do this in the result that follows. The result that follows is extremely useful in number theory. As we will see, it can be used to prove special cases of Dirichlet’s theorem and, as we have already seen, it can be used to prove Fermat’s two squares theorem (Theorem 3.3.2) in three different ways.

**Theorem 3.4.4.** $-1$ is a residue of all primes of the form $4n + 1$ and a nonresidue of all primes of the form $4n + 3$.

Note, that Theorem 3.4.4 is essentially the same as Theorem 3.3.1. Theorem 3.3.1 is written in terms of quadratic congruences while Theorem 3.4.4 is written in terms of quadratic residues.

Also, note that Theorem 3.4.4 can be generalized to allow for composite moduli. Here, we prove this result for prime moduli of the forms $4n + 1$ and $4n + 3$. The result for composite
moduli of the forms $4n + 1$ and $4n + 3$ will then follow by results in Gauss’ paper [7] that we shall not mention. As mentioned before, we are only interested in prime moduli. We now give four different proofs as follows: The first three of these proofs are from [7] while the fourth is from [4].

**Proof.** Let $p$ have the form $p = 4n + 1$ let $a = -1$. Then $a^{\frac{p-1}{2}} = (-1)^{2n} \equiv 1 \pmod{p}$. If we let $p$ have the form $p = 4n + 3$ and $a = -1$. Then $a^{\frac{p-1}{2}} = (-1)^{2n+1} \equiv -1 \pmod{p}$.

The result now follows from Euler’s criterion (Theorem 3.4.3).

**Proof.** Let $H$ be the set of residues of a prime $p$ that are less than $p$ and exclude the residue 0. Thus, $H$ is the set of residues in the set $\mathbb{Z}_p^* = \{1, 2, 3, \ldots, p - 1\}$.

Note, that $H$ is a subgroup of $\mathbb{Z}_p^*$. This follows, from the fact that in any group $G$, the set of perfect squares form a subgroup of $G$.

Thus, by Theorem 3.4.1, the order of the group $H$ is: $|H| = \frac{p-1}{2}$.

If $p = 4n + 1$ then $|H|$ is even. If $p = 4n + 3$ then $|H|$ is odd. Note that every residue in $H$ has an inverse in $H$. Thus, we can write $H$ as a union of pairs as follows by pairing each element in $H$ with its inverse:

$$H = \bigcup_{xy \equiv 1 \pmod{p}} \{x, y\}.$$

Now, if $\{x, y\}$ is a pair of residues where $xy \equiv 1 \pmod{p}$ then it is possible for $x = y$. In this case, we say that $x$ is self-invertible modulo $p$.

Let $a$ be the number of self-invertible residues in $H$. That is, $a$ is the number of $x \in H$ with $x^2 \equiv 1 \pmod{p}$.

Let $2b$ be the number of residues in $H$ that are not self-invertible. That is, $b$ is the number of pairs $\{x, y\}$ such that $x \neq y$ and $xy \equiv 1 \pmod{p}$.

Therefore, $|H| = a + 2b$.

If $p = 4n + 1$ then $a$ is even. If $p = 4n + 3$ then $a$ is odd.

Now, from Theorem 2.1.2 the only elements in $\mathbb{Z}_p^*$ that are self-invertible are 1 and $p - 1$. Therefore, the only elements in $H$ that can be self-invertible are 1 and $p - 1$. Clearly $1 \in H$. Thus, $a = 1$ or $a = 2$. If $a = 2$ then $p - 1 \in H$. If $a = 1$ then $p - 1 \notin H$.

If $p = 4n + 1$ then $a = 2$ and therefore, $p - 1$ and hence also $-1$ is a residue of $p$. If $p = 4n + 3$ then $a = 1$ and therefore, $p - 1$ and hence also $-1$ is nonresidue of $p$.

The result now follows.
Proof. For this proof we shall use Wilson’s theorem (Theorem 2.1.1).

By Theorem 3.4.1, among the integers $Z^*_p = \{1, 2, ..., p - 1\}$ there are $\frac{p-1}{2}$ residues and $\frac{p-1}{2}$ nonresidues.

If $p = 4n + 1$ then the number of residues is even. If $p = 4n + 3$ then the number of residues is odd.

Let $H$ be the subgroup of residues in $Z^*_p$. Therefore, $|H| = \frac{p-1}{2}$ which is the number of residues.

Thus, if $p = 4n + 1$ then $|H|$ is even. Say, $|H| = 2n$. If $p = 4n + 3$ then $|H|$ is odd. Say, $|H| = 2n + 1$.

Let $a \in Z^*_p \setminus H$ be fixed. Thus, $a$ is a fixed nonresidue in $Z^*_p$.

By Theorem 3.4.2, the product of a residue and a nonresidue is a nonresidue and there are exactly $\frac{p-1}{2}$ nonresidues in $Z^*_p$. Thus, the set of nonresidues is the coset:

$$aH = \{ah : h \in H\}.$$  

With this, we have: $Z^*_p = H \cup aH$ and

$$\prod_{k \in Z^*_p} k = \left( \prod_{k \in H} k \right) \cdot \left( \prod_{k \in aH} k \right) = a^{|H|} \left( \prod_{k \in H} k \right)^2.$$  

Now, by Wilson’s theorem (Theorem 2.1.1):

$$\prod_{k \in Z^*_p} k \equiv -1 \pmod{p}.$$  

Thus, if $p = 4n + 1$ then $|H| = 2n$ and:

$$-1 \equiv a^{2n} \left( \prod_{k \in H} k \right)^2 \pmod{p}.$$  

Therefore, $-1$ is a residue modulo $p$.

If $p = 4n + 3$ then $|H| = 2n + 1$ and:

$$-1 \equiv a^{2n+1} \left( \prod_{k \in H} k \right)^2 = a \left( a^n \prod_{k \in H} k \right)^2 \in aH \pmod{p}.$$  

46
Thus,

\[-1 \in aH.\]

So \(-1\) is a nonresidue mod \(p\).

We now give a fourth proof of Theorem 3.4.4. In particular we shall prove Theorem 3.3.1, which is clearly equivalent to Theorem 3.4.4.

We now restate Theorem 3.3.1 as follows:

**Theorem 3.4.5.** Let \(p\) be prime. Then the congruence \(x^2 \equiv -1 \pmod{p}\) has a solution if and only if \(p = 2\) or \(p \equiv 1 \pmod{4}\).

This result appears as Theorem 2.12 in Niven, Zuckerman, and Montgomery [4].

The following proof, which like the previous proof uses Wilson’s theorem, is from pages 53-54 in Niven, Zuckerman, and Montgomery [4].

**Proof.** Let us suppose that there exists an integer \(x\) such that \(x^2 \equiv -1 \pmod{p}\) and that \(p\) is an odd prime.

Now, \(p\) does not divide \(x\). Therefore, by Fermat’s little theorem, we have:

\[x^{p-1} \equiv 1 \pmod{p}.\]

Now, \(p \neq 2\) and so \(\frac{p-1}{2}\) is an integer. Thus, from the congruence: \(x^2 \equiv -1 \pmod{p}\) we have:

\[(-1)^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} = x^{p-1} \equiv 1 \pmod{p}.\]

Thus

\[(-1)^{\frac{p-1}{2}} = 1,\]

which means that \(p \equiv 1 \pmod{4}\).

Conversely let \(p = 2\) or \(p \equiv 1 \pmod{4}\). If \(p = 2\) then the congruence \(x^2 \equiv -1 \pmod{2}\) has a solution \(x = 1\). We now let \(p \equiv 1 \pmod{4}\).

By Wilson’s theorem we have:

\[-1 \equiv (1)(2)(3)...(p - 1) \pmod{p}.\]
We now write this product as:

\[
(1)(2)(3)...(p - 1) = (1)(2)...(j)...\left(\frac{p - 1}{2}\right)(\frac{p + 1}{2})...(p - j)...(p - 1) = \prod_{j=1}^{p-1} j(p - j).
\]

Now

\[
\prod_{j=1}^{p-1} j(p - j) \equiv \prod_{j=1}^{p-1} (-1)j^2 = (-1)^{\frac{p-1}{2}} \left(\prod_{j=1}^{\frac{p-1}{2}} j \right)^2 = (-1)^{\frac{p-1}{2}} \left(\frac{p - 1}{2}!\right)^2
\]

and by Wilson:

\[
(-1)^{\frac{p-1}{2}} \left(\frac{p - 1}{2}!\right)^2 \equiv -1 \pmod{p}.
\]

Now, \( p \equiv 1 \pmod{4} \). Therefore, \( (-1)^{\frac{p-1}{2}} = 1 \). Thus, \( x = \frac{p-1}{2}! \) is a solution of the congruence \( x^2 \equiv -1 \pmod{p} \).

The following useful result allows us to determine the quadratic nature of an integer \(-a\) modulo a prime \( p \) given that we know the quadratic nature of \( a \) and the least residue of \( p \) modulo 4.

**Theorem 3.4.6.** If \( a \) is a residue of a prime of the form \( 4n + 1 \) then \(-a\) is a residue of this prime. If \( a \) is a nonresidue of a prime of the form \( 4n + 1 \) then \(-a\) is a nonresidue of this prime. If \( a \) is a residue of a prime of the form \( 4n + 3 \) then \(-a\) is a nonresidue of this prime. If \( a \) is a nonresidue of a prime of the form \( 4n + 3 \) then \(-a\) is a residue of this prime.

**Proof.** This follows immediately by Theorems 3.4.2 and 3.4.4.

**3.4.3 The Quadratic Nature of \( \pm 2 \) Modulo a Prime**

We continue our investigation of residues by considering the quadratic nature of \(+2\) and \(-2\).

**Theorem 3.4.7.** \(+2\) is a nonresidue and \(-2\) is a residue of all primes of the form \( 8n + 3 \).

**Theorem 3.4.8.** \(+2\) and \(-2\) are both nonresidues of all primes of the form \( 8n + 5 \).
Proof. We now prove these two results simultaneously.

We first show that no prime number of the forms \( 8n + 3 \) and \( 8n + 5 \) can have +2 as a residue.

We now proceed by the method of infinite descent. That is, we use contradiction and the well-ordering principle.

Suppose that our result is incorrect. Suppose that there is a prime number of the form \( 8n + 3 \) or \( 8n + 5 \) with residue +2. Thus, by the well-ordering principle, there exists a prime \( t \) of the form \( 8n + 3 \) or \( 8n + 5 \) with residue +2 and \( t \) is the least such prime.

Therefore, +2 is a residue of \( t \) but a nonresidue of all primes of the form \( 8n + 3 \) or \( 8n + 5 \) that are less than \( t \). Thus, we choose an integer \( a \) such that:

\[
a^2 \equiv 2 \pmod{t}.
\]

Note that from the proof of Theorem 3.1.1 the congruence: \( x^2 \equiv 2 \pmod{t} \) has two solutions that sum to \( t \) one solution is even while the other solution is odd. Thus, we can choose an integer \( a \) such that \( a \) is odd, \( a < t \), and \( a^2 \equiv 2 \pmod{t} \).

Let \( a = 2m + 1 \) for some integer \( m \) and let \( a^2 = 2 + tu \) for some integer \( u \).

Therefore, \( a^2 = (2m + 1)^2 = 4m(m + 1) + 1 \) and so \( a^2 \) has the form \( 8n + 1 \). Now, \( tu = a^2 - 2 \) has the form \( 8n - 1 \).

From this, we see that if \( t \) is of the form \( 8n + 5 \) then \( u \) is of the form \( 8n + 3 \) and if \( t \) is of the form \( 8n + 3 \) then \( u \) is of the form \( 8n + 5 \).

Now, from \( a^2 = 2 + tu \), we have \( a^2 \equiv 2 \pmod{u} \), and so, +2 is a residue of \( u \).

Now, \( t > a \). Thus, \( t^2 > a^2 = 2 + tu > tu \). This gives, \( u < t \).

Thus, we have constructed the integer \( u \) of the form \( 8n + 3 \) or \( 8n + 5 \) where \( u < t \). If \( u \) is prime we have established a contradiction and the proof is complete. Now suppose \( u \) is composite of the form \( 8n + 3 \) or \( 8n + 5 \). If all prime factors of \( u \) are of the form \( 8n + 1 \) and \( 8n + 7 \) then \( u \) would be of one of these forms. Therefore, \( u \) has a prime factor of the form \( 8n + 3 \) or \( 8n + 5 \). This prime factor is less than \( t \) and has +2 as a residue. Again we have established a contradiction.

Therefore, there are no primes of the form \( 8n + 3 \) or \( 8n + 5 \) that have +2 as a residue. In other words, +2 is a nonresidue of all primes of the form \( 8n + 3 \) or \( 8n + 5 \).

Now an integer of the form \( 8n + 3 \) is of the form \( 4n + 3 \) and an integer of the form \( 8n + 5 \) is of the form \( 4n + 1 \).

Thus, by Theorem 3.4.6, \( -2 \) is a residue of all primes of the form \( 8n + 3 \) and \( -2 \) is a nonresidue of all primes \( 8n + 5 \).
This completes the proof.

We now show the following:

**Theorem 3.4.9.** −2 is a nonresidue and +2 is a residue of all primes of the form $p = 8n + 7$.

Previously we proved Theorem 3.4.7 and Theorem 3.4.8 simultaneously. In a similar manner we now prove Theorem 3.4.8 and Theorem 3.4.9 simultaneously. Thus, in proving Theorem 3.4.9, we also have another proof of Theorem 3.4.8.

**Proof.** As before, we shall use the method of infinite descent or, what is the same thing, contradiction and the well-ordering principle.

We first show that −2 is a nonresidue of all primes of the form $8n + 5$ and of the form $8n + 7$.

Suppose that this is not the case. Thus, by the well-ordering principle we can choose $t$ such that $t$ is a prime of the form $8n + 5$ or of the form $8n + 7$, $t$ has −2 as a residue, and $t$ is least of these.

Thus, we can choose the integer $a$ such that $a$ is odd, $a < t$, and $a^2 \equiv -2 \pmod{t}$.

There exists an integer $u$ such that $a^2 = tu - 2$. Thus, −2 is a residue of $u$.

Now, $a$ is odd so $tu$ is of the form $8n + 3$. Therefore, if $t$ is of the form $8n + 7$ then $u$ is of the form $8n + 5$. If $t$ is of the form $8n + 5$ then $u$ is of the form $8n + 7$.

Now, $a \leq t - 1$, $t \geq 5$, and $tu = a^2 + 2$.

Thus,

$$tu = a^2 + 2 \leq (t - 1)^2 + 2 = t^2 - 2t + 3 \leq t^2 - 10 + 3 = t^2 - 7 < t^2.$$  

Therefore, $u < t$.

If $u$ is a prime then the inequality $u < t$ implies a contradiction. If $u$ is a composite then we note that if every prime factor of $u$ has the form $8n + 1$ or $8n + 3$ then $u$ has the form $8n + 1$ or $8n + 3$. Thus, if $u$ is composite then $u$ has a prime factor of the form $8n + 5$ or of the form $8n + 7$. This prime factor is less than $t$ and −2 is a residue of this prime factor. Thus, we have established a contradiction.

Therefore, −2 is a nonresidue of all primes of the form $8n + 5$ and the form $8n + 7$.

Now an integer of the form $8n + 5$ is of the form $4n + 1$ and an integer of the form $8n + 7$ is of the form $4n + 3$. Thus, by Theorem 3.4.6, +2 is a nonresidue of all primes of the form $8n + 5$ and +2 is residue of all primes of the form $8n + 7$.

50
This completes the proof. \hfill \Box

With these theorems we can determine the quadratic nature of $+2$ and $-2$ modulo a prime of the form $8n + 3$, $8n + 5$, or $8n + 7$. That is, we can determine whether $+2$ and $-2$ are residues or nonresidues modulo any odd prime not of the form $8n + 1$. We now consider a prime modulus of the form $8n + 1$.

We have the following:

**Theorem 3.4.10.** $+2$ and $-2$ are residues of any prime of the form $8n + 1$.

*Proof.* Consider the prime $p$ of the form $8n + 1$. Say $p = 8n + 1$.

Now by the existence part of Theorem 2.3.7, there exists $g$, a primitive congruence root modulo the fixed prime $p = 8n + 1$.

Therefore, $g^{p-1} \equiv 1 \pmod{p}$ and $g^k \not\equiv 1 \pmod{p}$ for all $1 \leq k < p - 1$.

Thus,

$$g^{\frac{p-1}{2}} = g^{4n} \not\equiv 1 \pmod{p}.$$  

By Fermat’s little theorem (Theorem 2.3.1):

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

Therefore,

$$g^{4n} \equiv -1 \pmod{p},$$

$$(g^{2n} + 1)^2 = g^{4n} + 2g^{2n} + 1 \equiv 2g^{2n} \pmod{p},$$

and

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

Therefore, since $g^{2n} \not\equiv 0 \pmod{p}$, both $2g^{2n}$ and $-2g^{2n}$ are residues of the prime $p$. It now follows by Theorem 3.4.2 that both $+2$ and $-2$ are residues modulo $p = 8n + 1$.  

\hfill \Box
Thus, we arrive at the following general result that completely determines the quadratic nature of $+2$ and $-2$ modulo any odd prime.

**Theorem 3.4.11.** $+2$ is a residue of all primes of the form $8n + 1$ and $8n + 7$. $+2$ is a nonresidue of all primes of the form $8n + 3$ and $8n + 5$. $-2$ is a residue of all primes of the form $8n + 1$ and $8n + 3$. $-2$ is a nonresidue of all primes of the form $8n + 5$ and $8n + 7$.

Note that if we assume that the primes are asymptotically equally distributed among reduced residue classes then the previous general result tells us that if an odd prime $p$ is chosen randomly then there is a fifty percent chance that $2$ (or $-2$) is a residue (or nonresidue) of $p$.

### 3.4.4 The Quadratic Nature of $\pm 3$ Modulo a Prime

We now consider integers $+3$ and $-3$ modulo a prime number $p$. As before we consider proof by cases, depending on which reduced residue class the modulus $p$ belongs to. Before, when we considered the quadratic nature of $+2$ and $-2$ modulo a prime $p$ we considered cases depending on which residue class in $\mathbb{Z}_8$ that $p$ belongs to. In considering the quadratic nature of $+3$ and $-3$ modulo a prime $p$ we consider cases depending on which residue class in $\mathbb{Z}_{12}$ that $p$ belongs to. Recall that in our investigation of the quadratic nature of $+2$ and $-2$ modulo a prime $p$ we considered only odd primes. That is, we excluded the prime $p = 2$. Here we exclude the primes 2 and 3 which are the prime factors of 12. Our modulus $p$ (where $p$ is a prime not equal to 2 or 3) will belong to one of the following classes in $\mathbb{Z}_{12}$: $(1), (5), (7), (11)$. We use the notation $(a)$ to denote the residue class $(a) = \{x \in \mathbb{Z} \mid x \equiv a \ (mod\ 12)\}$ in $\mathbb{Z}_{12}$. In other words, the prime modulus $p$ (which is any prime not 2 and not 3) will have one of the following forms: $12n + 1, 12n + 5, 12n + 7, 12n + 11$.

We have the following two results that we shall prove simultaneously:

**Theorem 3.4.12.** $-3$ and $+3$ are nonresidues of primes of the form $12n + 5$.

**Theorem 3.4.13.** $-3$ is a nonresidue and $+3$ is a residue of primes of the form $12n + 11$.

**Proof.** We start with $-3$. We first show that there is no prime of the form $6n + 5$ that has $-3$ as a residue. As in the proof of Theorems 3.4.7 and 3.4.8, we proceed by method of infinite descent which boils down to a proof by contradiction and the well-ordering principle.

Suppose that the result is false. Therefore, there exists a prime $t$ of the form $6n + 5$ that has $-3$ as a residue. Now, by the well-ordering principle, there exists such a $t$, where $t$ is the least such prime.
Thus, there exists integers $a$ and $u$ such that $tu = a^2 + 3$, $u$ is odd, $a$ is even, and $a < t$.

Now, $a \leq t - 1$, $t \geq 5$, and $tu = a^2 + 3$.

Thus,

$$tu = a^2 + 3 \leq (t - 1)^2 + 3 = t^2 - 2t + 4 \leq t^2 - 10 + 4 = t^2 - 6 < t^2.$$  

Therefore, $u < t$. We have shown that $-3$ is a residue of $u$ and that $u < t$.

Now, $a$ is even. Therefore, $a$ will be of one of the following forms: $6n$, $6n + 2$, or $6n + 4$. We consider each of these cases separately as follows:

For the first case, let us suppose that $a$ is of the form $6n$. Thus, $tu = a^2 + 3 = 36n^2 + 3$.

