SHEPHERD, RICK L., M.A. Binary Quadratic Forms and Genus Theory. (2013)
Directed by Dr. Brett Tangedal. 191 pp.

The study of binary quadratic forms arose as a natural generalization of questions about the integers posed by the ancient Greeks. A major milestone of understanding occurred with the publication of Gauss's *Disquisitiones Arithmeticae* in 1801 in which Gauss systematically treated known results of his predecessors and vastly increased knowledge of this part of number theory. In effect, he showed how collections of sets of binary quadratic forms can be viewed as groups, at a time before group theory formally existed. Beyond that, he even defined and calculated genus groups, which are essentially quotient groups, that explain which congruence classes of numbers can be represented by given sets of forms. This thesis examines Gauss's main results as interpreted and refined over two centuries. Also, code has been created to implement many of the algorithms used in studying the relationships of such forms to each other, to generate examples, and to provide a small toolkit of software for analyzing the corresponding algebraic structures.

BINARY QUADRATIC FORMS AND GENUS THEORY

by

Rick L. Shepherd

A Thesis Submitted to
the Faculty of the Graduate School at
The University of North Carolina at Greensboro
in Partial Fulfillment
of the Requirements for the Degree
Master of Arts

Greensboro
2013

Approved by

Committee Chair

APPROVAL PAGE

This thesis has been approved by the following committee of the Faculty of The Graduate School at The University of North Carolina at Greensboro.

Committee Chair ________________________________
Brett Tangedal

Committee Members ________________________________
Sebastian Pauli

____
Dan Yasaki

____
Date of Acceptance by Committee

____
Date of Final Oral Examination

ACKNOWLEDGMENTS

The author would like to acknowledge and thank Dr. Tangedal, Dr. Pauli, and Dr. Yasaki for their number-theory-related classes and talks, personal communications, guidance, pointers, LaTeX expertise — and patience — especially as the scope and timing of this thesis changed. Appreciation is also directed toward the staff of the Jackson Library, who were always very helpful and prompt in fulfilling interlibrary loan requests.

PREFACE

This topic is motivated by interest in representations of integers, particularly primes, that increased in general from independent study of On-Line Encyclopedia of Integer Sequences (OEIS) entries. UNCG course MAT 742, Algebraic Number Theory, which focused on quadratic number fields, further encouraged this interest.

TABLE OF CONTENTS

LIST OF TABLES

Page

CHAPTER I

INTRODUCTION

1.1 Preliminary Terminology, Notation, and Foundational Results

Because there are many instances in Number Theory where definitions and notation vary depending upon the author (albeit often only subtly), we begin with a few basics for clarity. By *natural numbers* we mean here the whole numbers beginning with **one — not zero**, namely, $1, 2, 3, 4, ...$, which we denote by $\mathbb{N}$. The *integers* include precisely the natural numbers, the negatives of the natural numbers, and zero, and this set is denoted by $\mathbb{Z}$. Thus the terms "natural numbers" and "positive integers" (denoted by $\mathbb{Z}^+$) may be used interchangeably below. Lower case Latin letters will almost always represent integers or generic elements in a group. Bold upper case Latin letters will represent matrices. We assume familiarity with the rational, real, and complex numbers, which are denoted by $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$, respectively. Greek letters are usually used to represent functions.

Our interest and focus is on integers, though, and central to that is the notion of "divisibility." We say an integer $a \neq 0$ *divides* an integer b (or that a is a *divisor* or *factor* of b) if there exists an integer c such that $b = ca$. We denote this by $a \mid b$. For example, $6 \mid 12$ since $12 = 2 \cdot 6$. However, 7 does not divide 10 and we use the notation $7 \nmid 10$ to denote this. Related to the concept of divisors there is of course the *greatest common divisor.*

Definition 1.1.1. *Assume $a, b, c \in \mathbb{Z}$ with $a \neq 0$. The largest positive integer d that divides both a and b is called the greatest common divisor* (*or* gcd) *of a and b, denoted* *by* $d = \gcd(a,b)$*. Similarly, the largest positive integer* e *that simultaneously divides* a*,* b*, and* c *is called the* gcd *of* a*,* b*, and* c*, and is denoted by* $e = \gcd(a,b,c)$*.*