Therefore, $tu$ has the form $36n + 3$, $\frac{tu}{3}$ has the form $12n + 1$, and since $u$ has the form $6n + 5$ it follows that $\frac{u}{3}$ has the form $6n + 5$.

However, $-3$ is a residue of $u$ and therefore also a residue of $\frac{u}{3}$ and $\frac{u}{3} < t$. If $\frac{u}{3}$ is prime then it is less than $t$ and we have a contradiction. If $\frac{u}{3}$ is composite then it has a prime factor of the form $6n + 5$ and again we have a contradiction.

For the second case, let us suppose that $a$ is of the form $6n + 2$. Thus, $tu = a^2 + 3 = (6n + 2)^2 + 3 = 6(6n^2 + 4n) + 7$. Therefore, $tu$ has the form $6n + 1$ and since $t$ has the form $6n + 5$ it follows that $u$ has the form $6n + 5$. Now $u < t$. Thus, if $u$ is prime then we have constructed a prime less than $t$ and so we have a contradiction. If $u$ is composite then it has a prime factor of the form $6n + 5$ and again, we have a contradiction.

For the third case, let us suppose that $a$ is of the form $6n + 4$. Thus, $tu = a^2 + 3 = (6n + 4)^2 + 3 = 36n^2 + 48n + 19$. Therefore, $tu$ has the form $6n + 1$ and since $t$ has the form $6n + 5$ it follows that $u$ has the form $6n + 5$. As in the previous case, $u$ is a prime of the form $6n + 5$ or $u$ has a prime factor of the form $6n + 5$. Either way, $u < t$ means we have constructed a prime less than $t$ and so we have established a contradiction.

Therefore, $-3$ is a nonresidue of every prime of the form $6n + 5$.

Now every integer of the form $12n + 5$ or $12n + 11$ is of the form $6n + 5$. Thus, $-3$ is a nonresidue of primes of the form $12n + 5$ and of the form $12n + 11$.

Every integer of the form $12n + 5$ is of the form $4n + 1$ and every integer of the form $12n + 11$ is of the form $4n + 3$. Thus, by Theorem 3.4.6, $+3$ is a nonresidue of primes of the form $12n + 5$ and $+3$ is a residue of all primes of the form $12n + 11$.

The result now follows.

\[ \Box \]

It can be shown by a proof similar to the proof of Theorems 3.4.8 and 3.4.9, that $+3$ is
a nonresidue of all primes of the forms $12n + 5$ and $12n + 7$. Although, we already know that $+3$ is a nonresidue of all primes of the form $12n + 5$. As before, we can prove these two results simultaneously by the method of infinite descent, which is the same as proof by contradiction and an application of the well-ordering principle. Any integer of the form $12n + 5$ is of the form $4n + 1$ and every integer of the form $12n + 7$ is of the form $4n + 3$. Thus, by Theorem 3.4.6, we have the following two results:

**Theorem 3.4.14.** $+3$ and $-3$ are nonresidues of primes of the form $12n + 5$.

**Theorem 3.4.15.** $+3$ is a nonresidue and $-3$ is a residue of primes of the form $12n + 7$.

We have stated and proved results concerning the quadratic nature of $+3$ and $-3$ modulo a prime $p$ where $p$ is in one of the following reduced residue classes: $(5)$, $(7)$, and $(11)$, where these classes are sets in $Z_{12}$. That is, we have considered primes of the forms: $12n + 5$, $12n + 7$, and $12n + 11$. It only remains to consider the prime modulus $p$ to be a prime in the class $(1)$. That is, it remains to consider the prime modulus $p$ to be of the form $12n + 1$.

We first prove the following:

**Theorem 3.4.16.** $-3$ is a residue of all primes of the form $3n + 1$.

*Proof.* Let $p = 3n + 1$.

By the existence part of Theorem 2.3.7 there exists $g$, a primitive congruence root of the fixed prime $p = 3n + 1$.

Let $a = g^{\frac{p-1}{3}}$.

Thus, with this choice of $a$, and from Theorem 2.3.1, we have $ord_p a = 3$. That is, there exists an integer $a$ such that $a^3 \equiv 1 \pmod{p}$, $a^1 \not\equiv 1 \pmod{p}$, and $a^2 \not\equiv 1 \pmod{p}$.

Now, $p|(a^3 - 1)$. Therefore, $p|(a - 1)(a^2 + a + 1)$. Thus $p|(a^2 + a + 1)$, by Euclid’s lemma (Lemma 2.1.1), and so $p|(4a^2 + 4a + 4)$.

Therefore,

$$4a^2 + 4a + 1 + 3 \equiv 0 \pmod{p}.$$  

This gives the following:

$$(2a + 1)^2 \equiv -3 \pmod{p}.$$  

This means that $-3$ is a residue of $p$. 

\[ \Box \]
Note that a prime of the form $12n + 1$ is of the form $3n + 1$ and of the form $4n + 1$. Thus, by theorem 3.4.6, we have:

**Theorem 3.4.17.** $+3$ and $-3$ are residues of primes of the form $12n + 1$.

Also note that a prime of the form $12n + 7$ is of the form $3n + 1$ and of the form $4n + 3$. Thus, we now have a second proof of Theorem 3.4.15.

We now have the following result which completely determines the quadratic nature of $+3$ and $-3$ modulo a prime $p$:

**Theorem 3.4.18.** $+3$ and $-3$ are residues of all primes of the form $12n + 1$. $+3$ and $-3$ are nonresidues of all primes of the form $12n + 5$. $+3$ is a nonresidue and $-3$ is a residue of all primes of the form $12n + 7$. $+3$ is a residue and $-3$ is a nonresidue of all primes of the form $12n + 11$.

Now, by Theorem 3.4.16, $-3$ is a residue of all primes $p$ of the form $3n + 1$. If $p$ is a residue of $3$ then $p$ is of the form $3n + 1$. It now follows that $-3$ is a residue of all primes that are residues of $3$.

Now, by the proof of Theorems 3.4.12 and 3.4.13, $-3$ is a nonresidue of all primes of the form $6n + 5$. Any prime of the form $3n + 2$ is either equal to $2$ or is of the form $6n + 5$. Therefore an odd prime $p$ is of the form $3n + 2$ if and only if $p$ is a nonresidue of $3$. Thus, $-3$ is nonresidue of all primes that are nonresidues of $3$.

Thus, we have proved the following key result:

**Theorem 3.4.19.** $-3$ is a residue of all odd primes that are residues of $3$ and $-3$ is a nonresidue of all odd primes that are nonresidues of $3$.

Thus, for any odd prime $p$, $-3$ is a residue of $p$ if and only if $p$ is a residue of $3$.

Thus, we have established a connection between the quadratic nature of $-3$ modulo an odd prime $p$ and the quadratic nature of $p$ modulo the prime $3$. This evidence suggests a general result, first proved by Gauss, who referred to it in [7] as the fundamental theorem.

In the next section we state a result using the Legendre symbol that generalizes Theorem 3.4.19 and is equivalent to Gauss’ fundamental theorem. This result is now known as the law of quadratic reciprocity.

### 3.4.5 The Quadratic Nature of $\pm 5$ Modulo a Prime

We now turn our attention to the quadratic nature of $+5$ and $-5$ modulo a prime $p$. 
Theorem 3.4.20. +5 is a nonresidue of odd primes of the form $5n + 2$ and of the form $5n + 3$. In other words, +5 is a nonresidue of all odd primes that are nonresidues of 5.

Proof. As before, we proceed by the method of infinite descent.

Let $t$ be an odd prime that is a nonresidue of 5, +5 is a residue of $t$, and $t$ is the least such prime.

Let $a^2 = 5 + tu$, $a$ is even, and $a < t$. Then $u$ is odd and $u < t$. Clearly, +5 is a residue of $u$.

We now consider two cases. One case where $5 \nmid a$ and another case where $5 | a$.

Consider the first case where $5 \nmid a$. Thus, $5 \nmid u$. Now, $tu$ is a residue of 5. Therefore, since $t$ is a nonresidue of 5 by Theorem 3.4.2, $u$ is a nonresidue of 5. Thus, there exists an odd integer $u$ such that $u < t$, $u$ is a nonresidue of 5, and +5 is a residue of $u$. Now, $u$ is prime or has a prime factor of the form $5n + 2$ or $5n + 3$. Either way, this contradicts $t$ being the least such prime, and so the result follows.

Consider the second case where $5 | a$. Thus, $5 | u$.

Let $a = 5b$ and let $u = 5v$. Now, $tu = a^2 - 5$. Thus, $(tv)u = a^2v - 5v$ and $(tv)(5v) = 25b^2v - 5v$.

Thus $tv = 5b^2 - 1$. This becomes:

$$tv \equiv -1 \equiv 2^2 \pmod{5}.$$ 

Therefore $tv$ is a residue of 5 and $t$ is a nonresidue of 5.

Thus, $v$ is a nonresidue of 5, +5 is a residue of $v$, $v$ is odd, and $v < t$.

We now have established a contradiction as in the previous case.

Note that primes of the form $20n + 13$ are of the form $5n + 3$ of the form $4n + 1$. Primes of the form $20n + 17$ are of the form $5n + 2$ and of the form $4n + 1$. Primes of the form $20n + 3$ are of the form $5n + 3$ and of the form $4n + 3$. Primes of the form $20n + 7$ are of the form $5n + 2$ and of the form $4n + 3$.

Thus, by Theorem 3.4.6, we have the following:

Theorem 3.4.21. +5 is a nonresidue of all primes of the form $20n + 13$, $20n + 17$, $20n + 3$, and $20n + 7$. −5 is a residue of all primes of the form $20n + 3$ and $20n + 7$ and is a nonresidue of all primes of the form $20n + 13$ and $20n + 17$.

We now show the following:
Theorem 3.4.22. +5 is a residue of all primes of the form $5n + 1$ and $5n + 4$. In other words, +5 is a residue of all odd primes that are residues of $5$.

From this we immediately have the following:

Theorem 3.4.23. +5 is a residue of all primes of the form $20n + 1$, $20n + 9$, $20n + 11$, and $20n + 19$. $−5$ is a residue of all primes of the form $20n + 1$ and $20n + 9$ and a nonresidue of all primes of the form $20n + 11$ and $20n + 19$.

We now prove Theorem 3.4.22 as follows:

Proof. We now show that +5 is a residue of all of all primes of the form $5n + 1$ and $5n + 4$.

First, let $p = 5n + 1$.

By the existence part of Theorem 2.3.7 there exists $g$ a primitive congruence root of the fixed prime $p = 5n + 1$.

Let $a = g^{\frac{p-1}{5}}$. Thus, there exists an integer $a$ such that $\text{ord}_p a = 5$. Therefore,

$$a^5 \equiv 1 \pmod{p}.$$  

So

$$(a - 1)(a^4 + a^3 + a^2 + a + 1) \equiv 0 \pmod{p}.$$  

Now $a - 1 \not\equiv 0 \pmod{p}$. Thus

$$(a^4 + a^3 + a^2 + a + 1) \equiv 0 \pmod{p}$$

and

$$4(a^4 + a^3 + a^2 + a + 1) = (2a^2 + a + 2)^2 - 5a^2 \equiv 0 \pmod{p}.$$  

Therefore, $5a^2$ is a quadratic residue of $p$ and by Theorem 3.4.2, +5 is a residue of $p$.

Next, let $p = 5n + 4$ and let $b$ be a fixed nonresidue modulo $p$. Let:

$$A = \frac{(x + \sqrt{b})^{p+1} - (x - \sqrt{b})^{p+1}}{\sqrt{b}}.$$  

Now by the binomial theorem, we have the following:
A = \frac{1}{\sqrt{b}} \left( \sum_{k=0}^{p+1} \binom{p+1}{k} x^{p+1-k} \sqrt{b}^k - \sum_{k=0}^{p+1} \binom{p+1}{k} (-1)^k x^{p+1-k} \sqrt{b}^k \right) \\
= 2 \sum_{j=0}^{p-1} \binom{p+1}{2j+1} x^{p-2j} b^j.

Now, the binomial coefficient \binom{p+1}{2j+1} contains a factor of \( p \) unless \( j = 0 \) or \( j = \frac{p-1}{2} \). Thus,

\[ A \equiv 2(p+1)x^p + 2(p+1)x b^{\frac{p-1}{2}} \pmod{p} \]

\[ \equiv 2(p+1)(x^p + x b^{\frac{p-1}{2}}) \pmod{p}. \]

Now, by Euler’s criterion (Theorem 3.4.3) we have:

\[ b^{\frac{p-1}{2}} \equiv -1 \pmod{p} \]

and by Fermat’s little theorem (Theorem 2.3.1) we have:

\[ x^p \equiv x \pmod{p}. \]

Thus for every integer \( x \) we have that \( A \equiv 0 \pmod{p} \). In other words, all the integers in \( Z_p = \{0, 1, 2, ..., p-1\} \) are roots of \( A \equiv 0 \pmod{p} \).

Let:

\[ B = \frac{(x + \sqrt{b})^e - (x - \sqrt{b})^e}{\sqrt{b}} \]

and let \( e | (p + 1) \).

From this, it follows that for any \( x \), \( B | A \) so let us write \( A = BC \). Now, \( deg A = p \) and \( deg B = e - 1 \). Now, \( deg C = deg A - deg B \). Therefore, \( deg C = p - (e - 1) = p - e + 1 \).

Thus, by Lagrange’s theorem (Theorem 2.4.1), the congruence: \( C \equiv 0 \pmod{p} \) has at most \( p - e + 1 \) solutions in \( Z_p \). Therefore, the congruence: \( B \equiv 0 \pmod{p} \) has at least \( e - 1 \) solutions in \( Z_p \).

We now let \( p = 5n + 4, e = 5, b \) a nonresidue of \( p \), and the integer \( a \) such that:
\[ B = \frac{(a + \sqrt{b})^5 - (a - \sqrt{b})^5}{\sqrt{b}} \equiv 0 \pmod{p}. \]

Now

\[ B = 10a^4 + 20a^2b + 2b^2 = 2((b + 5a^2)^2 - 20a^4). \]

Thus

\[ (b + 5a^2)^2 \equiv 20a^4 \pmod{p}. \]

Therefore, \(20a^4\) is a residue. Now, \(4a^4\) is a residue and \(20a^4 = (5)(4a^4)\). Therefore, by Theorem 3.4.2, we have that \(+5\) is a residue of \(p\).

\[ \square \]

From Theorems 3.4.20 and 3.4.22 we have the following:

**Theorem 3.4.24.** \(+5\) is a residue of all odd primes that are residues of \(5\). \(+5\) is a nonresidue of all odd primes that are nonresidues of \(5\).

**Proof.** \(+5\) is a residue of all primes of the forms: \(20n + 1\), \(20n + 9\), \(20n + 11\), and \(20n + 19\). Each of these primes is a residue of \(5\).

\(+5\) is a nonresidue of all primes of the form \(20n + 3\), \(20n + 7\), \(20n + 13\), and \(20n + 17\). Each of which is a nonresidue of \(5\).

In this proof we have accounted for all primes except for \(2\) and \(5\). It is easy to see that the theorem holds for the prime \(p = 5\) and fails for the prime \(p = 2\).

\[ \square \]

In the next section, we note that Theorem 3.4.24 is a special case of a more general result now known as the law of quadratic reciprocity. The law of quadratic reciprocity is concisely written using the Legendre symbol.
3.5 Quadratic Residues: Evaluating the Legendre Symbol

3.5.1 The Legendre Symbol

We now further pursue the problem: given an integer \( a \) and a prime \( p \), is \( a \) a residue or nonresidue of \( p \)? If the integer \( a \) is one of \( \pm 1, \pm 2, \pm 3, \) or \( \pm 5 \) then this is a simple matter of determining the least residue of \( p \) modulo 4, 8, 12, or 20 respectively. We then apply the previous results in [7] due to Gauss. We now discuss more general methods for solving this problem.

We first introduce the Legendre symbol \((a/p)\) as in [3], [1], [8], and [4]. This allows us to concisely express results concerning quadratic residues modulo a prime:

\[
(a/p) = \begin{cases} 
+1 & \text{if } a \text{ is a quadratic residue of } p \\
-1 & \text{if } a \text{ is a quadratic nonresidue of } p
\end{cases}
\]

Some authors write the Legendre symbol \((a/p)\) as \( (a \pmod{p}) \) or as \( (a|p) \).

We now discuss several different ways of determining the quadratic nature of an integer \( a \) modulo a prime \( p \). In other words, we discuss different methods of determining the Legendre symbol \((a/p)\).

Our first such method is the following result known as Euler’s criterion. We have already stated this result in Theorem 3.4.3. We now restate this key result using the Legendre symbol as follows:

**Theorem 3.5.1 (Euler’s Criterion).** Let \( p \) be an odd prime, \( a \) an integer, and \( p \nmid a \). Then

\[
(a/p) \equiv a^{\frac{p-1}{2}} \pmod{p}.
\]

We now give an example:

We now use Euler’s criterion (Theorem 3.5.1) to evaluate the Legendre symbol \((5/13)\) as follows:

\[
(5/13) = (a/p) \equiv a^{\frac{13-1}{2}} = 5^{6} = 15625 \equiv -1 \pmod{13}
\]

Thus, \((5/13) = -1\). It now follows from Euler’s criterion (Theorem 3.5.1) that \( 5 \) is a nonresidue of 13.

Our next example is known as Gauss’ lemma. Most number theory books, including [3],
Theorem 3.5.2 (Gauss’ lemma). Let \( p \) be an odd prime, let \( a \) be an integer, let \( p \nmid a \), let \( v \) be the number of least positive residues of the integers: \( 1a, 2a, 3a, \ldots, \frac{p-1}{2}a \mod p \) that exceed \( \frac{p}{2} \). Then \( (a/p) = (-1)^v \).

We now give an example: We now use Gauss’ lemma (Theorem 3.5.2) to evaluate the Legendre symbol \((5/13)\).

Now \( \frac{p-1}{2} = \frac{13-1}{2} = 6 \). We now consider the set of integers: \( \{1\cdot5, 2\cdot5, 3\cdot5, 4\cdot5, 5\cdot5, 6\cdot5\} = \{5, 10, 15, 20, 25, 30\} \). The set of least residues modulo 13 of the elements in this set is: \( \{5, 10, 2, 7, 12, 4\} \).

Among this set of least residues the numbers: \( \{10, 7, 12\} \) exceed \( \frac{p}{2} = \frac{13}{2} \). Therefore, there are exactly \( v = 3 \) elements in \( \{5, 10, 2, 7, 12, 4\} \) that exceed \( \frac{p}{2} = \frac{13}{2} \). By Gauss’ lemma it follows that \( (5/13) = (-1)^3 = -1 \). Thus, we conclude that 5 is a nonresidue of 13.

Now, Euler’s criterion (Theorem 3.5.1) and Gauss’ lemma (Theorem 3.5.2) give methods for computing the Legendre symbol. However, there are other methods that are computationally more efficient. We mention two such methods here.

That is, we mention the law of quadratic reciprocity and, in the next section, the generalized law of quadratic reciprocity.

We now state the law of quadratic reciprocity in terms of the Legendre symbol. This result together with the following results in this section that contain the Legendre symbol appear in [3], [1], [8], and [4] on pages 86-98, 498-533, 71-80, and 131-147 respectively.

Theorem 3.5.3 (Law of Quadratic Reciprocity). If \( p \) and \( q \) are distinct odd primes then we have the following:

\[
(p/q)(q/p) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.
\]

Now, [3], [1], [8], and [4] each give proofs of the law of quadratic reciprocity (Theorem 3.5.3) and of Theorem 3.5.8. In [3], [1], and [4] these proofs use Gauss’ lemma (Theorem 3.5.2). Whereas, the proof that appears in Rademacher [8] uses Gaussian sums.

The law of quadratic reciprocity in this form is fine for theoretical purposes. However, for computing the Legendre symbol the following form of the law of quadratic reciprocity is easier to work with:

Theorem 3.5.4. If \( p \) and \( q \) are distinct odd primes then we have the following:
\[
(p/q) = \begin{cases} 
(q/p) & \text{if } p \equiv 1 \pmod{4} \text{ or } q \equiv 1 \pmod{4} \\
-(q/p) & \text{if } p \equiv q \equiv 3 \pmod{4} 
\end{cases}
\]

The previous result (Theorem 3.5.4) is an equivalent form of the law of quadratic reciprocity (Theorem 3.5.3) and generalizes Theorems 3.4.19 and 3.4.24.

Our goal is to efficiently evaluate the Legendre symbol: \((a/p)\).

If \(a\) is prime and \(p\) is odd, then we can apply quadratic reciprocity (Theorem 3.5.3) to rewrite the Legendre symbol as \(\pm 1\) times another (possibly more simple) Legendre symbol. If \(a\) is composite or \(p = 2\), then quadratic reciprocity tells us nothing. In the case that \(a\) is composite, we use the following result, whose proof follows from Euler’s criterion (Theorem 3.5.1):

**Theorem 3.5.5.** \((ab/p) = (a/p)(b/p)\).

From this it follows that the product of two quadratic residues is a quadratic residue, the product of two quadratic nonresidues is a quadratic residue, and the product of a quadratic residue and a quadratic nonresidue is a quadratic nonresidue. Thus, we have another proof of Theorem 3.4.2.

If we let \(b = a\) in the previous result we have the following:

**Theorem 3.5.6.** \((a^2/p) = 1\).

With Theorem 3.5.5, in order to evaluate the Legendre symbol \((a/p)\) we first find the canonical decomposition of \(a\). Say \(a = p_1^{e_1}...p_k^{e_k}\). Thus, by Theorem 3.5.5 we have:

\[
(a/p) = (p_1^{e_1}...p_k^{e_k}/p) = (p_1^{e_1}/p)...(p_k^{e_k}/p) = (p_1/p)^{e_1}...(p_k/p)^{e_k}.
\]

The following result follows from the definition of a quadratic residue and tells us that in evaluating \((a/p)\) we can replace \(a\) by the least residue of \(a\) modulo \(p\):

**Theorem 3.5.7.** If \(a \equiv b \pmod{p}\) then \((a/p) = (b/p)\).

Thus, in evaluating the Legendre symbol \((a/p)\) we first replace the integer \(a\) with its least residue modulo \(p\). Next, we write \((a/p)\) as follows:

\[
(a/p) = (p_1^{e_1}...p_k^{e_k}/p) = (p_1^{e_1}/p)...(p_k^{e_k}/p) = (p_1/p)^{e_1}...(p_k/p)^{e_k}.
\]
We now consider the $k$ factors: $(p_i/p)^{e_i}$ where $1 \leq i \leq k$. If $e_i$ is even then $(p_i/p)^{e_i} = 1$ and if $e_i$ is odd then $(p_i/p)^{e_i} = (p_i/p)$. Thus:

$$(a/p) = \prod_{1 \leq i \leq k, e_i \text{ is odd}} (p_i/p).$$

We now use Theorem 3.5.4 to replace each $(p_i/p)$ in this product with $\pm (p/p_i)$. We then repeat this process for each $(p/p_i)$. Note that if at any of these steps we run into a Legendre symbol of the form: $(\pm 1/p)$, $(\pm 2/p)$, $(\pm 3/p)$, or $(\pm 5/p)$ then we can use the results in [7] due to Gauss that we mentioned in the previous section.

Clearly, the algorithm that we have just described must eventually terminate. Therefore, we can write the Legendre symbol $(a/p)$ as a product of Legendre symbols for which the law of quadratic reciprocity no longer applies. If $p$ is an odd prime then the Legendre symbols for which the law of quadratic reciprocity does not apply, are precisely the Legendre symbols: $(1/p)$, $(-1/p)$, $(2/p)$, and $(-2/p)$.

Now, clearly, we have $1/p = 1$ and $-2/p = (2/p)(-1/p)$. Thus, we need to know how to evaluate the Legendre symbols $(2/p)$ and $(-1/p)$. Both of these Legendre symbols can easily be evaluated using the results in [7] due to Gauss in the previous section.

We now write these results due to Gauss in terms of the Legendre symbol as follows:

The Legendre symbol $(2/p)$ can be evaluated by one of the following results which are equivalent to Theorem 3.4.11:

**Theorem 3.5.8.** If $p$ is an odd prime then

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

**Theorem 3.5.9.** If $p$ is an odd prime then

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

The Legendre symbol $(-1/p)$ can be evaluated by one of the following results which are equivalent to Theorems 3.4.4 and 3.4.5.

**Theorem 3.5.10.** If $p$ is an odd prime then

$$(-1/p) = (-1)^{\frac{p-1}{2}}.$$
Theorem 3.5.11. If $p$ is an odd prime then

$\left( -1/p \right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4} \end{cases}$.

Let $k$ be a positive integer. A Dirichlet character modulo $k$ is a function $\chi : \mathbb{Z} \to \mathbb{C}$ that satisfies the following conditions:

1. $\chi(1) \neq 0$
2. $\chi(a) = 0$ whenever $\gcd(a, k) > 1$
3. $\chi(a_1 a_2) = \chi(a_1) \chi(a_2)$ for all $a_1, a_2 \in \mathbb{Z}$
4. $\chi(a_1) = \chi(a_2)$ whenever $a_1 \equiv a_2 \pmod{k}$

Note, that from Theorems 3.5.5 and 3.5.7 and from the trivial fact that $(1/p) = 1 \neq 0$, the function $\chi(a) = (a/p)$ satisfies conditions 1, 3, and 4 given previously with $k = p$. If we define $(a/p)$ to be equal to 0 if $p|a$ then condition 2 is also satisfied. Thus, for fixed prime $p$, the function $(a/p)$ is a Dirichlet character modulo $p$.

As we mentioned previously, Gauss considered the integer 0 to be a quadratic residue modulo every prime $p$. This makes sense algebraically. However, results like Euler’s criterion (Theorem 3.4.3) must be modified if 0 is allowed to be a valid quadratic residue. If, as most modern mathematicians do, we are to agree that 0 is neither a quadratic residue nor a nonresidue, we then have two choices in defining the Legendre symbol. Choice one is to make $(a/p)$ undefined when $p|a$. Choice two is to make $(a/p) = 0$ when $p|a$. From our previous remark, if we choose to make $(a/p) = 0$ when $p|a$ then the Legendre symbol $(a/p)$ is a Dirichlet character modulo $p$. Also, if $p|a$ then $a^{\phi(p)} \equiv 1 \pmod{p}$. Thus, defining $(a/p)$ to be 0 whenever $p|a$ agrees with Euler’s criterion (Theorem 3.4.3).

With the previous results, we have all the tools we need to compute the Legendre symbol $(a/p)$. Computing the Legendre symbol using quadratic reciprocity and results due to Gauss is much more efficient than using Gauss’ lemma (Theorem 3.5.2) or Euler’s criterion (Theorem 3.5.1).

We now give an example. We now use the methods of this section to evaluate the Legendre symbol $(171/101)$ as follows:

Now, $171 \equiv 70 \pmod{101}$. Thus, by Theorem 3.5.7, $(171/101) = (70/101)$.

We now write 70 as the following canonical decomposition: $70 = 2 \cdot 5 \cdot 7$. 

64
By Theorem 3.5.5 we have: \((70/101) = (2 \cdot 5 \cdot 7/101) = (2/101)(5/101)(7/101)\).

We now evaluate each of the Legendre symbols: \((2/101), (5/101), \text{ and } (7/101)\) separately using results in this section.

\[(2/101) = (-1)\]

\[(5/101) = (101/5) = (1/5) = 1\]

\[(7/101) = (101/7) = (3/7) = (-1)(7/3) = (-1)(1/3) = (-1)(1) = -1\]

Thus, we now have:

\[(171/101) = (-1)(1)(-1) = 1\]

We now conclude that 171 is a residue of 101.

In the next section we describe a method even more efficient than quadratic reciprocity.

### 3.5.2 The Jacobi Symbol

The definition and properties of the Jacobi symbol mentioned here can be found in Koshy [1] and in Niven, Zuckerman, and Montgomery [4] on pages 527-534 and 142-147 respectively.

We define the Jacobi symbol \((a/m)\) in terms of the Legendre symbol as follows:

Let \(m\) be an odd positive integer with canonical decomposition \(m = \prod_{j=1}^{k} p_j^{e_j}\). Let \(a\) be an integer relatively prime to \(m\). We define the Jacobi symbol \((a/m)\) in terms of the Legendre symbol as follows:

\[(a/m) = \left(\frac{a}{\prod_{j=1}^{k} p_j^{e_j}}\right) = \prod_{j=1}^{k} (a/p_j)^{e_j}.\]

Here, \((a/p_j)\) is the Legendre symbol.

Note that all the Jacobi symbol results in this section are taken from Koshy [1].

From this it is clear that the Legendre symbol is a special case of the Jacobi symbol. Thus, any result that applies to the Jacobi symbol also applies to the Legendre symbol. Therefore, in evaluating the Legendre symbol, we can use properties of the Jacobi symbol. Also, note that if the congruence: \(x^2 \equiv a \pmod{m}\) has a solution then \((a/m) = 1\). To see
this, note that if the congruence: \( x^2 \equiv a \pmod{m} \) has a solution then for each prime factor \( p_i \) of \( m \) the congruence \( x^2 \equiv a \pmod{p_i} \) has a solution. Thus, for each prime factor \( p_i \) of \( m \) we have \( (a/p_i) = 1 \). Since the Jacobi symbol \( (a/m) \) is a product of Legendre symbols \( (a/p_i) \) where \( p_i \) divides \( m \), it follows that \( (a/m) = 1 \). Thus, if the congruence: \( x^2 \equiv a \pmod{m} \) has a solution then \( (a/m) = 1 \). The converse of this is not true in general.

The Jacobi symbol satisfies many of the same properties as the Legendre symbol. Indeed, we have the following results which generalize the properties of the Legendre symbol given previously. The following generalize Theorems 3.5.3, 3.5.4, 3.5.5, 3.5.7, 3.5.8, 3.5.9, 3.5.10, and 3.5.11. The first of these is known as the generalized law of quadratic reciprocity:

**Theorem 3.5.12** (Generalized Law of Quadratic Reciprocity). If \( m \) and \( n \) are odd relatively prime integers. Then

\[
(m/n)(n/m) = (-1)^{\frac{m-1}{2} \cdot \frac{n-1}{2}}. 
\]

**Theorem 3.5.13.** If \( m \) and \( n \) are odd relatively prime integers. Then

\[
(m/n) = \begin{cases} 
(n/m) & \text{if } m \equiv 1 \pmod{4} \text{ or } n \equiv 1 \pmod{4} \\
-(n/m) & \text{if } m \equiv n \equiv 3 \pmod{4}
\end{cases}
\]

**Theorem 3.5.14.** If \( m \) is an odd positive integer and \( a \) and \( b \) are integers both relatively prime to \( m \) then \( (ab/m) = (a/m)(b/m) \).

**Theorem 3.5.15.** If \( m \) is an odd positive integer and \( a \) and \( b \) are integers both relatively prime to \( m \) then if \( a \equiv b \pmod{m} \) then \( (a/m) = (b/m) \).

**Theorem 3.5.16.** If \( m \) is an odd positive integer. Then

\[
(2/m) = (-1)^{\frac{m^2-1}{8}}.
\]

**Theorem 3.5.17.** If \( m \) is an odd positive integer. Then

\[
(2/m) = \begin{cases} 
1 & \text{if } m \equiv \pm 1 \pmod{8} \\
-1 & \text{if } m \equiv \pm 3 \pmod{8}
\end{cases}
\]

**Theorem 3.5.18.** If \( m \) is an odd positive integer. Then

\[
(-1/m) = (-1)^{\frac{m-1}{2}}.
\]

66
Theorem 3.5.19. If $m$ is an odd positive integer. Then

$$(-1/m) = \begin{cases} 
1 & \text{if } m \equiv 1 \pmod{4} \\
-1 & \text{if } m \equiv 3 \pmod{4} 
\end{cases}.$$ 

We now use the previous results to evaluate the Legendre symbol $(a/p)$. We first replace the integer $a$ with its least residue modulo $p$. Now, every Legendre symbol is also a Jacobi symbol. Thus, if $a$ and $p$ are both odd and relatively prime, then we can apply the generalized law of quadratic reciprocity (Theorem 3.5.12 or Theorem 3.5.13) to $(a/p)$ to get the following:

$$(a/p) = \pm(p/a).$$

If $a$ is even then we use Theorem 3.5.14 to write the Legendre symbol $(a/p)$ as $(a/p) = (2/p)(b/p)$ where $b$ is odd. We now apply Theorem 3.5.17 to the symbol $(2/p)$ and Theorem 3.5.13 to the symbol $(b/p)$.

We now repeat this process. At each step we use Theorem 3.5.13 to evaluate the symbol $(a/p)$ where $a > 2$ is odd. We use Theorem 3.5.17 when $a = 2$ and Theorem 3.5.19 when $a = -1$.

Note that in applying the law of quadratic reciprocity to the Legendre symbol $(a/p)$, where $a < p$, we first write $a$ as a canonical decomposition. We then apply the law to get $(a/p)$ being equal to a product of Legendre symbols each of which must be evaluated the same way we evaluated $(a/p)$. Thus, at each step of this process, we write a Legendre symbol as a product of other Legendre symbols.

While, in applying the generalized law of quadratic reciprocity to the Legendre symbol $(a/p)$, where $p$ and $a$ are odd, relatively prime, and $a < p$, there is no need to write $a$ as a canonical decomposition. We simply apply the law to get $(a/p)$ being equal to $\pm 1$ times a single Jacobi symbol. Thus, we write a Jacobi symbol as $\pm 1$ times a single Jacobi symbol.

From this it is clear that evaluating a Legendre symbol using the generalized law of quadratic reciprocity is much less work than evaluating a Legendre symbol using the law of quadratic reciprocity.

As an example, consider the Legendre symbol $(171/101)$. We previously evaluated this Legendre symbol in the previous section. We now again evaluate this Legendre symbol this time using properties of the Jacobi symbol as follows:

$$(171/101) = (70/101) = (2/101)(35/101) = (-1)(101/35) =$$
\[
(-1)(31/35) = (-1)(-1)(35/31) = (-1)(-1)(4/31) = (-1)(-1)(+1) = 1
\]
Therefore, \((171/101) = 1\). Thus 171 is a residue of 101.

Thus, we have four methods for evaluating the Legendre symbol. These are: Euler’s criterion (Theorem 3.5.1), Gauss’ lemma (Theorem 3.5.2), the law of quadratic reciprocity (Theorem 3.5.3), and the generalized law of quadratic reciprocity (Theorem 3.5.12).

3.5.3 Quadratic Residues and Primitive Congruence Roots

In the previous sections we gave several methods for determining the quadratic nature of an integer \(a\) modulo a prime \(p\), where \(p \not| a\). In each of these methods we are essentially evaluating the single Legendre symbol \((a/p)\).

In this section we give a method from Rademacher [8], involving primitive congruence roots, for listing all the quadratic residues of the prime \(p\). We are essentially partitioning \(Z^*_p\) into two classes. One of these classes contains the residues of \(p\) while the other contains the nonresidues of \(p\).

The following result from page 70 of [8] in Rademacher’s chapter on Gaussian sums gives us such a method:

**Theorem 3.5.20.** Let \(p\) be an odd prime, let \(g\) be a primitive congruence root of \(p\).

Then the residues of \(p\) are: \(g^0, g^2, ..., g^{p-3}\). The nonresidues of \(p\) are: \(g^1, g^3, ..., g^{p-2}\).

Note that this result implies that each prime \(p\) has exactly \(p-1\) residues and \(p-1\) nonresidues. Thus, we now have another proof of Theorem 3.4.1.

It is interesting to note that Rademacher in [8] uses Theorem 3.5.20 as the definition of quadratic residues and quadratic nonresidues.

Also, note that from this theorem the exponents of the residues are even while the exponents of the nonresidues are odd. Since the sum of two even numbers is even, the sum of an even number and an odd number is odd, and the sum of two odd numbers is even; it follows that the product of a residue and a residue is a residue, the product of a residue and a nonresidue is a nonresidue, and the product of a nonresidue and a nonresidue is a residue. Thus, we have another proof of Theorem 3.4.2.

We use the following lemma from Koshy [1] to prove Theorem 3.5.20.

**Lemma 3.5.1.** Let \(m\) be a positive integer and let \(a\) be an integer relatively prime to \(m\). Let \(e = ord_m a\) be the order of \(a\) modulo \(m\). Then \(a^i \equiv a^j \pmod{m}\) if and only if \(i \equiv j \pmod{e}\).
We now use this lemma to prove Theorem 3.5.20. The proof we give is from page 70 in [8].

Proof. Let $p$ be an odd prime. Let $g$ be a primitive congruence root modulo $p$. Note, that by Theorem 2.3.7 the primitive congruence root $g$ exists, in fact there are $\phi(p-1)$ of them.

Let $a$ be an integer and $p \nmid a$. Then by Theorem 2.3.9, there exist a positive integer $u$ such that $g^u \equiv a \pmod{p}$.

Suppose that $a$ is a residue of $p$. Now, $a$ is a quadratic residue if and only if there exist an integer $x$ such that $x^2 \equiv a \pmod{p}$. Since $p \nmid a$ it follows from this congruence that $p \nmid x$. Again, by Theorem 2.3.9, there exist a positive integer $v$ such that $g^v \equiv x \pmod{p}$.

Thus, from the congruence $x^2 \equiv a \pmod{p}$ we have:

$$g^{2v} \equiv g^u \pmod{p}$$

From Lemma 3.5.1, this is equivalent to:

$$2v \equiv u \pmod{p-1}$$

Now, $2v$ and $p-1$ are even. Thus, $u$ is even. Therefore, $a$ is a residue if and only if there exists an even integer $u$ such that $a \equiv g^u \pmod{p}$.

This completes the proof. 

Thus, we now have a method, involving primitive congruence roots, for constructing the quadratic residues and quadratic nonresidues of an odd prime $p$. To apply this method we must first determine a primitive congruence root of $p$. If we were to use the methods in the previous section (such as quadratic reciprocity or generalized quadratic reciprocity) for constructing such a list, then this would involve evaluating the $p-1$ Legendre symbols: $(1/p), (2/p), \ldots, (p-1/p)$.

### 3.6 Wilson’s Theorem and the Legendre Symbol

We now follow Hardy and Wright [3] by proving Wilson’s theorem (Theorem 2.1.1) and Euler’s criterion (Theorem 3.5.1) using the notion of quadratic residues of a prime. These proofs are from pages 83-85 in [3]. The proofs that follow use the Legendre symbol and the definition of a quadratic residue. Note that these proofs do not use any of the properties
of quadratic residues (such as the law of quadratic reciprocity) that we mentioned in the previous section.

We first prove the following result, from Hardy and Wright [3], which establishes a connection between Wilson’s theorem, Euler’s criterion, and the Legendre symbol:

**Theorem 3.6.1.** If $p$ is an odd prime and $p \nmid a$ then

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

**Proof.** Let $p$ be an odd prime, $a$ an integer, and $p \nmid a$.

We consider two cases. In one case $a$ is a residue of $p$. In the second case $a$ is a nonresidue of $p$.

First, let us suppose that $a$ is a residue of $p$. We write this in terms of the Legendre symbol as $(a/p) = 1$. Therefore, the congruence $x^2 \equiv a \pmod{p}$ has a solution in $\{1, 2, ..., p - 1\}$. Thus, from the proof of Theorem 3.1.1, this congruence has exactly two solutions in $\{1, 2, ..., p - 1\}$ whose sum is $p$. Let these two solutions be $x_0$ and $p - x_0$. The product of these two solutions is:

$$x_0(p - x_0) \equiv -x_0^2 \equiv -a \pmod{p}.$$ 

Now group the remaining $p - 3$ integers in $\{1, 2, ..., p - 1\}$ into pairs of unequal integers such that the product the elements of each pair is $a$. We can do this since the congruence $bx \equiv a \pmod{p}$ has exactly one solution for all $b \not\equiv 0 \pmod{p}$. Thus, the product of these $p - 3$ integers is congruent to $a^{\frac{p-3}{2}}$ modulo $p$.

Therefore,

$$(p - 1)! \equiv -a \cdot a^{\frac{p-3}{2}} \equiv -a^{\frac{p-1}{2}} \pmod{p}.$$ 

Since $(a/p) = 1$ we can write this as:

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

For the second case, let us suppose that $a$ is a nonresidue of $p$. We write this in terms of the Legendre symbol as $(a/p) = -1$. Thus, the congruence $x^2 \equiv a \pmod{p}$ has no solution. We now group the integers $\{1, 2, ..., p - 1\}$ into unequal pairs whose product is $a$. As before, we can do this since the congruence $bx \equiv a \pmod{p}$ has exactly one solution for all $b \not\equiv 0 \pmod{p}$. Thus, the product of these $p - 1$ integers is congruent to $a^{\frac{p-1}{2}}$ modulo $p$. 