Definition 1.1.2. *If* $a, b \in \mathbb{Z}$ *with* $a \neq 0$*, then we say that* a *and* b *are relatively prime if* $\gcd(a,b) = 1$*.*

A basic theorem we will often use without further comment is

Theorem 1.1.3. *Assume* $a, b, c \in \mathbb{Z}$ *with* $a \neq 0$*. We have* $\gcd(a,b) = 1$ *if and only if there exist integers* s *and* t *such that* $as + bt = 1$*. Similarly, we have* $\gcd(a,b,c) = 1$ *if and only if there exist integers* s, t *and* u *such that* $as + bt + cu = 1$*. Also, if* $a \mid bc$ *and* $\gcd(a,b) = 1$*, then* $a \mid c$*. Finally,* $\gcd(a_1a_2, b) = 1$ *if* $\gcd(a_1, b) = 1$ *and* $\gcd(a_2, b) = 1$*.*

Prime numbers are especially important integers. Recall that a *prime number* is a natural number $p > 1$ whose only positive integer factors are 1 and p itself. The list of prime numbers (or just *primes*) begins as $2, 3, 5, 7, 11, 13, 17, \ldots$. A classic proof dating back to antiquity demonstrates that the list of primes is infinitely long. Composite numbers, on the other hand, are natural numbers greater than 1 that are not prime, namely, they can be expressed as the product of two integer factors with each factor ≥ 2. A defining property of prime numbers is

Theorem 1.1.4. *If* p *is a prime and* $a \in \mathbb{Z}$*, then* $p \nmid a$ *if and only if* $\gcd(p,a) = 1$*.*

This property does not hold for a composite number n because if $n = ab$, with $1 < a, b < n$, then $n \nmid a$ and yet $\gcd(n,a) = a \neq 1$. Another defining property for primes is

Theorem 1.1.5. *If* p *is a prime and* $p \mid ab$*, then* $p \mid a$ *or* $p \mid b$*.*

To see that this does not hold for composite numbers, note that $6 \mid (2 \cdot 3)$ and yet $6 \nmid 2$ and $6 \nmid 3$. Theorem 1.1.5 is the main ingredient needed to prove the

Fundamental Theorem of Arithmetic (or FTA): *Every positive integer greater than one can be written uniquely as a product of primes, with the prime factors in the product written in order of nondecreasing size.*

The first explicit statement and proof of this Theorem was given by Gauss in 1801 in his *Disquisitiones Arithmeticae* [Ga]. It should be noted, however, that the FTA was known and used from antiquity onward. The subject of "Elementary Number Theory" (we will usually just say more briefly "Number Theory") begins with the FTA and explores all of its many ramifications. Gauss preferred "The Higher Arithmetic" to "Elementary Number Theory" and indeed his Latin title *Disquisitiones Arithmeticae* translates to "Arithmetical Investigations." A crucial tool introduced by Gauss in his book was the notion of "congruence" with respect to a given modulus m.

Definition 1.1.6. *If $a, b, m \in \mathbb{Z}$ and $m \geq 2$, we say that "a is congruent to b modulo m" if $m \mid (b - a)$. This relation is written $a \equiv b \pmod{m}$.*

For instance, $16 \equiv 5 \pmod{11}$ since $11 \mid (16 - 5)$. However, $17 \not\equiv 2 \pmod{11}$ since $11 \nmid (17 - 2)$. The most basic properties of congruences are the following.

Theorem 1.1.7. *If $a, b, c, m \in \mathbb{Z}$ with $m \geq 2$, then*

(i) $a \equiv a \pmod{m}$;

(ii) *if* $a \equiv b \pmod{m}$, *then* $b \equiv a \pmod{m}$*; and*

(iii) *if* $a \equiv b \pmod{m}$ *and* $b \equiv c \pmod{m}$, *then* $a \equiv c \pmod{m}$.