70
Therefore,

\[(p - 1)! \equiv a^{\frac{p-1}{2}} \pmod{p}.\]

Since \((a/p) = -1\) we can write this as:

\[(p - 1)! \equiv -(a/p)a^{\frac{p-1}{2}} \pmod{p}.\]

The result now follows. \(\square\)

We now choose \(a = 1\) in Theorem 3.6.1. Since \(x^2 \equiv 1 \pmod{p}\) has the solutions 1 and \(p - 1\) it follows that \((1/p) = 1\). Thus,

\[(p - 1)! \equiv -1 \pmod{p}.\]

This we recognize as Wilson’s theorem (Theorem 2.1.1).

If we combine Theorem 3.6.1 with Wilson’s theorem (Theorem 2.1.1) we then have the following, which we recognize as Euler’s criterion (Theorem 3.5.1):

\[(a/p) \equiv a^{\frac{p-1}{2}} \pmod{p}.\]

Thus, Wilson’s theorem (Theorem 2.1.1) and Euler’s theorem (Theorem 3.5.1) follow immediately from Theorem 3.6.1.

### 3.7 Primes in Residue Classes

#### 3.7.1 Connection Between Quadratic Residues and Primes in Reduced Residue Classes

As we have seen in the previous two sections, the notion of quadratic residues modulo a prime \(p\) is closely related to the notion of primes in reduced residue classes. Both of these notions are essential to this thesis. To determine the quadratic nature of an integer \(a \in \{\pm1, \pm2, \pm3, \pm5\}\) modulo a prime \(p\), we simply determine which residue class \(p\) belongs to modulo \(4a\). The quadratic nature of \(a\) modulo \(p\) now follows from Gauss or from quadratic reciprocity.
3.7.2 The Number of Primes Congruent to 1 and 3 Modulo 4 Using Elementary Methods

It is a well-known fact from number theory that there are infinitely many primes. This fact can be proved in many different ways. Consider, for example, Euclid’s proof of this result. Euclid’s proof, which can be found in any number theory book, is as follows:

**Proof.** We proceed by contradiction. Suppose that there are only finitely many such primes. Say, \( \{p_1, p_2, \ldots, p_n\} \).

Now consider the integer:

\[
N = p_1p_2\ldots p_n + 1.
\]

This integer has no prime factor. Thus, we have established a contradiction. Therefore, there are in fact infinitely many primes.

Thus, we have proved:

**Theorem 3.7.1.** There are infinitely many primes.

We now consider primes in the reduced residue classes \((1) = \{x \in \mathbb{Z} | x \equiv 1 \pmod{4}\}\) and \((3) = \{x \in \mathbb{Z} | x \equiv 3 \pmod{4}\}\) in \(\mathbb{Z}_4\). That is, we are considering primes of the form \(4n + 1\) and \(4n + 3\).

Now, every prime with the exception of 2 is in either \((1)\) or \((3)\). In light of Theorem 3.7.1 there are two possibilities. Either both of the classes \((1)\) and \((3)\) contain infinitely many primes or one of these classes contains infinitely many primes while the other contains only finitely many primes.

It turns out that both classes contain infinitely many primes. Thus, we have the following two results which are Example 11.7 and Theorem 3.15 in Koshy [1]:

**Theorem 3.7.2.** There are infinitely many primes of the form \(4n + 1\).

**Theorem 3.7.3.** There are infinitely many primes of the form \(4n + 3\).

We now follow Koshy by proving Theorems 3.7.2 and 3.7.3. Note that these proofs, which are taken directly from Koshy [1], are in many ways similar to Euclid’s proof that there are infinitely many primes. Both proofs proceed by assuming that there are only finitely many such primes, taking the product of all such primes, and then establishing a contradiction.
 Also, note that for the proof of primes of the form $4n + 1$ we use Theorem 3.3.1 which describes the quadratic nature of $-1$ modulo a prime $p$.

We now prove Theorem 3.7.2 as follows: This proof is from pages 504-505 from [1].

\textbf{Proof.} We proceed with a proof by contradiction. Suppose that there are only finitely many primes of the form $4n + 1$. Let these primes form the set $\{p_1, p_2, ..., p_k\}$.

We now define the positive integer $N$ as follows:

$$N = (2p_1p_2...p_k)^2 + 1.$$ 

Now, $N$ is odd. Thus, $N$ has an odd prime factor say $p$. Therefore, $N \equiv 0 \ (mod \ p)$. From which it follows that:

$$(2p_1p_2...p_k)^2 \equiv -1 \ (mod \ p).$$

Now, $x = 2p_1p_2...p_k$ is a solution of the congruence:

$$x^2 \equiv -1 \ (mod \ p).$$

From Theorem 3.3.1 on the quadratic nature of $-1$ modulo the prime $p$, it follows that either $p = 2$ or $p \equiv 1 \ (mod \ 4)$. However, $p$ is odd. Thus, $p \equiv 1 \ (mod \ 4)$.

So, $p$ is a prime of the form $4n + 1$. Therefore, $p \in \{p_1, p_2, ..., p_k\}$.

Thus, $N \equiv 1 \ (mod \ p)$. This contradicts $N \equiv 0 \ (mod \ p)$.

There are, therefore, infinitely many primes of the form $4n+1$. This completes the proof. \hfill \Box

We now follow Koshy by proving 3.7.3. The proof we give together with the proof of the required lemma is from pages 181-182 in [1].

We require the following lemma:

\textbf{Lemma 3.7.1.} The product of two integers of the form $4n + 1$ is also of the form $4n + 1$.

The proof which follows is straightforward.

\textbf{Proof.}

$$(4n + 1)(4m + 1) = 4(4nm + n + m) + 1$$

\hfill \Box
We now prove Theorem 3.7.3 as follows:

Proof. Let us suppose that there are only finitely many primes of the form \( 4n + 3 \). Let these primes by given by the set: \( \{p_0, p_1, p_3, ..., p_k\} \). Here we have written \( p_0 = 3 \), which is clearly the least element of this set of primes.

We now define the positive integer \( N \) as follows:

\[
N = 4p_1p_2...p_k + 3.
\]

Thus, the integer \( N \) is of the form \( 4n + 3 \) and is greater than every prime of the form \( 4n + 3 \). Therefore, \( N \) is composite.

Now \( N \) is odd. Thus, every prime factor of \( N \) is of the form \( 4n + 1 \) or of the form \( 4n + 3 \). If every prime factor of \( N \) is of the form \( 4n + 1 \), then by Lemma 3.7.1, then \( N \) is of the form \( 4n + 1 \).

Thus, \( N \) has a prime factor of the form \( 4n + 3 \). Let us denote this prime factor of \( N \) of the form \( 4n + 3 \) by \( p \). Therefore, \( p|N \) and \( p \) is of the form \( 4n + 3 \).

Clearly, \( p \in \{p_0, p_1, p_3, ..., p_k\} \).

We now consider two cases. In the first case \( p = p_0 = 3 \) in the second case \( p \in \{p_1, p_3, ..., p_k\} \).

First, suppose that \( p = p_0 = 3 \). Thus, \( 3|N \). From which it follows that \( 3|(N - 3) \). From our expression for \( N \) this is equivalent to:

\[
3|4p_1p_2...p_k.
\]

By Euclid’s lemma (Lemma 2.1.1) this reduces to: \( 3|2 \) or \( 3|p_j \) for some \( j \) with \( 1 \leq j \leq k \). This is impossible, since each \( p_j \) is prime.

Secondly, suppose that \( p = p_i \) for some \( i \) with \( 1 \leq i \leq k \). Thus, \( p|N \) and \( p|4p_1p_2...p_k \).

From which it follows that \( p|(N - 4p_1p_2...p_k) \). Therefore \( p|3 \), which is again impossible. Thus, in either case we have established a contradiction.

Therefore, there are infinitely many primes of the form \( 4n + 3 \).

\[\square\]

### 3.8 Dirichlet’s Theorem

The two results in the previous section (Theorem 3.7.2 and Theorem 3.7.3) are both special cases of a more general result known as Dirichlet’s theorem, which has to do with primes in
residue classes, or what is the same thing, primes in arithmetic progressions.

Here, when we say primes in an arithmetic progression, we of course mean primes in an arithmetic sequence. Consider the arithmetic progression (i.e. arithmetic sequence) \( \{a, a + b, a + 2b, a + 3b, \ldots \} \). Then the prime \( p \) is in this arithmetic progression if and only if there exists a nonnegative integer \( n \) such that \( p = a + bn \).

Primes in residue classes (i.e. primes in arithmetic progressions) are essential to this paper because of their connection to both the order and the number of self-invertible elements in the groups that we shall consider.

Let \( a \) and \( b \) be two fixed positive integers. Now consider the arithmetic progression starting with \( a \) and having common difference \( b \): \( a, a + b, a + 2b, a + 3b, \ldots \)

If \( a \) and \( b \) have a common factor, then the first term \( a \) may be prime however, every other term is composite.

If \( a \) and \( b \) are relatively prime, then we have the following well-known result which appears in [1] as Theorem 3.16 and is known as Dirichlet’s theorem:

**Theorem 3.8.1** (Dirichlet’s Theorem). If \( a \) and \( b \) are relatively prime positive integers, then the arithmetic progression: \( a, a + b, a + 2b, a + 3b, \ldots \) contains infinitely many primes.

Note that if the prime \( p \) is in the arithmetic progression: \( a, a + b, a + 2b, a + 3b, \ldots \) then this is equivalent to \( p \equiv a \pmod{b} \). Thus, we can rewrite Dirichlet’s theorem in terms of congruence as follows:

**Theorem 3.8.2** (Dirichlet’s Theorem). If \( a \) and \( b \) are relatively prime positive integers then there exist infinitely many primes \( p \) such that \( p \equiv a \pmod{b} \).

Note that Theorems 3.7.2 and 3.7.3 are special cases of Dirichlet’s theorem. If we choose \( a = 1 \) and \( b = 4 \) then Dirichlet’s theorem reduces to Theorem 3.7.2. While if we choose \( a = 3 \) and \( b = 4 \) then Dirichlet’s theorem reduces to Theorem 3.7.3.
Chapter 4

Higher Dimensional Analogs of Wilson’s Theorem

All the results in this chapter are new with the exception of the expression for the order of the general linear group of $n \times n$ invertible matrices over $\mathbb{Z}_p$.

4.1 Wilson’s Theorem In two Dimensions

4.1.1 Defining The Group $G_2$ in Terms of The Quotient Ring $\mathbb{Z}[\rho]/<1 + \rho + \rho^2>$

In this section, we first define a group, which we call $G_2$, of polynomials modulo a prime $p$ that generalizes the well-known multiplicative group $\mathbb{Z}_p^* = \{1, 2, 3, ..., p - 1\}$. We then classify the order of the group $|G_2|$ and the number of self-invertible elements in the group $|S(G_2)|$. Here, we have written $S(G_2)$ to denote the subgroup of self-invertible elements in $G_2$. This classification, which depends on the reduced residue class in $\mathbb{Z}_3$ to which $p$ belongs, lead us to generalize both Wilson’s theorem and Fermat’s little theorem.

To generalize Wilson, we apply the results from [2] that are due to Górowski and Lomnicki (Theorem 2.2.2) to the group $G_2$. To generalize Fermat, we apply Theorem 2.3.19 to the group $G_2$.

In proving Wilson’s theorem using the result due to Górowski and Lomnicki [2], we first considered the multiplicative group of nonzero residues modulo a prime $p$. We then considered the product of every element in this group. This product rests on the fact that the group $\mathbb{Z}_p^*$ contains precisely two self-invertible elements when $p$ is an odd prime. These
elements are 1 and $p - 1$. This method can be extended to prove what we shall call Wilson’s theorem in two dimensions and Wilson’s theorem in three dimensions, then can be generalized to prove Wilson in $N - 1$ dimensions.

Consider the ring of integers $\mathbb{Z}$. Let $\mathbb{Z}[\rho] = \{a_n\rho^n + \cdots + a_1\rho + a_0 \mid a_i \in \mathbb{Z}\}$ be the set of polynomials in the variable $\rho$ with coefficients in $\mathbb{Z}$. Consider the principal ideal generated by the polynomial $1 + \rho + \rho^2$, $<1 + \rho + \rho^2> = \{f(\rho)(1 + \rho + \rho^2) \mid f(\rho) \in \mathbb{Z}[\rho]\}$. We now form the quotient ring:

$$Z[\rho]/<1 + \rho + \rho^2> = \{g(\rho) + <1 + \rho + \rho^2> \mid g(\rho) \in \mathbb{Z}[\rho]\}.$$ 

Notice, that in this quotient ring we have: $\rho^3 = \rho^1(-1-\rho) = -\rho^1-\rho^2 = 1-(1+\rho+\rho^2) = 1$ in addition to $1 + \rho + \rho^2 = 0$.

In this section and in the rest of this thesis, we shall refer to elements in this quotient ring as polynomials. However, it should be noted that these elements are not polynomials, they are equivalence classes of polynomials.

We now define the notion of congruence as it applies to polynomials in $\mathbb{Z}[\rho]$. Consider $f(\rho), g(\rho) \in \mathbb{Z}[\rho]$. We say that $f(\rho)$ and $g(\rho)$ are congruent modulo $p$ and write $f(\rho) \equiv g(\rho) \pmod{p}$ if every coefficient of $f(\rho) - g(\rho)$ is divisible by $p$. From this definition it follows that $f(\rho)$ and $g(\rho)$ are congruent modulo $p$ if and only if there exists a polynomial $h(\rho) \in \mathbb{Z}[\rho]$ such that $f(\rho) = g(\rho) + p \cdot h(\rho)$.

Now let $p$ be a prime number and consider the quotient ring of polynomials modulo $p$. We now have what is essentially equivalence classes whose elements are themselves equivalence classes. Let $\alpha$ be any such polynomial. Now $\rho^3 = 1$. Thus, we may assume that $\alpha$ is quadratic. Say $\alpha = a + b\rho + c\rho^2$. We now reduce $\alpha$ modulo $p$ by adding polynomial multiples of $p$. Essentially, we are finding the least residue of $\alpha$ modulo $p$. Now, $\rho^2 = -1 - \rho$. Thus,

$$\alpha = a + b\rho + c(-1 - \rho) = (a - c) + (b - c)\rho.$$ 

Now, the coefficients $a - c$ and $b - c$ might be negative. However, we are considering $\alpha$ modulo $p$, and so we can add a positive integer multiple of $p$ to $\alpha$ to make the constant coefficient a nonnegative integer. We do the same for the coefficient of $\rho$.

Thus, $\alpha = a + b\rho$ (the $a$ and $b$ are different from those used previously) where $a$ and $b$ are nonnegative integers. In fact, since we are considering polynomials modulo $p$, we may further assume that $0 \leq a \leq p - 1$ and $0 \leq b \leq p - 1$. Thus, in the same way that every integer $n$ is congruent to a least residue modulo $p$, every polynomial in $Z[\rho]/<1 + \rho + \rho^2>$
is congruent modulo $p$ to a unique polynomial in the following set:

$$\{a + bp \mid 0 \leq a \leq p - 1, 0 \leq b \leq p - 1\}.$$

We shall call this set the least residue region, for obvious reasons. We refer to the main result in this section as Wilson’s theorem in two dimensions because the least residue region may be considered as a two dimensional vector space over the field $\mathbb{Z}_p$.

We would like to consider the product of all invertible polynomials in the least residue region modulo $p$. When we say that $a + bp$ is invertible we of course mean that there exists a polynomial $c + dp$ such that $(a + bp)(c + dp) \equiv 1 \pmod{p}$. With this notion of invertible polynomials, we introduce the notation $(a + bp)^*$ as follows:

$$(a + bp)^* = \begin{cases} a + bp & \text{if } a + bp \text{ is invertible} \\ 1 & \text{otherwise} \end{cases}.$$

We use this * notation to remove from our product polynomials that are not invertible.

We now consider the group of invertible polynomials in the least residue region $\{a + bp \mid 0 \leq a \leq p - 1, 0 \leq b \leq p - 1\}$. We call this group $G_2$.

Thus,

$$G_2 = \{a + bp \mid 0 \leq a \leq p - 1, 0 \leq b \leq p - 1, a + bp \text{ is invertible mod } p\}.$$ 

We denote the order of this group by $|G_2|$.

The zero polynomial $0 + 0 \rho$ is clearly not invertible. Thus, we have $(0 + 0\rho)^* = 1$. Therefore, for any choice of $p$, $|G_2| \leq p^2 - 1$. This raises the question: Are there nonzero elements in the least residue region that are not invertible? At the end of this section, we shall prove that the least residue region $\{a + bp \mid 0 \leq a \leq p - 1, 0 \leq b \leq p - 1\}$ contains at least one noninvertible element other than $0 + 0\rho$ if and only if $p$ is equal to 3 or is of the form $3^n + 1$. Thus, $|G_2| \leq p^2 - 2$ if and only if $p$ is equal to 3 or is of the form $3n + 1$.

Note, that if we remove elements from the least residue region that are not invertible, we then end up with the finite abelian group $G_2$. Here, when we say a polynomial is not invertible, we of course mean not invertible modulo $p$. 

78
4.1.2 Inverses of Elements in The Group $G_2$ and an Isomorphic Ring of Matrices

Every nonzero polynomial $\alpha = a + b\rho$ with $a^2 - ab + b^2$ not divisible by $p$, in the least residue region has an inverse in this region. It can be shown by mimicking the algebra of complex numbers that if $a^2 - ab + b^2 \not\equiv 0 \pmod{p}$ then the inverse of the polynomial $a + b\rho$ in the least residue region is uniquely given by:

$$(a + b\rho)^{-1} = \frac{1}{a + b\rho} = \frac{1}{a + b\rho} \cdot \frac{a + b\rho^2}{a + b\rho^2} = \frac{(a - b) + (-b)\rho}{a^2 - ab + b^2}.$$

Here we have used complex arithmetic. However, we want $(a + b\rho)^{-1}$ to have coefficients in $\mathbb{Z}_p$. Thus, we proceed as follows: Let $k$ be the natural number less than $p$ satisfying $k(a^2 - ab + b^2) \equiv 1 \pmod{p}$. If $a^2 - ab + b^2 \not\equiv 0 \pmod{p}$ then we define the inverse of $a + b\rho$ as follows:

$$(a + b\rho)^{-1} \equiv k[(a - b) + (-b)\rho] \pmod{p}.$$

This inverse, if it exists, is congruent modulo $p$ to a unique polynomial in the least residue region.

Thus, if $a^2 - ab + b^2 \not\equiv 0 \pmod{p}$ then $a + b\rho$ has an inverse. We now show conversely, that if $a + b\rho$ has an inverse then $a^2 - ab + b^2 \not\equiv 0 \pmod{p}$.

In finding the inverse of $\alpha = a + b\rho$ we are required to find a polynomial $\beta = c + d\rho$ such that:

$$(a + b\rho)(c + d\rho) = (ac - bd) + (ad + bc - bd)\rho = 1.$$

This gives the following system of equations:

$$ac - bd = 1$$

and

$$ad + bc - bd = 0.$$

Writing this system in terms of matrices gives the following:
Thus, the task of finding the inverse of the polynomial \( \alpha = a + b\rho \) now becomes the task of finding the inverse of the matrix \(
abla\begin{bmatrix} a & -b \\ b & a-b \end{bmatrix}\). Notice that the first column of this matrix is the coefficients, that is the coordinate vector, of \( a + b\rho \). While the second column of this matrix is the coefficients, that is the coordinate vector, of \( \rho(a + b\rho) = -b + (a-b)\rho \).

It can be shown by straightforward computation, that the function which maps the polynomial \( \alpha = a + b\rho \) to the matrix \(
abla\begin{bmatrix} a & -b \\ b & a-b \end{bmatrix}\) is a ring isomorphism. Before we prove this, we state a corollary to the Cayley Hamilton theorem.

**Theorem 4.1.1** (Corollary to the Cayley Hamilton theorem). If \( A \) is an \( n \times n \) matrix with integer entries, distinct eigenvalues, and \( p(x) \) is the characteristic polynomial of \( A \) then there exists a ring isomorphism from \( \mathbb{Z}[x]/<p(x)> \) to \( M_n(\mathbb{Z}) \) that sends \( q(x) \) to \( q(A) \).

Here we have written the set of \( n \times n \) matrices with integral entries as \( M_n(\mathbb{Z}) \).

**Theorem 4.1.2.** The map \( \Phi(a + b\rho) = \nabla\begin{bmatrix} a & -b \\ b & a-b \end{bmatrix} \) is a ring isomorphism from \( \mathbb{Z}[\rho]/<1+\rho+\rho^2> \) to \( M_2(\mathbb{Z}) \).

We prove this theorem in two different ways. The first way is by straightforward algebra. The second way uses Theorem 4.1.1.