There are many other important properties, for example, if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$. We refer to [Da] for a full list of other such properties which will be used repeatedly and often without further reference throughout this thesis. Theorem 1.1.7 shows that "congruence modulo m" (m fixed with $m \geq 2$) gives an "equivalence relation on $\mathbb{Z}$." The notion of an equivalence relation being defined on any given set is elaborated upon more fully in Section 2.2, but the key feature we wish to stress here is that congruence modulo m partitions $\mathbb{Z}$ into exactly m distinct "congruence classes." The class of 0 modulo m is denoted by $\overline{0}$ and consists of all integers congruent to 0 modulo m. Indeed, $\overline{0} = \{\dots, -2m, -m, 0, m, 2m, \dots\}$. Similarly, $\overline{1} = \{\dots, 1-2m, 1-m, 1, 1+m, 1+2m, \dots\}$. Congruence classes with respect to a fixed modulus may be added and multiplied together in a consistent way. For example, if $m = 6$, then $\overline{2} + \overline{8} = \overline{4}$. With respect to the operation of addition, the congruence classes modulo m form an "abelian group" of order m which we denote by $\mathbb{Z}_m$, where by definition, $\mathbb{Z}_m := \{\overline{0}, \overline{1}, \dots, \overline{m-1}\}$. Group Theory is a vast subject (see [DF] as a standard reference), but most of the groups encountered in this thesis are "commutative" or "abelian."

Definition 1.1.8. *An abelian group is a set G with a binary operation $\star$ defined on G such that G is closed under the operation, and such that*

(i) $a \star b = b \star a$, *for all* $a, b \in G$, *i.e.,* $\star$ *is commutative;*

(ii) $(a \star b) \star c = a \star (b \star c)$, *for all* $a, b, c \in G$, *i.e.,* $\star$ *is associative;*

(iii) *there exists an element e in G, called the identity of G, such that for all $a \in G$ we have $e \star a = a$;*

(iv) *for each $a \in G$ there is an element a^{-1} of G, called the inverse of a, such that $a \star a^{-1} = e$.*

With regard to the group $G = \mathbb{Z}_m$ introduced above, and with respect to the operation of addition, the identity element is $\overline{0}$ and the additive inverse of $\overline{a}$ is $\overline{-a}$. The group

$\mathbb{Z}_m$ has the additional property of being "cyclic" since it is generated by $\overline{1}$. A group is "finite" or "infinite" according to whether it contains a finite or an infinite number of elements. The integers $\mathbb{Z}$ form an infinite abelian group under addition. If G is a finite group, we denote the number of elements in G, known as the "order" of G, by $|G|$. As noted above, $|\mathbb{Z}_m| = m$. The congruence classes modulo m do not form a group under multiplication but we do obtain a group if we restrict ourselves to working with the "reduced residue classes modulo m." If $\gcd(a, m) = 1$, then we call $\overline{a} \in \mathbb{Z}_m$ a reduced residue class modulo m. It is important to note that if a single integer in a given congruence class modulo m is relatively prime to m, then every integer in this class is relatively prime to m. More generally, we have

Theorem 1.1.9. *If $m \geq 2$ is a fixed modulus and $a \equiv b \pmod{m}$, then* $\gcd(a, m) = \gcd(b, m)$.

The following finite abelian group will figure prominently in Chapter IV.

Definition 1.1.10. *Given a fixed modulus $m \geq 2$, the multiplicative abelian group of reduced residue classes modulo m is denoted by U_m.*

For example, $U_6 = \{\overline{1}, \overline{5}\}$. The identity element e in this group is $\overline{1}$. The only difficulty in establishing that U_m forms a group under multiplication is axiom (iv) in Definition 1.1.8 and this follows readily from Theorem 1.1.3. An important arithmetic function (i.e., a function whose domain is $\mathbb{N}$) directly connected with the order of U_m is the Euler φ-function. This function is defined as follows: $\varphi(1) = 1$, and $\varphi(m) = |U_m|$ for each $m \geq 2$. An alternate definition when $m \geq 2$ is that $\varphi(m)$ is equal to the number of integers n in the range $1 \leq n \leq m - 1$ such that $\gcd(n, m) = 1$. For example, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, and $\varphi(6) = 2$ (as noted above).

It follows from Theorem 1.1.4 that $\varphi(p) = p - 1$ when p is a prime number. We will return to the more general theory of finite abelian groups in Section 2.6 and will discuss the Fundamental Theorem of this subject in great detail there because of its importance to this thesis.

A classic result which will be used more than once in this thesis is the **Chinese Remainder Theorem (or CRT):** *If $m_1, m_2 \in \mathbb{Z}^{\geq 2}$ are fixed moduli such that $\gcd(m_1, m_2) = 1$ and a_1, a_2 are arbitrarily fixed integers, then there exist integers x that simultaneously solve the two congreunces $x \equiv a_1 \pmod{m_1}$ and $x \equiv a_2 \pmod{m_2}$, and the set of all such simultaneous solutions consists precisely of all integers in a fixed congruence class defined modulo $m_1 \cdot m_2$.*

More generally, let $r \geq 3$, and assume every pair from among the numbers $m_1, m_2, \ldots, m_r \in \mathbb{Z}^{\geq 2}$ is relatively prime. If $a_1, a_2, \ldots, a_r$ are arbitrarily fixed integers, then there exist integers x that simultaneously solve the system of congruences $x \equiv a_j \pmod{m_j}$, $j = 1, 2, \ldots, r$, and the set of all such simultaneous solutions consists precisely of all integers in a fixed congruence class defined modulo $m_1 \cdot m_2 \cdots m_r$.

One of the most famous theorems proved in the *Disquisitiones Arithmeticae* [Ga] is the Quadratic Reciprocity Law (Gauss referred to it in his private papers as the *Theorema Aureum* or the "golden theorem"). Because of the importance of this Law to our subject, we give a careful statement of it here and refer the reader to the book by Landau [La] for its proof.

Definition 1.1.11. *Given a fixed modulus $m \geq 2$ and an integer r such that $\gcd(r, m) = 1$, we say that r is a "quadratic residue modulo m" if there exists an integer x such that $x^2 \equiv r \pmod{m}$. If no such x exists, we say that r is a "quadratic nonresidue modulo m."*

Working within the group U_m, the question of whether r is a quadratic residue modulo m or not is equivalent to asking if there is a class $\overline{x} \in U_m$ such that $\overline{x}^2 = \overline{r}$. Since U_m is a finite group, this boils down to a finite check. Note, for example, that 5 is not a quadratic residue modulo 6 since $\overline{1}^2 = \overline{5}^2 = \overline{1}$ in U_6. Definition 1.1.11 is of particular interest when $m = p$ is an *odd* prime. In this case, we use a special and very well-chosen notation introduced by Legendre.

Definition 1.1.12. *If p is an odd prime number and a is an integer not divisible by p, the "Legendre symbol," denoted by $(\frac{a}{p})$, is defined to have the value $+1$ if a is a quadratic residue $\pmod p$, and -1 if a is a quadratic nonresidue $\pmod p$.*

For example, if $p = 5$, then $(\frac{2}{5}) = -1$, whereas $(\frac{4}{5}) = 1$.

The most easily derived properties of the Legendre symbol are given in the following theorem.

Theorem 1.1.13. *Let p be an odd prime and assume a and b are integers that are relatively prime to p.*

(i) *If $a \equiv b \pmod p$, then $(\frac{a}{p}) = (\frac{b}{p})$.*

(ii) *Euler's criterion: $a^{(p-1)/2} \equiv (\frac{a}{p}) \pmod p$.*

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

(iv) *Of the integers in the set $\{1, 2, \ldots, p-1\}$, exactly $(p-1)/2$ are quadratic residues $\pmod p$ and the remaining $(p-1)/2$ are quadratic nonresidues (this implies there is at least one integer in this set that is a quadratic residue $\pmod p$ and at least one such integer that is a nonresidue $\pmod p$).*

The Quadratic Reciprocity Law is a three-part statement which is most conveniently stated in terms of the Legendre symbol. Before stating this Law, we note that every odd prime is congruent to either 1 or 3 modulo 4.

Quadratic Reciprocity Law (or QRL): *Assume p and q are odd primes with $p \neq q$.*

(i) $(\frac{-1}{p}) = 1$ *if* $p \equiv 1 \pmod 4$ *and is equal to* -1 *if* $p \equiv 3 \pmod 4$.