**Proof.** Clearly, \( \Phi \) is a bijection that preserves addition. We now show that it also preserves multiplication.

\[
\Phi((a + b\rho)(c + d\rho)) = \Phi((ac - bd) + ((a - b)d + bc)\rho))
\]

\[
= \begin{bmatrix} ac - bd & -(a-b)d - bc \\ (a-b)d + bc & (a-b)c - ad \end{bmatrix} = \begin{bmatrix} a & -b \\ b & a-b \end{bmatrix} \begin{bmatrix} c & -d \\ d & c - d \end{bmatrix}
\]

\[
= \Phi(a + b\rho)\Phi(c + d\rho).
\]

Thus, \( \Phi \) is a bijection that preserves addition and multiplication.

This completes the proof.
We now give a second proof.

Proof. Note that the function \( \Phi \) maps the polynomial \( \rho \) to the matrix \( \Phi(\rho) = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix} \).

This matrix is called the companion matrix of the monic polynomial \( 1 + x + x^2 \). Companion matrices are studied in [9]. Now the characteristic equation of the matrix \( \Phi(\rho) \) is \( 1 + x + x^2 \).

Thus, by Theorem 4.1.1, there exists a ring isomorphism from \( \mathbb{Z}[x]/\langle 1 + x + x^2 \rangle \) to \( M_2 \) that sends every \( q(x) = a + bx \in \mathbb{Z}[x]/\langle 1 + x + x^2 \rangle \) to \( q(\Phi(\rho)) \).

Now, \( q(\Phi(\rho)) = aI + b\Phi(\rho) = \begin{bmatrix} a & -b \\ b & a - b \end{bmatrix} \).

Thus, there exists a ring isomorphism that maps the element \( a+b\rho \) in \( \mathbb{Z}[\rho]/\langle 1+\rho+\rho^2 \rangle \) to the matrix \( \begin{bmatrix} a & -b \\ b & a - b \end{bmatrix} \).

This completes the proof.

4.1.3 Wilson’s Theorem in Two Dimensions

If we count the number of self-invertible polynomials in the group \( G_2 \), take the product of every polynomial in this group, then apply Górowski and Lomnicki (Theorem 2.2.2) we have the following:

**Theorem 4.1.3** (Wilson’s Theorem in two Dimensions). If \( p \) is prime then the product of all the elements in \( \mathbb{Z}[\rho]/\langle 1+\rho+\rho^2 \rangle \) that are invertible modulo \( p \) is:

\[
G_2 = \{ a + b\rho \mid 0 \leq a \leq p - 1, 0 \leq b \leq p - 1, a^2 - ab + b^2 \not\equiv 0 \pmod{p} \}.
\]
\[
\prod_{i=0}^{p-1} \prod_{j=0}^{p-1} (i + j\rho)^* \equiv \begin{cases} 
1 \pmod{p} & \text{if } -3 \text{ is a quadratic residue of } p \\
-1 \pmod{p} & \text{otherwise}
\end{cases}.
\]

In Theorem 4.1.3 we are taking the product of all invertible elements in the least residue region. The least residue region is a two dimensional vector space over \(\mathbb{Z}_p\). Thus, we call Theorem 4.1.3 Wilson’s theorem in two dimensions.

We now prove Theorem 4.1.3 as follows:

**Proof.** We apply Theorem 2.2.2 to the product: \(\prod_{g \in G_2} g\), of all elements in the group \(G_2\) as follows: We will show that this product depends on the quadratic nature of \(-3\) modulo the prime \(p\), or equivalently by Theorem 3.4.16, on what residue class in \(\mathbb{Z}_3\) to which \(p\) belongs.

Note that \(1 = 1 + 0\rho\) appears in the product and is self-invertible. However, \(1\) is the identity. Thus it has order one. If we choose the prime \(p = 2\) then \(1\) is the only self-invertible polynomial in \(G_2\). Thus, if \(p = 2\) then by Górowski and Lomnicki (Theorem 2.2.2), this product is congruent to \(1 \equiv -1 \pmod{2}\). The result therefore holds for \(p = 2\).

Now let \(p > 2\). Another self-invertible polynomial that appears in this product is \(p - 1 = p - 1 + 0\rho\). This polynomial has order two. Thus, there is at least one polynomial in this product that has order two. Also, note that by Lemma 2.1.2, \(1\) and \(p - 1\) are the only self-invertible elements in the set \(\{1, 2, 3, ..., p-1\}\). By Górowski and Lomnicki (Theorem 2.2.2), this product is congruent modulo \(p\) to 1 if the product contains self-invertible polynomials other than \(1\) and \(p - 1\) and is congruent modulo \(p\) to \(p - 1 \equiv -1\) if \(1\) and \(p - 1\) are the only self-invertible polynomials in the product.

Consider the polynomial \(i + j\rho\). This polynomial is self-invertible if and only if:

\[(i + j\rho)(i + j\rho) \equiv 1 \pmod{p}.
\]

This is equivalent to:

\[(i^2 - j^2) + (2ij - j^2)\rho \equiv 1 \pmod{p}.
\]

We can write this as the system of congruences:

\[i^2 - j^2 \equiv 1 \pmod{p} \quad (4.1)
\]

and
\[ 2ij - j^2 \equiv 0 \pmod{p} \quad (4.2) \]

From the congruence (4.2), we have the following:

\[ j \equiv 0 \pmod{p} \]

or

\[ j \equiv 2i \pmod{p}. \]

First suppose that \( j \equiv 0 \pmod{p} \) then from the congruence (4.1) we have \( i^2 \equiv 1 \pmod{p} \). This is equivalent to \( i = 1 \) or \( i = p - 1 \) by Theorem 2.1.2. Thus, in this case, we have that \( i + j\rho \) is one of the trivial self-invertible polynomials: 1 or \( p - 1 \).

Thus, \( i + j\rho \) is a nontrivial self-invertible polynomial modulo \( p \) if and only if \( i \) and \( j \) satisfy:

\[ i^2 - j^2 \equiv 1 \pmod{p} \]

and

\[ j \equiv 2i \pmod{p}. \]

This is equivalent to:

\[ -3i^2 \equiv 1 \pmod{p} \]

and

\[ j \equiv 2i \pmod{p}. \]

Thus, \( i + j\rho \) is a nontrivial self-invertible polynomial in the product \( \prod_{i=0}^{p-1} \prod_{j=0}^{p-1} (i + j\rho)^* \) if and only if \( i \) and \( j \) satisfy both of the following:

\[ -3i^2 \equiv 1 \pmod{p} \]

and
\[ j \equiv 2i \ (mod \ p). \]

Note that the fact that there exists an \( i \) which satisfies the congruence:

\[ -3i^2 \equiv 1 \ (mod \ p) \]

is, by Theorem 3.4.2, equivalent to \(-3\) being a quadratic residue of \( p \).

Thus, there exists a nontrivial self-invertible polynomial in the product \( \prod_{i=0}^{p-1} \prod_{j=0}^{p-1} (i + j\rho)^* \) if and only if \(-3\) is a quadratic residue modulo \( p \). By Theorem 3.4.16, \(-3\) being a quadratic residue of \( p \) is equivalent to \( p \) being of the form \( 3n + 1 \).

\[ \square \]

Note, that if \(-3\) is a quadratic residue of \( p \) then there exist exactly two polynomials \( i + j\rho \) that satisfy:

\[ -3i^2 \equiv 1 \ (mod \ p) \]

and

\[ j \equiv 2i \ (mod \ p). \]

Thus, if \(-3\) is a quadratic residue of \( p \), then there exist exactly 2 nontrivial self-invertible polynomials.

As an example of two such nontrivial self-invertible polynomials modulo a prime \( p \), consider the prime \( p = 13 \). The prime \( p = 13 \) is of the form \( 3n + 1 \). Thus, by Theorem 3.4.17, \(-3\) is a quadratic residue of 13. Alternatively, using quadratic reciprocity (Theorem 3.5.4), it can be shown that \((-3/13) = 1 \) and therefore \(-3\) is a quadratic residue of 13. By substitution, it can be shown that \( i = 2 \) satisfies \(-3i^2 \equiv 1 \ (mod \ p)\). Now set \( j = 2i = 4 \).

Thus, we have constructed the polynomial \( 2 + 4\rho \) which is a nontrivial self-invertible polynomial modulo \( p \), where \( p = 13 \). Another nontrivial self-invertible polynomial modulo 13 is \( 11 + 9\rho \).

Note, that for \( p = 13 \) there exist exactly 4 self-invertible polynomials. These are: 1, 12, \( 2 + 4\rho \), and \( 11 + 9\rho \).
4.1.4 Two Dimensional Wilson Results for Matrices and Determinants of Matrices

In considering inverses of polynomials, we have shown that the ring of polynomials \((a + b\rho) \in \mathbb{Z}[\rho]/<1 + \rho + \rho^2>\) is ring isomorphic to the ring of two by two matrices of the form \(\begin{bmatrix} a & -b \\ b & a - b \end{bmatrix}\). Thus, in Wilson’s theorem in two dimensions, we can essentially replace polynomials by matrices and polynomial multiplication by matrix multiplication. In this manner, we replace \(i + j\rho\) with \(\begin{bmatrix} i & -j \\ j & i - j \end{bmatrix}\).

We define the * notation to remove noninvertible matrices from the product by the following:

\[
\begin{bmatrix} i & -j \\ j & i - j \end{bmatrix}^* = \begin{cases} \begin{bmatrix} i & -j \\ j & i - j \end{bmatrix} & \text{if } i^2 - ij + j^2 \not\equiv 0 \pmod{p} \\ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & \text{otherwise} \end{cases}
\]

With this we have:

**Theorem 4.1.4.** If \(p\) is prime, then:

\[
\prod_{i=0}^{p-1} \prod_{j=0}^{p-1} \begin{bmatrix} i & -j \\ j & i - j \end{bmatrix}^* \equiv \begin{cases} I \pmod{p} & \text{if } -3 \text{ is a quadratic residue of } p \\ -I \pmod{p} & \text{otherwise} \end{cases}.
\]

Here, \(I\) is the two by two identity matrix.

If we take determinants of both sides of the previous result and use the fact that the determinant of a product is the product of the determinants, we then have the following result:

**Theorem 4.1.5.** If \(p\) is prime, then:

\[
\prod_{i=0}^{p-1} \prod_{j=0}^{p-1} (i^2 - ij + j^2)^* \equiv 1 \pmod{p}.
\]

Here, as before, we use the * notation to remove noninvertible elements from the product defined as follows:
\[(i^2 - ij + j^2)^* = \begin{cases} 
  i^2 - ij + j^2 & \text{if } i^2 - ij + j^2 \not\equiv 0 \pmod{p} \\
  1 & \text{otherwise} 
\end{cases} \]

Note that in Theorem 4.1.5, we are essentially considering a product of values of the binary quadratic form \(x^2 - xy + y^2\).

### 4.1.5 The Group of Self-Invertible Elements in \(G_2\)

Now, in proving Wilson’s theorem in 2 dimensions, we have also shown that if \(|S(G_2)|\) denotes the number of self-invertible elements in the group \(G_2\) then we have the following:

**Theorem 4.1.6.**

\[|S(G_2)| = \begin{cases} 
  1 & \text{if } p = 2 \\
  4 & \text{if } -3 \text{ is a residue of } p \\
  2 & \text{otherwise} 
\end{cases} \]

By Theorem 3.4.19, this result can be written in terms of primes in residue classes instead of in terms of quadratic residues as follows:

**Theorem 4.1.7.**

\[|S(G_2)| = \begin{cases} 
  1 & \text{if } p = 2 \\
  4 & \text{if } p \equiv 1 \pmod{3} \\
  2 & \text{otherwise} 
\end{cases} \]

Note, that in addition to rigorously proving this, I have verified it for the first 25 primes by writing code in C.

### 4.1.6 The Order of the Group \(G_2\)

Note that we generalized Wilson’s theorem by counting self-invertible elements and then applying the results in [2] due to Gorowski and Lomnicki (Theorem 2.2.2) to the group:

\[G_2 = \{i + j\rho \mid 0 \leq i \leq p - 1, 0 \leq j \leq p - 1, i^2 - ij + j^2 \not\equiv 0 \pmod{p}\}.\]

We now generalize Fermat’s little theorem by determining the order of the group \(G_2\) and then applying Theorem 2.3.19. Thus, we are essentially counting the number of invertible elements in the least residue region: \(\{i + j\rho \mid 0 \leq i \leq p - 1, 0 \leq j \leq p - 1\}\).
As we mentioned previously, since $0 + 0\rho$ is not in $G_2$, it follows that the order of $G_2$, denoted by $|G_2|$, satisfies:

$$|G_2| \leq p^2 - 1.$$  

Note that the group $G_2$ defined as:

$$G_2 = \{i + j\rho \mid 0 \leq i \leq p - 1, 0 \leq j \leq p - 1, i^2 - ij + j^2 \not\equiv 0 \pmod{p}\}$$

is isomorphic to the group:

$$\left\{\begin{bmatrix} i & -j \\ j & i-j \end{bmatrix} \mid i, j \in \mathbb{Z}_p, i^2 - ij + j^2 \not\equiv 0 \pmod{p}\right\}.$$  

This is a subgroup of the general linear group of $2 \times 2$ matrices over $\mathbb{Z}_p$, defined as follows:

$$GL_2(\mathbb{Z}_p) = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{Z}_p, ad - bc \not\equiv 0 \pmod{p}\right\}.$$  

To compute the order of the group $GL_2(\mathbb{Z}_p)$ consider a group element, say: $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Now for the first column of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ there are $p$ possible values for $a \in \mathbb{Z}_p$ and $p$ possible values for $c \in \mathbb{Z}_p$. However, for the matrix to be invertible, $a$ and $c$ cannot both be 0. Thus, there are $p^2 - 1$ possible values for the first column of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$.

Now for the second column of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ there are $p^2$ possible values for $b$ and $d$. However, for the matrix to be invertible, the second column cannot be a multiple of the first column. There are exactly $p$ multiples of the first column. Thus, there are $p^2 - p$ possible values for the second column of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$.

Thus, we conclude that the order of the group $GL_2(\mathbb{Z}_p)$ is precisely $(p^2 - 1)(p^2 - p)$.

Now, it is a well-known fact from algebra, that the order of a subgroup divides the order of the group. Thus, the order of the group $G_2$, which we shall write as $|G_2|$, divides $(p^2 - 1)(p^2 - p)$.

We now strengthen this by the following result which shows that the order of $G_2$ depends
on the residue class in $\mathbb{Z}_3$ to which $p$ belongs. This result can equivalently be written in terms of the quadratic nature of $-3$ modulo the prime $p$ instead of in terms of residue classes in $\mathbb{Z}_3$.

Let $G_2$ be the group defined previously and let $|G_2|$ denote the order of $G_2$. Then $|G_2|$ is given by the following:

**Theorem 4.1.8.**

\[
|G_2| = \begin{cases} (p - 1)^2 & \text{if } p = 3n + 1 \\ p^2 - p - 6 & \text{if } p = 3 \\ p^2 - 1 & \text{if } p = 3n + 2 \end{cases}
\]

From Gauss [7], this theorem can be written in terms of quadratic residues modulo a prime $p$ instead of in terms of residue classes as follows:

**Theorem 4.1.9.**

\[
|G_2| = \begin{cases} (p - 1)^2 & \text{if } -3 \text{ is a residue of } p \\ p^2 - 1 & \text{if } -3 \text{ is a nonresidue of } p \\ p^2 - p - 6 & \text{if } p = 3 \end{cases}
\]

Note, that each of: $(p - 1)^2$, $p^2 - p$, and $p^2 - 1$ divides the order of $GL_2(\mathbb{Z}_p)$ which is $=(p^2 - 1)(p^2 - p)$. This agrees with our remark about the order of a subgroup dividing the order of the group.

Also, note, that in addition to proving Theorem 4.1.8, I have written code in C which verifies it for the first 25 prime numbers $p$.

From Theorem 4.1.8 it follows immediately that $\frac{|G_2|}{P^2} \to 1$ as $P \to \infty$. This means that the number of noninvertible elements in the set $\{i + j\rho \mid 0 \leq i \leq p - 1, 0 \leq j \leq p - 1\}$ is $o(P^2)$.

Before we prove Theorem 4.1.8, we first establish the two Lemmas 4.1.1 and 4.1.3, each which classify noninvertible elements in additive cosets, and either of which can be used to prove Theorem 4.1.8:

**Lemma 4.1.1.** let $a \in \mathbb{Z}_p^\times$. Then each additive coset $\mathbb{Z}_p + ap = \{i + ap \mid i \in \mathbb{Z}_p\}$ contains:

1. 2 noninvertible elements if $p = 3n + 1$
2. 1 noninvertible element if $p = 3$
3. 0 noninvertible elements if $p = 3n + 2$

As with Theorem 4.1.8, this lemma can be written in terms of quadratic residues instead of in terms of residue classes as follows:

**Lemma 4.1.2.** let $a \in \mathbb{Z}_p^*$. Then each additive coset $\mathbb{Z}_p + a\rho = \{i + a\rho \mid i \in \mathbb{Z}_p\}$ contains:

1. 2 noninvertible elements if $-3$ is residue of $p$.
2. 1 noninvertible element if $p = 3$.
3. 0 noninvertible elements if $-3$ is a nonresidue of $p$.

We now prove Lemma 4.1.1 as follows:

**Proof.** In this proof, we classify noninvertible elements in additive cosets.

If $p = 2$ then the result follows. Thus, let $p$ be an odd prime.

Let $a \in \mathbb{Z}_p^*$ be fixed.

We now consider the additive coset:

$$\mathbb{Z}_p + a\rho = \{i + a\rho \mid i \in \mathbb{Z}_p\}.$$

Let $i + a\rho$ where $i \in \mathbb{Z}_p$ be an arbitrary element in the additive coset $\mathbb{Z}_p + a\rho$.

Thus, we know that $i + a\rho$ is not invertible if and only if:

$$i^2 - ia + a^2 \equiv 0 \pmod{p}.$$

Thus, if we multiply by 4 and complete the square then we find that the previous congruence becomes the following quadratic congruence:

$$(2i - a)^2 \equiv -3a^2 \pmod{p}.$$

Now $p$ is odd. Thus, we can reverse our steps and we find that the following congruences are equivalent:

$$i^2 - ia + a^2 \equiv 0 \pmod{p}$$

and

$$(2i - a)^2 \equiv -3a^2 \pmod{p}.$$
Thus, $i + a\rho$ is not invertible if and only if:

$$(2i - a)^2 \equiv -3a^2 \pmod{p}.$$ 

We can write this quadratic congruence in the following form:

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

This has (by Theorem 3.1.1): no solutions if $b$ is a nonresidue of $p$, exactly two noncongruent solutions if $b$ is a residue of $p$, and exactly one solution if $b \equiv 0 \pmod{p}$.

Now, by Theorem 3.4.19, $-3$ is a residue of all primes of the form $3n + 1$ and a nonresidue of all primes of the form $3n + 2$. Thus, if $p = 3n + 1$ then there exist exactly two $i$’s in $Z_p$ such that:

$$(2i - a)^2 \equiv -3a^2 \pmod{p}.$$ 

If $p = 3n + 2$ then there exist 0 $i$’s in $Z_p$ such that:

$$(2i - a)^2 \equiv -3a^2 \pmod{p}.$$ 

If $p = 3$ then there exist exactly one $i$ in $Z_p$ such that:

$$(2i - a)^2 \equiv -3a^2 \pmod{p}.$$ 

Thus, if $p = 3n + 1$ then the additive coset $Z_p + a\rho$ contains exactly 2 noninvertible elements. If $p = 3$ then the additive coset $Z_p + a\rho$ contains exactly 1 noninvertible elements. If $p = 3n + 2$ then the additive coset $Z_p + a\rho$ contains exactly 0 noninvertible elements.

This completes the proof.

By similar reasoning, we can prove the following which applies to additive cosets of the form $a + \rho Z_p = \{a + i\rho \mid i \in Z_p\}$, where $a \in Z_p^*$ is fixed:

**Lemma 4.1.3.** let $a \in Z_p^*$. Then each additive coset $a + \rho Z_p = \{a + i\rho \mid i \in Z_p\}$ contains:

1. 2 noninvertible elements if $p = 3n + 1$

2. 1 noninvertible element if $p = 3$
3. 0 noninvertible elements if $p = 3n + 2$

As with the previous lemma, this lemma can be written in terms of quadratic residues instead of in terms of residue classes.

We now use Lemma 4.1.1 to prove Theorem 4.1.8. Note, however, that Theorem 4.1.8 also follows from Lemma 4.1.3.