(ii) $(\frac{2}{p}) = 1$ *if* $p \equiv 1$ *or* $7 \pmod 8$ *and is equal to* -1 *if* $p \equiv 3$ *or* $5 \pmod 8$.

(iii) $(\frac{p}{q}) = (\frac{q}{p})$, *unless* $p \equiv q \equiv 3 \pmod 4$, *in which case* $(\frac{p}{q}) = -(\frac{q}{p})$.

Part (i) of the QRL may be stated more concisely as $(\frac{-1}{p}) = (-1)^{(p-1)/2}$ and is often referred to as the First Supplement of the QRL or simply as the "first supplement." Part (ii) of the QRL may be stated more concisely as $(\frac{2}{p}) = (-1)^{(p^2-1)/8}$ and is often referred to as the Second Supplement of the QRL or simply as the "second supplement." The deepest part of the QRL is part (iii) and it may be written more concisely as $(\frac{p}{q})(\frac{q}{p}) = (-1)^{[(p-1)(q-1)]/4}$. Part (iii) is what gives this Law its name.

Another useful symbol that will be used extensively in Chapter IV of this thesis is the "Jacobi symbol." Assume throughout that $m \in \mathbb{N}$ is odd and that $a \in \mathbb{Z}$ is such that $\gcd(a, m) = 1$. If the prime factorization of $m > 1$ according to the FTA is given by $\prod_{i=1}^{t} p_i^{e^i}$, then the *Jacobi symbol*, denoted by $(\frac{a}{m})$, is defined as the product of Legendre symbols: $(\frac{a}{m}) = \prod_{i=1}^{t} (\frac{a}{p_i})^{e_i}$. We set $(\frac{a}{1})$ equal to 1 for all nonzero integers a. For example, the Jacobi symbol $(\frac{2}{75})$ is equal to -1 because $75 = 3 \cdot 5^2$ and $(\frac{2}{3}) \cdot (\frac{2}{5})^2 = (-1) \cdot (-1)^2 = -1$. Note that the Legendre and Jacobi symbols are equivalent when m is an odd prime. We will say much more about the Jacobi symbol in Chapter IV and will find that almost every result stated above with respect to the Legendre symbol holds as well with respect to this new "composite" symbol. There is one important caveat: It is possible for a Jacobi symbol $(\frac{a}{m})$ to be equal to one without a being a quadratic residue modulo m. For example, $(\frac{2}{15}) = (\frac{2}{3})(\frac{2}{5}) = (-1)(-1) = 1$, and yet 2 is not a quadratic residue modulo 15.

1.2 Overview

A binary quadratic form as discussed here is a degree two polynomial expression $ax^2+bxy+cy^2$, denoted by (a, b, c), where the coefficients a, b, and c are fixed integers and the variables x and y are restricted to integers. Binary quadratic forms are an enticing topic of study as one way of representing given integers. Computational examples will be provided not only to demonstrate established results during this summary of the theory but also to provide new, useful reference tables and sequences mentioned here (in Appendix B) and included in the On-Line Encyclopedia of Integer Sequences (OEIS).

While covering binary quadratic forms, we implement some of the most important algorithms in accompanying code. The code is written in PARI/GP (often abbreviated simply as "PARI"), a programming and scripting language and computer algebra system originally developed by Henri Cohen and his colleagues at the Université Bordeaux I, France, and currently available for free download from http://pari.math.u-bordeaux.fr/. Most of the software included with this thesis enables us to find and generate good examples much more easily. Beyond that, the code — although unlikely to be original because of the age of these algorithms — allows us to explore many more forms and other algebraic objects constructed from them than we reasonably could if all our calculations were manual. As these procedures provide several simple but useful tools for beginning serious further investigations of these objects, they are included in Appendix A, sometimes with sample output in Appendix B. Note that in some cases there are built-in PARI data types and commands that may perform some of these functions more efficiently but not as transparently as the code in Appendix A.

In this Section, we first give the main topics of this thesis some historical context. The ancient Greeks posed many number theoretical questions including seeking the solutions to what are now known as "Diophantine equations." Such equations are named after Diophantus of Alexandria of the 3rd century A.D. (whose years of birth and death are much-debated). Although Diophantus himself actually permitted positive rational solutions to his equations, the term "Diophantine equation" refers generally to equations where only integer solutions are desired. Every math student who has ever contemplated the Pythagorean Theorem while confining the solutions to integers has certainly dealt with the Diophantine equation $x^2 + y^2 = z^2$ to find "Pythagorean triples" of integers (x, y, z) such as $(3, 4, 5)$ and $(5, 12, 13)$. Another famous Diophantine equation is $n = x^2 + y^2$ (i.e., writing a positive integer as a sum of two squares), the solutions to which are discussed in detail in Section 1.3. Yet another famous example is "Pell's equation," which is discussed in Section 2.7. Pell's equation has different variants, but the version studied here is $x^2 - dy^2 = 4$, where d is a fixed constant of a special type (a so-called "fundamental discriminant"). Solutions to Pell's equation are important to the theory of binary quadratic forms for determining which "transformations" of a form actually take the form back to itself.

The great Number Theorists who have contributed most directly to the development of the classical theory of binary quadratic forms and Genus Theory are Fermat, Euler, Lagrange, Legendre, and Gauss. Pierre de Fermat (1601-1665) stated several theorems giving results for Diophantine equations similar to $n = x^2+y^2$. For example, these three theorems of Fermat assume p is an odd prime:

$$p = x^2 + y^2 \text{ has solutions } x, y \in \mathbb{Z} \text{ if and only if } \ p \equiv 1 \pmod 4, \tag{1.2.1}$$

$$p = x^2 + 2y^2 \text{ has solutions } x, y \in \mathbb{Z} \text{ if and only if } \ p \equiv 1 \text{ or } 3 \pmod 8, \tag{1.2.2}$$

$$p = x^2 + 3y^2 \text{ has solutions } x, y \in \mathbb{Z} \text{ if and only if } \ p = 3 \text{ or } p \equiv 1 \pmod 3. \tag{1.2.3}$$

The first theorem above will be proved in Section 1.3 and again in Section 4.2. We will also address Fermat's second theorem in Section 4.2. Leonhard Euler (1707-1783), in addition to discovering the important Quadratic Reciprocity Law discussed in Section 1.1, proved Fermat's statements above and made several similar conjectures, for example, for p an odd prime not equal to 5:

$$p = x^2 + 5y^2 \text{ has solutions } x, y \in \mathbb{Z} \text{ if and only if } \ p \equiv 1 \text{ or } 9 \pmod{20}, \tag{1.2.4}$$

which is provable using the methods of Genus Theory, as we will see in Section 4.2. All of these theorems due to Fermat and Euler address the same question: Which prime numbers may be represented when integer values for x and y are plugged into specific binary quadratic forms? This simple-minded question leads one directly into surprisingly deep mathematical waters, whose currents still influence modern research in Number Theory! Euler made other even deeper conjectures, for example, an odd prime p is representable by the form $x^2 + 27y^2$ if and only if $p \equiv 1 \pmod 3$ and 2 is a cubic residue modulo p, and p is representable by the form $x^2 + 64y^2$ if and only if $p \equiv 1 \pmod 4$ and 2 is a biquadratic residue modulo p. The appearance of higher degree residues already begins to show the depth and subtlety of this subject. Although the discussion of higher degree residues is beyond the scope of this thesis, it is noteworthy that Genus Theory can prove something similar to the above, namely, an odd prime p can be represented by either x^2+27y^2 or $4x^2+2xy+7y^2$ if and only if $p \equiv 1 \pmod 3$. Genus Theory, the main topic of this thesis, involves the classification of binary quadratic forms according to which congruence classes of integers they represent with respect to a specific modulus. This theory allows us to decide on whether certain second degree Diophantine equations have solutions or not and is especially powerful when it comes to ruling out solutions in particular instances. The main weakness of this theory is illustrated in the last theorem just quoted: We might know that one of two or more binary quadratic forms represents a particular integer but we do not know which one. Genus Theory is sometimes too "coarse" to distinguish among several possibilities.