**Proof.** We consider three cases as follows. In the first case $p$ is a prime of the form $p = 3n+1$. In the second case $p$ is the prime $p = 3$. In the third case $p$ is a prime of the form $p = 3n + 2$.

In each case we note that the set: $\{i + j\rho \mid 0 \leq i \leq p - 1, 0 \leq j \leq p - 1\}$ has $p^2$ elements.

Thus, to compute the order of $G_2$, $|G_2|$ we take $p^2$ and subtract the number of noninvertible elements in the set: $\{i + j\rho \mid 0 \leq i \leq p - 1, 0 \leq j \leq p - 1\}$.

We consider the $p$ additive cosets:

$$Z_p + a\rho = \{i + a\rho \mid i \in Z_p\}$$

where $a \in Z_p$ is fixed.

We now count the number of noninvertible elements in each of these $p$ additive cosets as follows: Note, that if $a = 0$ then the additive coset $Z_p + 0\rho = Z_p$ contains exactly one noninvertible element $0 + 0\rho$. We now consider $a \in Z_p^*$.

Case one.

Let $p = 3n + 1$. We now count the number of noninvertible elements in each of the $p - 1$ additive cosets:

$$Z_p + a\rho = \{i + a\rho \mid i \in Z_p\}$$

for $a \in Z_p^*$.

Thus, by Lemma 4.1.1, each of the $p - 1$ additive cosets $Z_p + a\rho$ contains exactly 2 noninvertible elements. Thus, the total number of noninvertible elements in $\{i + j\rho \mid 0 \leq i \leq p - 1, 0 \leq j \leq p - 1\}$ is equal to $2(p - 1) + 1$.

Thus, the order of the group $G_2$ is given as:

$$|G_2| = p^2 - (2(p - 1) + 1) = p^2 - 2p + 1 = (p - 1)^2.$$

Case two.
Let \( p = 3 \). Then, by Lemma 4.1.1 each of the \( p - 1 \) additive cosets \( Z_p + a\rho = \{i + a\rho \ | \ i \in Z_p\} \), where \( a \in Z_p^* \) contains exactly one noninverting element. Thus, the total number of noninverting elements is \( p \). Therefore, the order of the group \( G_2 \) is given as:

\[ |G_2| = p^2 - p. \]

Case three.

Let \( p \) be of the form \( p = 3n + 2 \). By Lemma 4.1.1, the \( p - 1 \) additive cosets: \( Z_p + a\rho = \{i + a\rho \ | \ i \in Z_p\} \) contain no noninverting elements. Thus, \( 0 = 0 + 0\rho \) is the only noninverting element. Therefore, the order of the group \( G_2 \) is given as:

\[ |G_2| = p^2 - 1. \]

This completes the proof.

\( \square \)

4.1.7 Fermat’s Little Theorem Results For The Group \( G_2 \)

Now that we have expressions for the order of the group \( G_2 \), we can prove Fermat’s little theorem like (i.e. Fermat-like) results for this group.

Theorem 2.3.19 and Theorem 4.1.8, immediately give the following three results:

**Theorem 4.1.10.** If \( p \) is a prime of the form \( p = 3n + 1 \) then for any \((a + b\rho) \in G_2\) we have the following:

\[ (a + b\rho)^{(p-1)^2} \equiv 1 \ (mod \ p). \]

**Theorem 4.1.11.** If \( p \) is the prime \( p = 3 \) then for any \((a + b\rho) \in G_2\) we have the following:

\[ (a + b\rho)^{p^2 - p} = (a + b\rho)^6 \equiv 1 \ (mod \ p). \]

**Theorem 4.1.12.** If \( p \) is a prime of the form \( p = 3n + 2 \) then for any \((a + b\rho) \in G_2\) we have the following:

\[ (a + b\rho)^{p^2 - 1} \equiv 1 \ (mod \ p). \]

Recall, that Fermat’s little theorem (Theorem 2.3.1), states that if \( p \) is prime, \( a \) is an integer, and \( p \nmid a \) then:

92
Note, that each of the expressions for $|G_2|$, that is each of $(p - 1)^2$, $p^2 - p$, and $p^2 - 1$, is divisible by $p - 1$.

Thus, if we choose $b = 0$ to be fixed and $a \in \mathbb{Z}^*_p$ to be arbitrary, then Fermat’s little theorem immediately proves each of the congruences in the previous 3 theorems.

Therefore, each of the 3 Theorems 4.1.10, 4.1.11, and 4.1.12 are in fact generalizations of Fermat’s little theorem.

Note that in each of the Theorems 4.1.10, 4.1.11, and 4.1.12 we can replace the polynomial $a + b\rho$ with the matrix \[
\begin{bmatrix}
a & -b \\
b & a - b
\end{bmatrix}
\] to get similar results.

We can also replace the polynomial $a + b\rho$ with the binary quadratic form $a^2 - ab + b^2$ by taking the determinant and noting that the determinant of a product is the product of the determinants.

4.1.8 A Table of Values For The Order of $G_2$ and the Number of Self-Invertible Elements in $G_2$

From writing code in C, I have constructed the following table:
| Prime $p$ | $|G_2|/2^k$ | $|S(G_2)|/2^l$ |
|-----------|------------|------------|
| 2         | 3          | 1          |
| 3         | 6          | 2          |
| 5         | 24         | 2          |
| 7         | 36         | 4          |
| 11        | 120        | 2          |
| 13        | 144        | 4          |
| 17        | 288        | 2          |
| 19        | 324        | 4          |
| 23        | 528        | 2          |
| 29        | 840        | 2          |
| 31        | 900        | 4          |
| 37        | 1296       | 4          |
| 41        | 1680       | 2          |
| 43        | 1764       | 4          |
| 47        | 2208       | 2          |
| 53        | 2808       | 2          |
| 59        | 3480       | 2          |
| 61        | 3600       | 4          |
| 67        | 4356       | 4          |
| 71        | 5040       | 2          |
| 73        | 5184       | 4          |
| 79        | 6084       | 4          |
| 83        | 6888       | 2          |
| 89        | 7920       | 2          |
| 97        | 9216       | 4          |

This table agrees with Theorems 4.1.8 and 4.1.7.
4.2 Wilson’s Theorem in Three Dimensions

4.2.1 Polynomials In a Quotient Ring

Let $Z[\rho]$ be defined as in the previous section. Consider the principal ideal generated by the polynomial $1 + \rho + \rho^2 + \rho^3$, $< 1 + \rho + \rho^2 + \rho^3 > = \{ f(\rho)(1 + \rho + \rho^2 + \rho^3) \mid f(\rho) \in Z[\rho] \}$. We now form the quotient ring:

\[ Z[\rho]/ < 1 + \rho + \rho^2 + \rho^3 > = \{ g(\rho) + < 1 + \rho + \rho^2 + \rho^3 > \mid g(\rho) \in Z[\rho] \}. \]

As in the last section, we refer to these as polynomials even though they are actually equivalence classes of polynomials. Note that in $Z[\rho]/< 1 + \rho + \rho^2 + \rho^3 >$ we have $1 + \rho + \rho^2 + \rho^3 = 0$ and $\rho^4 = 1$. We define the notion of congruence for these polynomials modulo a prime $p$ in the same way as in the previous section.

As with the two dimensional case, every polynomial in $Z[\rho]/< 1 + \rho + \rho^2 + \rho^3 >$ is congruent modulo $p$ to some element in the set:

\[ \{ a + b\rho + c\rho^2 \mid 0 \leq a \leq p - 1, 0 \leq b \leq p - 1, 0 \leq c \leq p - 1 \}. \]

We shall call this set the least residue region.

We first define the notation $(i + j\rho + r\rho^2)^*$ to be equal to $i + j\rho + r\rho^2$ if $i + j\rho + r\rho^2$ is invertible mod $p$ and to be equal to 1 if $i + j\rho + r\rho^2$ is not invertible mod $p$.

Thus,

\[ (a + b\rho + c\rho^2)^* = \begin{cases} 
  a + b\rho + c\rho^2 & \text{if } a + b\rho + c\rho^2 \text{ is invertible mod } p \\
  1 & \text{otherwise}
\end{cases}. \]

In this way, we remove from the product, polynomials without inverses.

4.2.2 Wilson’s Theorem in Three Dimensions

We now have the following result which we shall call Wilson’s theorem in three dimensions:

**Theorem 4.2.1** (Wilson’s Theorem in Three Dimensions). If $p$ is prime then the product of all the elements in $Z[\rho]/< 1 + \rho + \rho^2 + \rho^3 >$ that are invertible modulo $p$ is:
\[
\prod_{i=0}^{p-1} \prod_{j=0}^{p-1} \prod_{r=0}^{p-1} (i + j\rho + r\rho^2)^* \equiv \begin{cases} 
\rho^2 \pmod{p} & \text{if } p = 2 \\
1 \pmod{p} & \text{otherwise} 
\end{cases}.
\]

We call Theorem 4.2.1 Wilson’s theorem in three dimensions because the least residue region is a three dimensional vector space over \(\mathbb{Z}_p\).

We would like to take the product of all invertible polynomials in the least residue region modulo \(p\). The invertible polynomials in the least residue region form a group which we denote as \(G_3\). Thus,

\[G_3 = \{a+b\rho+c\rho^2 \mid 0 \leq a \leq p-1, 0 \leq b \leq p-1, 0 \leq c \leq p-1, a+b\rho+c\rho^2 \text{ is invertible mod } p\}\].

We now take the product of all elements in the group \(G_3\).

Thus, we consider:

\[\prod_{g \in G_3} g.\]

Thus, we are taking the product of all members from the finite abelian group \(G_3\) and so we can apply the results in [2] due to Górowski and Lomnicki (Theorem 2.2.2) to prove Theorem 4.2.1 as follows:

**Proof.** Now, if \(p = 2\), then 1 and \(\rho^2\) are the only self-invertible elements in the product. Thus, this product is congruent to \(\rho^2\) by Theorem 2.2.2. The result now follows.

If \(p\) is odd then the product contains the trivial self-invertible elements: 1, \(p - 1\), \(\rho^2\), and \((p - 1)\rho^2\). Thus, by Górowski and Lomnicki (Theorem 2.2.2), the product is congruent to 1 modulo \(p\) and the result now follows.

\[\Box\]

### 4.2.3 The Number of Self-invertible Elements in the Group \(G_3\)

We have shown that 1, \(p - 1\), \(\rho^2\), and \((p - 1)\rho^2\) are the trivial self-invertible polynomials in the product \(\prod_{i=0}^{p-1} \prod_{j=0}^{p-1} \prod_{r=0}^{p-1} (i + j\rho + r\rho^2)^*\) for any odd prime \(p\). In the following result we show that with certain conditions on the prime \(p\), there are other, nontrivial, self-invertible polynomials in this product:
**Theorem 4.2.2.** If \( p = 2 \) then \( 1 \) and \( \rho^2 \) are the only self-invertible polynomials in the group \( G_3 \). If \( p \equiv 1 \) (mod 4) then \( G_3 \) contains exactly 4 self-invertible polynomials in addition to the trivial self-invertible polynomials: \( 1, p - 1, \rho^2, \) and \( (p - 1)\rho^2 \). If \( p \equiv 3 \) (mod 4) then the only self-invertible polynomials in \( G_3 \) are the trivial self-invertible polynomials: \( 1, p - 1, \rho^2, \) and \( (p - 1)\rho^2 \).

**Proof.** Let \( p \) be a prime.

Consider the polynomial: \( i + j\rho + r\rho^2 \).

This polynomial is self-invertible if and only if:

\[
(i + j\rho + r\rho^2)^2 \equiv 1 \pmod{p}.
\]

That is:

\[
(i^2 + r^2 - 2jr) + (2ij - 2jr)\rho + (j^2 + 2ir - 2jr)\rho^2 \equiv 1 \pmod{p}.
\]

By uniqueness of polynomials in the least residue region, this gives the following system of congruences:

\[
i^2 + r^2 - 2jr \equiv 1 \pmod{p} \quad (4.3)
\]

\[
2ij - 2jr \equiv 0 \pmod{p} \quad (4.4)
\]

and

\[
j^2 + 2ir - 2jr \equiv 0 \pmod{p} \quad (4.5)
\]

Thus, \( i + j\rho + r\rho^2 \) is a self-invertible polynomial if and only if \( i, j, \) and \( r \) satisfy the congruences (4.3), (4.4), and (4.5).

If \( p = 2 \) then this system of congruences becomes:

\[
i^2 + r^2 \equiv 1 \pmod{2}
\]

and

\[
j \equiv 0 \pmod{2}.
\]
This system has exactly 2 solutions. These are: \((i, j, r) = (1, 0, 0)\) and \((i, j, r) = (0, 0, 1)\).

Thus, if \(p = 2\) then the only self-invertible polynomials in \(G_3\) are 1 and \(\rho^2\).

If \(p\) is an odd prime, then \(i + j\rho + r\rho^2\) is a self-invertible polynomial if and only if \(i, j,\) and \(r\) satisfy the system of congruences (4.3), (4.4), and (4.5).

By the congruence (4.4), we have:

\[ j \equiv 0 \pmod{p} \]

or

\[ i \equiv r \pmod{p}. \]

If \(j \equiv 0 \pmod{p}\) then the congruence (4.5) gives: \(i \equiv 0\) or \(r \equiv 0 \pmod{p}\). These correspond to the trivial self-invertible polynomials 1, \(p - 1\), \(\rho^2\), and \((p - 1)\rho^2\).

Now let \(i \equiv r \pmod{p}\). The congruence (4.5) gives:

\[ j^2 + 2i^2 - 2ij \equiv 0 \pmod{p}. \]

Which is the same as:

\[ i^2 + (i - j)^2 \equiv 0 \pmod{p}. \]

The congruence (4.3) gives:

\[ i^2 + r^2 - 2jr \equiv 2i(i - j) \equiv 1 \pmod{p}. \]

Thus, we have:

\[ i^2 + (i - j)^2 \equiv 0 \pmod{p} \]

and

\[ 2i(i - j) \equiv 1 \pmod{p}. \]

From these we have:

\[ (2i - j)^2 \equiv 1 \pmod{p} \]
\[ j^2 \equiv -1 \pmod{p}. \]

Thus, \( i + j\rho + r\rho^2 \) is a nontrivial self-invertible polynomial if and only if \( i, j, \) and \( r \) satisfy:

\[ j^2 \equiv -1 \pmod{p}, \]

\[ (2i - j)^2 \equiv 1 \pmod{p}, \]

and

\[ r \equiv i \pmod{p}. \]

If \( p \equiv 3 \pmod{4} \) then by Theorem 3.3.1, the congruence \( j^2 \equiv -1 \pmod{p} \) has no solution. Therefore, this system of congruences has no solution. Thus \( G_3 \) contains no nontrivial self-invertible polynomials.

If \( p \equiv 1 \pmod{4} \) by Theorems 3.3.1 and 3.1.1 there exist exactly 2 integers \( j \) in \( \mathbb{Z}_p \) that satisfy the congruence \( j^2 \equiv -1 \pmod{p} \). For a fixed integer \( j \), there exist exactly 2 integers \( i \) in \( \mathbb{Z}_p \) that satisfy the congruence \( (2i - j)^2 \equiv 1 \pmod{p} \). Therefore, there exist exactly 4 ordered triples of integers \( (i, j, r) \) that satisfy this system of congruences. Thus, if \( p \equiv 1 \pmod{4} \), then \( G_3 \) contains exactly 4 nontrivial self-invertible polynomials.

The result now follows.
Theorem 4.2.3.

\[ |S(G_3)| = \begin{cases} 
2 & \text{if } p = 2 \\
8 & \text{if } p \equiv 1 \pmod{4} \\
4 & \text{if otherwise} 
\end{cases} \]

This result can be written in terms of quadratic residues instead of in terms of residue classes as follows:

Theorem 4.2.4.

\[ |S(G_3)| = \begin{cases} 
8 & \text{if } -1 \text{ is a residue of } p \\
4 & \text{if } -1 \text{ is a nonresidue of } p \\
2 & \text{otherwise} 
\end{cases} \]

Note, that in addition to proving this result, I have also verified it for the first 25 primes by writing code in C.

4.2.4 Matrices in a Quotient Ring

We now make the connection to matrices.

In finding the inverse of \( \alpha = a + b\rho + c\rho^2 \) we are required to find \( \beta = d + e\rho + f\rho^2 \) such that \( \alpha\beta = 1 \). That is,

\[(a + b\rho + c\rho^2)(d + e\rho + f\rho^2) = 1.\]

Now since \( \rho^4 = 1 \) and \( 1 + \rho + \rho^2 + \rho^3 = 0 \), this is the same as:

\[(ad + cf - bf - ce) + (ae + bd - bf - ce)\rho + (af + bc + cd - bf - ce)\rho^2 = 1.\]

If we write this system of linear equations in matrix form, we have the following:

\[
\begin{bmatrix}
a & -c & c-b \\
b & a-c & -b \\
c & b-c & a-b \\
\end{bmatrix}
\begin{bmatrix}
d \\
e \\
f \\
\end{bmatrix}
= 
\begin{bmatrix}
1 \\
0 \\
0 \\
\end{bmatrix}
\]

Let \( M_3(a,b,c) = 
\begin{bmatrix}
a & -c & c-b \\
b & a-c & -b \\
c & b-c & a-b \\
\end{bmatrix} \) denote the coefficient matrix for this system. We have taken the problem of trying to find the inverse of the polynomial \( a + b\rho + c\rho^2 \) and
converted to the problem of finding the inverse of the matrix $M_3(a,b,c)$. This suggests that the function that maps the polynomial $a + b\rho + c\rho^2$ to the matrix $M_3(a,b,c)$ is a ring isomorphism.

Thus, we have the following:

**Theorem 4.2.5.** The map $\Phi(a+b\rho+c\rho^2) = \begin{bmatrix} a & -c & c-b \\ b & a-c & -b \\ c & b-c & a-b \end{bmatrix}$ is a ring isomorphism from $Z[\rho]/ < 1 + \rho + \rho^2 + \rho^3 >$ to $M_3(Z)$.

We prove this as follows:

**Proof.** Let the function $\Phi$ that maps polynomials in $Z[\rho]/ < 1 + \rho + \rho^2 + \rho^3 >$ to $M_3(Z)$ be defined as follows:

$$\Phi(a+b\rho+c\rho^2) = \begin{bmatrix} a & -c & c-b \\ b & a-c & -b \\ c & b-c & a-b \end{bmatrix}$$

We show that $\Phi$ is a ring isomorphism. Clearly, $\Phi$ is a bijection that preserves addition. We now show that $\Phi$ also preserves multiplication.

$$\Phi((a+b\rho+c\rho^2)(d+e\rho+f\rho^2))$$

$$= \Phi((ad-bf-ce+cf) + (ae+bd-bf-ce)\rho + (af+be+cd-bf-ce)\rho^2)$$

$$= \begin{bmatrix} d & -f & f-e \\ e & d-f & -e \\ f & e-f & d-e \end{bmatrix}$$

$$= \Phi(a+b\rho+c\rho^2)\Phi(d+e\rho+f\rho^2).$$

Thus, $\Phi$ is a bijection that preserves addition and multiplication. This completes the proof.
Note that Theorem 4.2.5 also follows from the corollary to the Cayley Hamilton theorem (Theorem 4.1.1).

Notice that the first column of $M_3(a, b, c)$ consists of the coefficients of $a + b\rho + c\rho^2$. The second column of $M_3(a, b, c)$ consists of the coefficients of $\rho(a + b\rho + c\rho^2) = (-c) + (a - c)\rho + (b - c)\rho^2$. The third column of $M_3(a, b, c)$ consists of the coefficients of $\rho^2(a + b\rho + c\rho^2) = (c - b) + (-b)\rho + (a - b)\rho^2$. Also, notice that this ring isomorphism maps the polynomial

$$\rho = 0(1) + 1\rho + 0\rho^2$$

to the matrix $M_3(0, 1, 0) = \begin{bmatrix} 0 & 0 & -1 \\ 1 & 0 & -1 \\ 0 & 1 & -1 \end{bmatrix}$. Now $\rho$ satisfies the polynomial equation $1 + \rho + \rho^2 + \rho^3 = 0$. Thus, $M_3(0, 1, 0)$ also satisfies this polynomial equation. $M_3(0, 1, 0)$ is in fact the companion matrix of this polynomial. Companion matrices of polynomials are studied in [9].