Joseph-Louis Lagrange (1736-1813) developed a theory of "reduction" of forms (see Sections 2.3 and 2.5) that is crucial in determining when two distinct binary quadratic forms represent exactly the same integers. Lagrange also showed how to "multiply" binary quadratic forms in a way that is consistent with the multiplication of ordinary integers (see Theorem 3.1.6). This binary operation on forms, known more formally as "composition" (a full development is given in Chapter III), weaves its way throughout this subject, in intimate interaction with Genus Theory. Adrien-Marie Legendre (1752-1833) refined, clarified, and further developed the best ideas of Fermat, Euler, and Lagrange. Legendre published the first full-length book on Number Theory in 1798 (we already saw his name appear in Section 1.1), which inspired much further research in the 19th century.

Carl Friedrich Gauss (1777-1855), in a classical mathematical masterpiece [Ga] published in 1801 at the age of 24, synthesized the known theory concerning binary quadratic forms; gave it a much more complete, explicit, theoretical underpinning; refined Lagrange and Legendre's ideas of composition; and exhibited some of the first examples of groups and quotient groups while fully developing and demonstrating the power of Genus Theory. Gauss was also the first person to give a rigorous proof of the Quadratic Reciprocity Law; Euler, and especially Legendre, had attempted to prove this Law but had only partial success. The importance of the QRL will become fully apparent throughout Chapter IV and especially in Section 4.1. An exposition of much of Gauss's work, as summarized largely by [Fl], but with many details filled in here, constitutes the bulk of this thesis.

1.3 Sums of Two Squares

To gain an appreciation for the type of problem the theory of binary quadratic forms addresses and for the beautiful answers this theory provides, we first consider the history of a single specific classical question: What natural numbers n can be expressed as $n = x^2 + y^2$, where x and y are integers? A concise description of the answer's development can be found in Chapter V of Davenport's book [Da]. He says that the *Arithmetic* of Diophantus (circa 250 A.D.) contains some statements related to the answer, although they are inconclusive. The correct answer "was first given by the Dutch mathematician Albert Girard in 1625, and again by Fermat a little later." Davenport goes on to state that Fermat probably "had proofs of his results, but the first proofs we know of are those published by Euler in 1749."

Since an even square $(2k)^2 = 4k^2$ is congruent to 0 (mod 4) and an odd square $(2k+1)^2 = 4k^2 + 4k + 1$ is congruent to 1 (mod 4), no natural number of the form $n = 4k + 3$ can be the sum of two squares. This is clear because the sum of two even squares is congruent to 0 (mod 4), the sum of two odd squares is congruent to 2 (mod 4), and the only other possibility, the sum of an odd and an even square, is congruent to 1 (mod 4). Thus, we know right away that $3, 7, 11, 15, 19, 23, 27, \ldots$ can not be expressed as a sum of two squares.

The above small result can be strengthened. Suppose the number n has a **prime factor** q of the form $4k + 3$. Then $x^2 + y^2 = n$ implies $x^2 \equiv -y^2 \pmod{q}$. By the First Supplement of the QRL, -1 is not a quadratic residue modulo q. If $q \nmid y$, there exists an integer z such that $zy \equiv 1 \pmod{q}$ by Theorem 1.1.3. Multiplying both sides of the congruence $x^2 \equiv -y^2 \pmod{q}$ by z^2 gives $(xz)^2 \equiv -1 \pmod{q}$, which implies that -1 is a quadratic residue (mod q) in contradiction to the first supplement. We conclude that $q \mid y$ and therefore also $q \mid x$, which implies in turn that $q^2 \mid n$. Dividing the equation $x^2 + y^2 = n$ by q^2, and letting $n = q^2 n_1$, then if n_1 itself is divisible by q, the same argument can be repeated with the new equation to find n_1 is also divisible by q^2. Eventually, after a finite number of repetitions, this argument gives the exact power of q that divides n — and that power must be even. Thus the prime factorization of any number n that can be expressed as the sum of two squares contains only **even** powers of its prime factors of the form $4k + 3$. This shows that $3, 6, 7, 11, 12, 14, 15, 19, 21, 22, 23, 24, 27, \ldots$ can not be expressed as a sum of two squares. This list includes the list we already made above since a number of the form $4k + 3$ must contain at least one prime factor of that same form to an **odd** power.