In light of Theorem 4.2.5, we can replace the polynomial $i + j\rho + r\rho^2$ in the product in Theorem 4.2.1 by the corresponding matrix:

$$M_3(i, j, r) = \begin{bmatrix} i & -r & r - j \\ j & i - r & -j \\ r & j - r & i - j \end{bmatrix},$$

this gives us the following:

**Theorem 4.2.6.** If $p$ is prime then:

$$\prod_{i=0}^{p-1} \prod_{j=0}^{p-1} \prod_{r=0}^{p-1} \begin{bmatrix} i & -r & r - j \\ j & i - r & -j \\ r & j - r & i - j \end{bmatrix}^* \equiv \begin{cases} \begin{bmatrix} 0 & -1 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} & \text{(mod } p\text{)} \text{ if } p = 2 \\ \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} & \text{(mod } p\text{)} \text{ otherwise} \end{cases}.$$

As usual, we have eliminated elements in the product without inverses by introducing the following notation:

$$\begin{bmatrix} i & -r & r - j \\ j & i - r & -j \\ r & j - r & i - j \end{bmatrix}^* = \begin{bmatrix} i & -r & r - j \\ j & i - r & -j \\ r & j - r & i - j \end{bmatrix}$$

if $(i + j\rho + r\rho^2)^* = i + j\rho + r\rho^2$ and

102
\[
\begin{bmatrix}
i & -r & r - j \\
\hline
j & i - r & -j \\
r & j - r & i - j
\end{bmatrix}^* = \begin{bmatrix}
1 & 0 & 0 \\
0 & 1 & 0 \\
0 & 0 & 1
\end{bmatrix}
\] if \((i + j\rho + r\rho^2)^* = 1\). Where the * notation for polynomials has been defined previously.

Note that in Theorem 4.2.2 we can replace the polynomial \(i + j\rho + r\rho^2\) with the corresponding matrix \[
\begin{bmatrix}
i & -r & r - j \\
\hline
j & i - r & -j \\
r & j - r & i - j
\end{bmatrix}
\]. In this way, we can restate Theorem 4.2.2 in terms of matrices instead of polynomials.

We now give a matrix proof of Theorem 4.2.2. The proof that follows is in one direction only.

We prove that if \(p\) is odd and the matrix \(A = \begin{bmatrix}
i & -r & r - j \\
\hline
j & i - r & -j \\
r & j - r & i - j
\end{bmatrix}\) is self-invertible modulo \(p\) then \(i, j,\) and \(r\) satisfy the following system of congruences:

\[
j^2 \equiv -1 \ (mod \ p),
\]

\[
(2i - j)^2 \equiv 1 \ (mod \ p),
\]

and

\[
r \equiv i \ (mod \ p).
\]

This system of congruences has no solutions if \(p \equiv 3 \ (mod \ 4)\) and exactly 4 solutions if \(p \equiv 1 \ (mod \ 4)\).

\textit{Proof.} Consider the matrix:

\[
A = \begin{bmatrix}
i & -r & r - j \\
\hline
j & i - r & -j \\
r & j - r & i - j
\end{bmatrix}.
\]

Let \(\Delta\) be the determinant of this matrix. That is:
\[ \Delta = \begin{vmatrix} i & -r & r - j \\ j & i - r & -j \\ r & j - r & i - j \end{vmatrix}. \]

We may assume that our matrix is invertible since only invertible matrices appear in our product. Thus, \( \Delta \not\equiv 0 \pmod{p} \) and:

\[
\begin{bmatrix} i & -r & r - j \\ j & i - r & -j \\ r & j - r & i - j \end{bmatrix}^{-1} = \frac{1}{\Delta} \text{adj}(A) = \frac{1}{\Delta} \begin{bmatrix} C_{11} & C_{21} & C_{31} \\ C_{12} & C_{22} & C_{32} \\ C_{13} & C_{23} & C_{33} \end{bmatrix}.
\]

Where \( \text{adj}(A) = \begin{bmatrix} C_{11} & C_{21} & C_{31} \\ C_{12} & C_{22} & C_{32} \\ C_{13} & C_{23} & C_{33} \end{bmatrix} \) is the adjugate of the matrix \( A \).

Here, \( C_{mn} \) is the co-factor of the matrix

\[
\begin{bmatrix} i & -r & r - j \\ j & i - r & -j \\ r & j - r & i - j \end{bmatrix}.
\]

The exact value of \( \Delta \) is as follows:

\[
\Delta = i^3 - i^2 j - i^2 r + ij^2 + 2ijr - ir^2 - j^3 + j^2 r - jr^2 + r^3.
\]

Note that from this expression, it follows that if \( i, j \equiv 0 \pmod{p} \) then \( \Delta \equiv r^3 \pmod{p} \) and that if \( j, r \equiv 0 \pmod{p} \) then \( \Delta \equiv i^3 \pmod{p} \).

If our matrix is self-invertible then it satisfies the following:

\[
\begin{bmatrix} i & -r & r - j \\ j & i - r & -j \\ r & j - r & i - j \end{bmatrix} \equiv \frac{1}{\Delta} \begin{bmatrix} C_{11} & C_{21} & C_{31} \\ C_{12} & C_{22} & C_{32} \\ C_{13} & C_{23} & C_{33} \end{bmatrix} \pmod{p}.
\]

Thus, by equating entries in the first column of this matrix congruence, we have the following system of three congruences:

\[
i\Delta \equiv C_{11} = \begin{vmatrix} i - r & -j \\ j - r & i - j \end{vmatrix} \pmod{p},
\]

\[
j\Delta \equiv C_{12} = (-1)^{\delta} \begin{vmatrix} j & -j \\ r & i - j \end{vmatrix} \pmod{p},
\]
and

\[ r\Delta \equiv C_{13} = \left| \begin{array}{cc} j & i - r \\ r & j - r \end{array} \right| (mod p). \]

This system of congruences is equivalent to the following system:

\[ i\Delta \equiv i^2 - ij + j^2 - ir (mod p) \quad (4.6) \]

\[ j\Delta \equiv (-1)(ij - j^2 + rj) (mod p) \quad (4.7) \]

and

\[ r\Delta \equiv r^2 - rj + j^2 - ri (mod p) \quad (4.8) \]

From the congruence (4.7) we can factor out a \( j \) from the right hand side to give \( j \equiv 0 \) or \( \Delta \equiv (-1)(i - j + r) \). We consider each of these two cases separately.

If \( j \equiv 0 \) then the congruence (4.6) gives \( i \equiv 0 \) or \( \Delta \equiv i - r \).

If \( i \equiv 0 \) then \( \Delta \equiv r^3 \neq 0 \). Thus, the congruence (4.8) becomes \( r^2 \equiv 1 (mod p) \). Thus, \( r = 1 \) or \( r = p - 1 \) and our matrix is either:

\[
\begin{bmatrix}
0 & -1 & 1 \\
-1 & 0 & 1 \\
1 & 1 & 0
\end{bmatrix} \quad \text{or} \quad \begin{bmatrix}
0 & -1 & 0 \\
1 & 1 & 0 \\
p - 1 & 1 & 0
\end{bmatrix}.
\]

If \( \Delta \equiv i - r \) then by the congruence (4.8) \( r \equiv 0 \). Thus, \( \Delta \equiv i^3 \neq 0 \).

From (4.6) \( i^2 \equiv 1 (mod p) \). Therefore, \( i = 1 \) or \( i = p - 1 \). and our matrix is either:

\[
\begin{bmatrix}
1 & 0 & 0 \\
0 & 1 & 0 \\
0 & 0 & 1
\end{bmatrix} \quad \text{or} \quad \begin{bmatrix}
p - 1 & 0 & 0 \\
0 & p - 1 & 0 \\
0 & 0 & p - 1
\end{bmatrix}.
\]

Thus, we have accounted for the trivial self-invertible matrices.

If \( \Delta \equiv (-1)(i - j + r) \) then by the congruences (4.6) and (4.8), we can eliminate \( \Delta \) to give:

\[ 2i^2 + j^2 - 2ij \equiv 0 (mod p) \]

and

\[ 2r^2 + j^2 - 2rj \equiv 0 (mod p). \]
From these quadratic form congruences it is clear that $r \equiv i \ (mod\ p)$ and $i^2 + (i - j)^2 \equiv 0 \ (mod\ p)$.

From $\Delta \equiv (-1)(i - j + r)$ and from $r \equiv i$ it follows that $(2i - j)^2 \equiv (i - r - \Delta)^2 \equiv \Delta^2$. Now the matrix $A$ is self-invertible. Thus, $\Delta^2 = (detA)^2 = det(A^2) = det(I) = 1$. It now follows that $(2i - j)^2 \equiv 1 \ (mod\ p)$.

Thus,

$$(2i - j)^2 = (i + (i - j))^2 = i^2 + (i - j)^2 + 2i(i - j) \equiv 1 \ (mod\ p).$$

Since $i^2 + (i - j)^2 \equiv 0 \ (mod\ p)$ we have:

$$2i(i - j) \equiv 1 \ (mod\ p).$$

Now, $i^2 + (i - j)^2 \equiv 0 \ (mod\ p)$. Thus,

$$i^2 + i^2 - 2ij + j^2 \equiv 0 \ (mod\ p).$$

Therefore,

$$2i(i - j) + j^2 \equiv 0 \ (mod\ p).$$

Thus, we have:

$$j^2 \equiv -1 \ (mod\ p).$$

Thus, we have shown that if the matrix $A$ is a nontrivial self-invertible matrix modulo $p$ then $i, j$, and $r$ satisfy the following system of congruences:

$$j^2 \equiv -1 \ (mod\ p),$$

$$(2i - j)^2 \equiv 1 \ (mod\ p),$$

and

$$r \equiv i \ (mod\ p).$$

This system of congruences is the same system that we encountered in the proof of
Theorem 4.2.2.

As in the proof of Theorem 4.2.2, the forward direction now follows. \(\square\)

4.2.5 Matrix and Determinant Forms of Wilson in Three Dimensions

If we now take the determinant of the previous result, we then have:

**Theorem 4.2.7.** If \(p\) is prime then:

\[
\prod_{i=0}^{p-1} \prod_{j=0}^{p-1} \prod_{r=0}^{p-1} \begin{vmatrix}
 i & -r & r - j \\
 j & i - r & -j \\
 r & j - r & i - j
\end{vmatrix}^* \equiv 1 \pmod{p}.
\]

Where we define:

\[
\begin{vmatrix}
 i & -r & r - j \\
 j & i - r & -j \\
 r & j - r & i - j
\end{vmatrix}^* = \det \begin{vmatrix}
 i & -r & r - j \\
 j & i - r & -j \\
 r & j - r & i - j
\end{vmatrix}.
\]

4.2.6 A Conjecture for The Order of The Group \(G_3\)

In order to apply Theorem 2.3.19 to the group \(G_3\), we need to know \(|G_3|\), the order of the group \(G_3\).

Now, \(G_3 = \{a + bp + cp^2 \mid 0 \leq a \leq p - 1, 0 \leq b \leq p - 1, 0 \leq c \leq p - 1, a + bp + cp^2\) is invertible mod \(p\}\) is isomorphic to the set of invertible matrices in the set:

\[
\left\{ \begin{bmatrix} i & -r & r - j \\ j & i - r & -j \\ r & j - r & i - j \end{bmatrix} : i, j, r \in \mathbb{Z}_p \right\}.
\]

This set of invertible matrices form a subgroup of \(GL_3(\mathbb{Z}_p)\), the general linear group of three by three matrices with entries in \(\mathbb{Z}_p\).

We now would like to know the order of \(GL_3(\mathbb{Z}_p)\). Consider an arbitrary element of \(GL_3(\mathbb{Z}_p)\):
Consider the first column of $A$. This column cannot be 0, and each entry is in $Z_p$. Thus, there are $p^3 - 1$ possibilities for the first column. Consider the second column. This cannot be a multiple of the first column. So there are $p^3 - p$ possibilities for the second column. Consider the third column. This cannot be a linear combination of the first and second columns. Thus, there are $p^3 - p^2$ possibilities for the third column.

Thus, we have proved the following:

**Theorem 4.2.8.** The order of the group $GL_3(Z_p)$ is given as:


From this and the well-known fact from algebra that the order of a subgroup divides the order of the group, we have the following result:

**Theorem 4.2.9.** The order of the group $G_3$ divides $(p^3 - 1)(p^3 - p)(p^3 - p^2)$.

From writing code in C and considering the first 25 primes, I have constructed the following table:
| Prime $p$ | $|G_3|$ | $|S(G_3)|$ |
|---------|------|--------|
| 2       | 4    | 2      |
| 3       | 16   | 4      |
| 5       | 72   | 8      |
| 7       | 288  | 4      |
| 11      | 1200 | 4      |
| 13      | 1784 | 8      |
| 17      | 4192 | 8      |
| 19      | 6480 | 4      |
| 23      | 11616| 4      |
| 29      | 22232| 8      |
| 31      | 28800| 4      |
| 37      | 47112| 8      |
| 41      | 64560| 8      |
| 43      | 77616| 4      |
| 47      | 101568| 4    |
| 53      | 141544| 8   |
| 59      | 201840| 4   |
| 61      | 217240| 8   |
| 67      | 296208| 4   |
| 71      | 352800| 4   |
| 73      | 375024| 8   |
| 79      | 486720| 4   |
| 83      | 564816| 4   |
| 89      | 684112| 8   |
| 97      | 887872| 8   |

Note, that this table agrees with theorem 4.2.4.

From this table, I am lead to conjecture the following three results:

**Conjecture 4.2.1.** If $p$ is a prime of the form $4n + 3$ then:

$$|G_3| = (p - 1)^2(p + 1) = p^3 - p^2 - p + 1.$$

**Conjecture 4.2.2.** $|G_3|$ is equal to a monic cubic polynomial in $Z[p]$.

**Conjecture 4.2.3.** $\frac{|G_3|}{p^r} \to 1$ as $p \to \infty$. 

109
4.2.7 A Fermat’s Little Theorem Conjecture for the Group $G_3$

Now that we have conjectured an expression for the order of the group $G_3$, we can apply Theorem 2.3.19 to get a conjectured Fermat-like result for this group.

From Conjecture 4.2.1, I make the following conjecture:

**Conjecture 4.2.4.** If $p$ is a prime of the form $4n + 3$ and $(a + b\rho + c\rho^2) \in G_3$ then:

$$(a + b\rho + c\rho^2)^{(p-1)^2(p+1)} = (a + b\rho + c\rho^2)^{p^3 - p^2 - p + 1} \equiv 1 \pmod{p}.$$ 

Note that this conjecture can be written in terms of matrices or determinants instead of in terms of polynomials.

Also, note that the Conjectures 4.2.1, 4.2.2, and 4.2.3 can be written in terms of quadratic residues instead of in terms of residue classes as follows:

**Conjecture 4.2.5.** If $-1$ is a nonresidue of $p$ then:

$$|G_3| = (p - 1)^2(p + 1) = p^3 - p^2 - p + 1.$$ 

**Conjecture 4.2.6.** If $-1$ is a nonresidue of $p$ and $a + b\rho + c\rho^2 \in G_3$ then:

$$(a + b\rho + c\rho^2)^{(p-1)^2(p+1)} = (a + b\rho + c\rho^2)^{p^3 - p^2 - p + 1} \equiv 1 \pmod{p}.$$ 

Note that we can write this Fermat-like conjectured result for the group $G_3$ in terms of matrices or determinants instead of polynomials.

4.3 Wilson’s Theorem in Four Dimensions

4.3.1 The Group $G_4$ In Terms of Polynomials in a Quotient Ring

In this section we consider polynomials in the quotient ring: $\mathbb{Z}[\rho]/ < 1 + \rho + \rho^2 + \rho^3 + \rho^4 >$. We take the group of polynomials in $\mathbb{Z}[\rho]/ < 1 + \rho + \rho^2 + \rho^3 + \rho^4 >$ that are invertible modulo a prime $p$.

Thus, we are lead to consider the group:

$$G_4 = \{a + b\rho + c\rho^2 + d\rho^3 \mid 0 \leq a, b, c, d \leq p - 1, a + b\rho + c\rho^2 + d\rho^3 \text{ is invertible mod } p \}.$$
4.3.2 Wilson’s Theorem in Four Dimensions

We now apply the results in [2] due to Górowski and Lomnicki (Theorem 2.2.2) to the product:

\[ \prod_{g \in G_4} g \]

to arrive at the following result. As usual we introduce the * notation to remove noninvertible elements from the product.

**Theorem 4.3.1** (Wilson’s Theorem in Four Dimensions). *If \( p \) is prime and 5 is a quadratic residue of \( p \) then the product of all the elements in \( Z[\rho]/ < 1 + \rho + \rho^2 + \rho^3 + \rho^4 > \) that are invertible modulo \( p \) is:

\[
\prod_{i=0}^{p-1} \prod_{j=0}^{p-1} \prod_{r=0}^{p-1} \prod_{s=0}^{p-1} (i + j\rho + r\rho^2 + s\rho^3)^* \equiv 1 \pmod{p}.
\]

**Proof.** This product contains the trivial self-invertible polynomials 1 and \( p - 1 \). As in our proof of Wilson in two dimensions, we show that with certain restrictions on the prime \( p \), (these restrictions being that 5 is a quadratic residue mod \( p \)) there exists nontrivial self-invertible polynomials in the product \( \prod_{i=0}^{p-1} \prod_{j=0}^{p-1} \prod_{r=0}^{p-1} \prod_{s=0}^{p-1} (i + j\rho + r\rho^2 + s\rho^3)^* \). The result will now follow by the results in [2] due to Górowski and Lomnicki (Theorem 2.2.2).

4.3.3 Self-Invertible Elements in the Group \( G_4 \)

Consider the polynomial in \( Z[\rho]/ < 1 + \rho + \rho^2 + \rho^3 + \rho^4 > \):

\[ i + j\rho + r\rho^2 + s\rho^3. \]

This polynomial will be self-invertible if and only if:

\[(i + j\rho + r\rho^2 + s\rho^3)^2 \equiv 1 \pmod{p}.\]

If we expand this expression and use the facts that \( 1 + \rho + \rho^2 + \rho^3 + \rho^4 = 0 \) and \( \rho^5 = 1 \) this gives the following system of congruences:

\[ i^2 - 2js - r^2 + 2rs \equiv 1 \pmod{p}, \]
\[
2ij - 2js + s^2 - r^2 \equiv 0 \pmod{p},
\]

\[
2ir - 2js + j^2 - r^2 \equiv 0 \pmod{p},
\]

and

\[
2is + 2jr - 2js - r^2 \equiv 0 \pmod{p}.
\]

We now make the assumption that \( j \equiv 0 \pmod{p} \). With this, the second congruence gives:

\[
s \equiv \pm r \pmod{p}.
\]

We choose \( s \equiv r \pmod{p} \) so that the fourth congruence is satisfied. The third congruence gives:

\[
r(2i - r) \equiv 0 \pmod{p}.
\]

Thus, \( r \equiv 0 \) or \( r \equiv 2i \pmod{p} \).

If \( r \equiv 0 \) then we have the trivial self-invertible polynomials: 1 and \( p - 1 \).

If \( r \equiv 2i \pmod{p} \), then the first congruence gives:

\[
5i^2 \equiv 1 \pmod{p}
\]

Thus, we have constructed the nontrivial self-invertible polynomial \( i + j\rho + r\rho^2 + s\rho^3 \) where \( i, j, r, \) and \( s \) are chosen such that \( 5i^2 \equiv 1 \pmod{p} \), \( j \equiv 0 \pmod{p} \), \( r \equiv 2i \pmod{p} \), and \( s \equiv r \pmod{p} \). We have not used the fourth congruence, however the reader may check that with our choice of \( i, j, r, \) and \( s \) it is satisfied.

Now, there exists an integer \( i \) such that \( 5i^2 \equiv 1 \pmod{p} \) if and only if 5 is a quadratic residue modulo \( p \). Thus, if 5 is a quadratic residue modulo \( p \) then the product:

\[
\prod_{i=0}^{p-1} \prod_{j=0}^{p-1} \prod_{r=0}^{p-1} \prod_{s=0}^{p-1} (i + j\rho + r\rho^2 + s\rho^3)^k
\]

contains a nontrivial self-invertible polynomial and therefore by results in [2] due to Górowski and Lomnicki (Theorem 2.2.2) this product is congruent to 1 mod \( p \).
This completes the proof.

As a special case of this, consider the prime $p = 11$. This prime is of the form $5n + 1$. Thus, by Gauss [7] (Theorem 3.4.22) or by quadratic reciprocity (Theorem 3.5.4) 5 is a quadratic residue of 11. Now choose $i = 3$, $j = 0$, $r = 6$, and $s = 6$. These choices clearly satisfy: $5i^2 \equiv 1 \pmod{11}$, $j \equiv 0 \pmod{11}$, $r \equiv 2i \pmod{11}$, and $s \equiv r \pmod{11}$ Thus, the polynomial $3 + 6\rho^2 + 6\rho^3$ is a nontrivial self-invertible polynomial modulo 11.

Note that because of our assumption: $j \equiv 0 \pmod{p}$ the previous proof tells us nothing if 5 is not a quadratic residue modulo $p$.

Note that if $p$ is a prime of the form $5n + 1$ or $5n + 4$, then it follows from either Gauss (Theorem 3.4.22) or quadratic reciprocity (Theorem 3.5.4), that 5 is a residue of $p$. Thus, we can write the previous result in terms of primes in residue classes rather than in terms of quadratic residues as follows:

**Theorem 4.3.2** (Wilson’s Theorem in Four Dimensions). *If $p$ is a prime of the form $5n + 1$ or $5n + 4$ then the product of all the elements in $\mathbb{Z} \left[ \rho \right]/ < 1 + \rho + \rho^2 + \rho^3 + \rho^4 >$ that are invertible modulo $p$ is:*

\[
\prod_{i=0}^{p-1} \prod_{j=0}^{p-1} \prod_{r=0}^{p-1} \prod_{s=0}^{p-1} (i + j\rho + r\rho^2 + s\rho^3)^* \equiv 1 \pmod{p}.
\]

Let $|S(G_4)|$ denote the number of self-invertible elements in the group $G_4$.

From the previous proof we have essentially shown that if $p$ is of the form $5n + 1$ or $5n + 4$, then $|S(G_4)| \geq 4$.

From writing code in C and considering the first 25 primes, I have constructed the following table:
From this table, I am led to believe the following conjecture:

**Conjecture 4.3.1.**

\[
|S(G_4)| = \begin{cases} 
1 & \text{if } p = 2 \\ 
\geq 4 & \text{if } p \equiv 1 \pmod{5} \\ 
4 & \text{if } p \equiv 4 \pmod{5} \\ 
2 & \text{otherwise}
\end{cases}
\]
Note that the inequality: $|S(G_4)| \geq 4$ when $p \equiv 1 \ (mod \ 5)$, follows from our previous proof where we constructed a nontrivial self-invertible polynomial from the assumption that 5 is a quadratic residue of $p$. Note, that from the previous table, the values of $|S(G_4)|$, when $p \equiv 1 \ (mod \ 5)$, are unusually large. In fact, $|S(G_4)| = 11$ when $p = 61$. This explains how easy it was in the previous proof to construct a nontrivial self-invertible polynomial when $p$ is of the form $5n + 1$.

4.4 Wilson’s Theorem in 5 Dimensions

4.4.1 The Group $G_5$ Defined In Terms of a Quotient Ring

In this section we consider polynomials in the quotient ring: $\mathbb{Z}[\rho]/<1 + \rho + \rho^2 + \rho^3 + \rho^4 + \rho^5>$. We take the group of polynomials in $\mathbb{Z}[\rho]/<1 + \rho + \rho^2 + \rho^3 + \rho^4 + \rho^5>$ that are invertible modulo a prime $p$.

Thus, we are lead to consider the group:

$$G_4 = \{a+b\rho+c\rho^2+d\rho^3+e\rho^4 \mid 0 \leq a, b, c, d, e \leq p-1, a+b\rho+c\rho^2+d\rho^3+e\rho^4 \text{ is invertible mod } p \}.$$ 

As usual, we introduce the $\ast$ notation to remove from the product elements that are not invertible modulo $p$.

4.4.2 Wilson’s Theorem in Five Dimensions

We now apply results in [2] due to Górowski and Lomnicki (Theorem 2.2.2) to the product:

$$\prod_{g \in G_5} g$$

to arrive at the following:

**Theorem 4.4.1** (Wilson’s Theorem in Five Dimensions). If $p$ is prime then the product of all the elements in $\mathbb{Z}[\rho]/<1 + \rho + \rho^2 + \rho^3 + \rho^4 + \rho^5>$ that are invertible modulo $p$ is:

$$\prod_{i=0}^{p-1} \prod_{j=0}^{p-1} \prod_{r=0}^{p-1} \prod_{s=0}^{p-1} \prod_{t=0}^{p-1} (i+j\rho+r\rho^2+s\rho^3+t\rho^4)^\ast \equiv \begin{cases} \rho^3 \ (mod \ p) & \text{if } p = 2 \\ 1 \ (mod \ p) & \text{otherwise} \end{cases}.$$
Proof. The proof is a straightforward application of Theorem 2.2.2. If $p = 2$ then the only self-invertible polynomials are 1 and $p^3$ and the result follows from Theorem 2.2.2.

If $p$ is odd then the product contains the trivial self-invertible polynomials: 1, $p - 1$, $p^3$, and $(p - 1)p^3$. The result now follows from Theorem 2.2.2.

As before, in this result we can replace polynomials with matrices and determinants.

4.4.3 Self-Invertible Elements in the Group $G_5$

If we let $|S(G_5)|$ denote the number of self-invertible elements in the group $G_5$, then in proving the previous theorem, we have also proved the following:

**Theorem 4.4.2.**

$$|S(G_5)| = \begin{cases} 2 & \text{if } p = 2 \\ \geq 4 & \text{if } p \neq 2 \end{cases}.$$

Note that from considering the first 25 prime numbers and writing code in C, I have constructed the following table:
| Prime $p$ | $|S(G_5)|$ |
|----------|-------|
| 2        | 2     |
| 3        | 4     |
| 5        | 7     |
| 7        | 20    |
| 11       | 7     |
| 13       | 23    |
| 17       | 7     |
| 19       | 21    |
| 23       | 7     |
| 29       | 7     |
| 31       | 20    |
| 37       | 21    |
| 41       | 7     |
| 43       | 23    |
| 47       | 7     |
| 53       | 7     |
| 59       | 7     |
| 61       | 21    |
| 67       | 20    |
| 71       | 7     |
| 73       | 20    |
| 79       | 20    |
| 83       | 7     |
| 89       | 7     |
| 97       | 20    |

This table leads me to believe the following conjecture:

**Conjecture 4.4.1.**

$$|S(G_5)| = \begin{cases} 
2 & \text{if } p = 2 \\
4 & \text{if } p = 3 \\
\geq 20 & \text{if } p \equiv 1 \pmod{6} \\
7 & \text{if } p \equiv 5 \pmod{6} 
\end{cases}$$
Note, that from the previous table, \(|S(G_5)|\) is unusually large when \(p \equiv 1 \pmod{6}\). As an example, \(|S(G_5)| = 23\) when \(p = 13\).

Also, in the previous table, when \(p \equiv 1 \pmod{6}\), \(|S(G_5)|\) takes on only 3 values. These values are 20, 21, and 23.

Similarly, in the previous section, I have observed from writing code in C, considering the first 25 primes, and constructing a table that when \(p \equiv 1 \pmod{5}\), \(|S(G_4)|\) takes on only 3 values. These are 8, 9, and 11.

\section{Wilson’s Theorem in \(N - 1\) Dimensions}

\subsection{The Group \(G_{N-1}\) Defined in Terms of Polynomials in a Quotient Ring}

Let \(Z[\rho] = \{a_n \rho^n + \ldots + a_1 \rho + a_0 \mid a_i \in Z\}\) be the set of polynomials in the variable \(\rho\) with coefficients in \(Z\). Consider the principal ideal generated by the polynomial \(1 + \rho + \rho^2 + \ldots + \rho^{N-1}\), \(< 1 + \rho + \rho^2 + \ldots + \rho^{N-1}\rangle = \{f(\rho)(1 + \rho + \rho^2 + \ldots + \rho^{N-1}) \mid f(\rho) \in Z[\rho]\}\). We now form the quotient ring:

\[Z[\rho]/< 1 + \rho + \rho^2 + \ldots + \rho^{N-1}> = \{g(\rho) + < 1 + \rho + \rho^2 + \ldots + \rho^{N-1}> \mid g(\rho) \in Z[\rho]\}\].

Notice that in this quotient ring we have \(1 + \rho + \ldots + \rho^{N-1} = 0\) and \(\rho^N = 1\).

We now consider the group of invertible elements in:

\[\{i_0 + i_1 \rho + \ldots + i_{N-2} \rho^{N-2} \mid 0 \leq i_0, i_1, \ldots, i_{N-2} \leq p - 1\}\].

Thus, we consider \(G_{N-1}\) to be the elements in the following set that are invertible modulo \(p\):

\[\{i_0 + i_1 \rho + \ldots + i_{N-2} \rho^{N-2} \mid 0 \leq i_0, i_1, \ldots, i_{N-2} \leq p - 1\}\]

\subsection{Wilson’s Theorem in \(N - 1\) Dimensions}

We now apply results in [2] due to Górowski and Lomnicki (Theorem 2.2.2) to the group \(G_{N-1}\). Thus, we are lead to consider the product:
\[ \prod_{g \in G_{N-1}} g. \]

From this we have the following main result of this thesis which clearly generalizes Wilson’s theorem in 3 dimensions (Theorem 4.2.1) and Wilson’s theorem in 5 dimensions (Theorem 4.4.1):

**Theorem 4.5.1** (Wilson’s Theorem in \( N−1 \) Dimensions). If \( p \) is prime and \( N > 2 \) is an even natural number then the product of all the elements in \( Z[\rho]/<1+\rho+\rho^2+...+\rho^{N-1}> \) that are invertible modulo \( p \) is:

\[
\prod_{i_0=0}^{p-1} \prod_{i_1=0}^{p-1} \prod_{i_{N-2}=0}^{p-1} (i_0 + i_1\rho + ... + i_{N-2}\rho^{N-2})^* \equiv \begin{cases} 
\rho^{N/2} \pmod{p} & \text{if } p = 2 \\
1 \pmod{p} & \text{otherwise}
\end{cases}.
\]

Or in sigma notation:

**Theorem 4.5.2** (Wilson’s Theorem in \( N−1 \) Dimensions). If \( p \) is prime and \( N > 2 \) is an even natural number then the product of all the elements in \( Z[\rho]/<1+\rho+\rho^2+...+\rho^{N-1}> \) that are invertible modulo \( p \) is:

\[
\prod_{i_0=0}^{p-1} \prod_{i_1=0}^{p-1} \prod_{i_{N-2}=0}^{p-1} \left( \sum_{j=0}^{N-2} i_j\rho^j \right)^* \equiv \begin{cases} 
\rho^{N/2} \pmod{p} & \text{if } p = 2 \\
1 \pmod{p} & \text{otherwise}
\end{cases}.
\]

As in previous sections, we have introduced the \( * \) notation to eliminate noninvertible elements from the product.

We now prove this theorem.

**Proof.** If \( p = 2 \) then 1 and \( \rho^{N/2} \) are the only self-invertible elements. Thus, by Górowski and Łomnicki (Theorem 2.2.2) the product is congruent to \( \rho^{N/2} \).

Now suppose that \( p \) is odd. Note that since \( \rho^N = 1 \) and \( N \) is even, it follows that 1, \( p−1 \), \( \rho^{N/2} \) and \( (p−1)\rho^{N/2} \) are all self-invertible.

Thus, by Górowski and Łomnicki (Theorem 2.2.2) the product is congruent to 1 modulo \( p \).
4.5.3 The Self-Invertible Elements in the Group $G_{N-1}$

If we let $|S(G_{N-1})|$ denote the number of self-invertible polynomials in $G_{N-1}$ then we have proved the following:

**Theorem 4.5.3.** If $p$ is prime and $N > 2$ is even, then:

$$|S(G_{N-1})| = \begin{cases} 
2 & \text{if } p = 2 \\
\geq 4 & \text{if } p \neq 2
\end{cases}.$$ 

From writing code in C and considering Wilson’s theorem in 2, 3, 4, and 5 dimensions I conjecture that $|S(G_{N-1})|$ is related to the residue class in $\mathbb{Z}_N$ to which $p$ belongs.

4.5.4 Matrices In a Quotient Ring

In finding the inverse of the polynomial $\alpha = a_0 + a_1 \rho + \ldots + a_{N-2} \rho^{N-2}$ we are required to find a polynomial $\beta = b_0 + b_1 \rho + \ldots + b_{N-2} \rho^{N-2}$ such that $\alpha \beta = 1$. Now, using the facts that $\rho^N = 1$ and $1 + \rho + \ldots + \rho^{N-1} = 0$, we can write $\alpha \beta = c_0 + c_1 \rho + \ldots + c_{N-2} \rho^{N-2}$ where $c_i$’s are integers that depend on the $a_i$’s and the $b_i$’s. Thus, from $\alpha \beta = 1$, we can have the following system of $N-1$ linear equations in the $N-1$ unknowns $b_0, b_1, \ldots, b_{N-2}$: $c_0 = 1$, $c_1 = 0$, ..., $c_{N-2} = 0$. This system can be written in terms of matrices as follows, by letting $M_{N-1}(a_0, a_1, \ldots, a_{N-2})$ denote the $N-1$ by $N-1$ coefficient matrix of:

$$M_{N-1}(a_0, a_1, \ldots, a_{N-2}) \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{N-2} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$ 

Thus, the problem of finding the inverse of the polynomial $\alpha$, has now become the problem of finding the inverse of the matrix $M_{N-1}(a_0, a_1, \ldots, a_{N-2})$ that clearly depends on the coefficients of $\alpha$. The function which maps $\alpha$ to $M_{N-1}(a_0, a_1, \ldots, a_{N-2})$ can be shown to preserve addition and multiplication. Thus, it is a ring isomorphism. Now because this function preserves multiplication, multiplying $\alpha = a_0 + a_1 \rho + \ldots + a_{N-2} \rho^{N-2}$ by $\beta = b_0 + b_1 \rho + \ldots + b_{N-2} \rho^{N-2}$ is the same as multiplying $M_{N-1}(a_0, a_1, \ldots, a_{N-2})$ by $\begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{N-2} \end{bmatrix}$. Thus, if we let $b_0 = 1$, $b_1 = 0$, ...
\[ b_{N-2} = 0 \text{ so } \beta = 1 = 1 + 0\rho + \ldots + 0\rho^{N-2} \text{ then the product } (a_0 + a_1\rho + \ldots + a_{N-2}\rho^{N-2})(1) \text{ is} \]

essentially the same as the product \( M_{N-1}(a_0, a_1, \ldots, a_{N-2}) \). Therefore, the first column \[ \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{N-2} \end{bmatrix} \]

of \( M_{N-1}(a_0, a_1, \ldots, a_{N-2}) \) is equal to \[ \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \]. Now, let \( b_1 = 1 \) let all other \( b_i \)'s be 0. Thus, \[ \beta = \rho = 0 + 1\rho^1 + \ldots + 0\rho^{N-2} \text{. Thus, the product } (a_0 + a_1\rho + \ldots + a_{N-2}\rho^{N-2})(\rho) \text{ is} \]

essentially the same as the product \( M_{N-1}(a_0, a_1, \ldots, a_{N-2}) \). We now use the facts that \( \rho^N = 1 \) and \[ 1 + \rho + \ldots + \rho^{N-1} = 0 \text{ to write } (a_0 + a_1\rho + \ldots + a_{N-2}\rho^{N-2})(\rho) = a_0\rho + a_1\rho^2 + \ldots + a_{N-2}\rho^{N-1} \text{ in} \]

the form \[ \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix} \]. We now have that \[ d_0 + d_1\rho + \ldots + d_{N-2}\rho^{N-2} \text{ is} \]

essentially the same as \( M_{N-1}(a_0, a_1, \ldots, a_{N-2}) \). Thus, the second column of \( M_{N-1}(a_0, a_1, \ldots, a_{N-2}) \)

\[ \begin{bmatrix} d_0 \\ d_1 \\ \vdots \\ d_{N-2} \end{bmatrix} \]. In general, to find the \( k \)th column of \( M_{N-1}(a_0, a_1, \ldots, a_{N-2}) \) we use the facts that \[ \rho^N = 1 \text{ and } 1 + \rho + \ldots + \rho^{N-1} = 0 \text{ to write } (a_0 + a_1\rho + \ldots + a_{N-2}\rho^{N-2})(\rho^{k-1}) \text{ in the form} \]

\[ d_0 + d_1\rho + \ldots + d_{N-2}\rho^{N-2} \text{. It now follows from considering the action of multiplying } \alpha \text{ by} \]

\[ \rho^{k-1} \text{ that the } k \text{th column of } M_{N-1}(a_0, a_1, \ldots, a_{N-2}) \text{ is} \]

\[ \begin{bmatrix} d_0 \\ d_1 \\ \vdots \\ d_{N-2} \end{bmatrix} \]. As a result of this isomorphism between polynomials and matrices, we obtain the following result by replacing polynomials by their corresponding matrices:

The corresponding result for matrices is:

**Theorem 4.5.4.** If \( p \) is an odd prime and \( N > 2 \) is an even natural number, then:
Here $M_{N-1}(i_0, i_1, ..., i_{N-2})$ is the matrix that is isomorphic to the polynomial $\sum_{j=0}^{N-2} i_j \rho^j$ in $Z[\rho]/ < 1 + \rho + \rho^2 + ... + \rho^{N-1} >$ and $I_{N-1 \times N-1}$ is the $N-1 \times N-1$ identity matrix.

As usual, we define:

$$(M_{N-1}(i_0, i_1, ..., i_{N-2}))^* = M_{N-1}(i_0, i_1, ..., i_{N-2}) \text{ if } (i_0 + i_1 \rho + ... + i_{N-2} \rho^{N-2})^* = (i_0 + i_1 \rho + ... + i_{N-2} \rho^{N-2})$$

and

$$(M_{N-1}(i_0, i_1, ..., i_{N-2}))^* = I_{N-1 \times N-1} \text{ if } (i_0 + i_1 \rho + ... + i_{N-2} \rho^{N-2})^* = 1.$$ 

Where $(i_0 + i_1 \rho + ... + i_{N-2} \rho^{N-2})^*$ has been defined previously.

As before, we now take determinants of the previous result to give the following:

**Theorem 4.5.5.** If $p$ is an odd prime and $N > 2$ is an even natural number, then:

$$\prod_{i_0=0}^{p-1} \prod_{i_1=0}^{p-1} ... \prod_{i_{N-2}=0}^{p-1} \det((M_{N-1}(i_0, i_1, ..., i_{N-2}))^*) \equiv 1 \pmod{p}.$$ 

### 4.5.5 A Conjecture For The Order of The Group $G_{N-1}$

We now let $|G_{N-1}|$ denote the order of the group $G_{N-1}$. The order of the general linear group of invertible $N-1$ by $N-1$ matrices with entries in $Z_p$, denoted by $GL_{N-1}(Z_p)$, has order given by:

$$|GL_{N-1}(Z_p)| = \prod_{j=0}^{N-2} (p^{N-1} - p^j).$$ 

Now the order of a subgroup divides the order of the group. Thus, $|G_{N-1}|$ divides $\prod_{j=0}^{N-2} (p^{N-1} - p^j)$.

From numerical evidence that I have collected from the groups $G_2$, $G_3$, $G_4$ and $G_5$ (i.e. writing code in C, considering the first 25 primes, and constructing tables) I have arrived at the following two conjectures:

**Conjecture 4.5.1.** The order of the group $G_{N-1}$ is related to the residue class in $Z_N$ to which $p$ belongs.

and
Conjecture 4.5.2. The order of the group $G_{N-1}$ is equal to a monic polynomial of degree $N - 1$ in $Z[p]$.

In other words, $\frac{|G_{N-1}|}{p^{N-1}} \to 1$ as $p \to \infty$.

From this, it follows that the number of noninvertible elements in $\{i_0 + i_1\rho + ... + i_{N-2}\rho^{N-2} \mid 0 \leq i_0, i_1, ..., i_{N-2} \leq p - 1\}$ is $o(p^{N-1})$. 
Chapter 5

Conclusion

In conclusion, Wilson’s theorem (Theorem 2.1.1) and Fermat’s little theorem (Theorem 2.3.1) are among the most important results in the theory of numbers and the theory of groups. Both of these apply to the multiplicative group $\mathbb{Z}_p^*$. Both can easily be generalized to apply to any finite abelian group $G$. Thus, Theorems 2.1.1 and 2.3.1 are special cases of Theorems 2.2.2 and 2.3.19. In this thesis, we have considered groups of invertible polynomials in certain quotient rings. For each of these groups, we have either derived, or made a conjecture for, the order of the group and the number of self-invertible elements in the group. These derivations and conjectures use the number theoretic notions of quadratic residues and primes in residue classes. These notions are closely related to binary quadratic forms and sums of squares. Having the order of the group gives us, by Theorem 2.3.19, a Fermat-like result for the group. Having the number of self-invertible elements gives us, by Theorem 2.2.2, a Wilson-like result for the group.
Bibliography