We have by now compiled a long list of natural numbers that can **not** be represented as a sum of two squares. Can this process of elimination be carried any further? The answer is "No!," namely, every natural number not on the (infinite) list just above **can** be expressed as a sum of two squares. This is the content of the main theorem of this section.

Theorem 1.3.1. *A natural number n may be written in the form x^2+y^2, $x, y \in \mathbb{Z}$, if and only if every prime number of the form $4k+3$ appearing in the prime factorization of n appears to an even power.*

Proof: We already proved the "only if" direction above. The hard part is the other direction, namely, if every prime number of the form $4k+3$ appearing in the prime factorization of n appears to an even power, then n can be written as a sum of two squares. Proving this harder direction requires an identity "generally attributed to Leonardo of Pisa (also called Fibonacci), who gave it in his *Liber Abaci* of 1202" ([Da], p. 116):

$$(a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2 \tag{1.3.1}$$

Observe that the identity expresses the product of two sums of two squares as the sum of two squares.

If a natural number $n > 1$ satisfies the criterion in Theorem 1.3.1, n is a product of factors (repetition is allowed), each of which is either 2, a prime of the form $4k+1$, or the **square** of a prime of the form $4k+3$. Once we have shown that each such type of factor is itself expressible as the sum of two squares, then repeated application of equation (1.3.1) demonstrates that n itself is so representable. Certainly $2 = 1^2 + 1^2$

is not a problem. If q is a prime of the form $4k+3$, then $q^2 = q^2 + 0^2$, which takes care of the third type of factor. It remains to show that any prime of the form $4k+1$ is representable as $x^2 + y^2$, and this is where the real crux of the whole matter lies.

The classical proof that any prime p of the form $4k+1$ is representable as a sum of two squares is essentially due to Euler. The first part of the proof shows that some multiple of p is representable as z^2+1; the second part deduces from this first representation that p itself has a representation as x^2+y^2.

The first part is equivalent to proving that given any prime p of the form $4k+1$, there exists an integer z such that $z^2 + 1 \equiv 0 \pmod{p}$. From the first supplement, we know there is such a solution (mod p) and the integer z may be chosen in the range $1 \leq z \leq p-1$. It is actually more convenient to choose z instead in the range $-(p-1)/2 \leq z \leq (p-1)/2$, which may be done since we are working modulo p (of course, $z \neq 0$). We conclude that there exists a natural number m such that $mp = z^2 + 1$, and with

$$m = \frac{1}{p}(z^2+1) < \frac{1}{p}\left(\frac{p^2}{4}+1\right) < p.$$

Hence there exist integers x and y with

$$mp = x^2 + y^2, \tag{1.3.2}$$

where m is a natural number less than p (y^2 is used here instead of 1^2 in order to fit this into the more general argument used below). The method of proof used (which is usually referred to as a "descent argument") is to demonstrate that if $m > 1$, then there exists a natural number $m_1 < m$ having the same property as m in (1.3.2).

Continuing in this way, after a finite number of steps we will obtain $m_n = 1$ in equation (1.3.2), which implies that p itself is a sum of two squares.

To carry out the argument, assume that $m > 1$ in (1.3.2) (for otherwise there is nothing left to prove) and choose two fixed integers u and v such that

$$-\frac{m}{2} \leq u, v \leq \frac{m}{2}$$

with

$$u \equiv x, \quad v \equiv y \pmod{m}. \tag{1.3.3}$$

We then have

$$u^2 + v^2 \equiv x^2 + y^2 \equiv 0 \pmod{m},$$

which implies that

$$mr = u^2 + v^2 \tag{1.3.4}$$

for some integer r. Now $r \neq 0$, since otherwise $u^2 + v^2 = 0$, which implies $u = v = 0$, which with (1.3.3) implies in turn that x and y are multiples of m, say $x = ms$ and $y = mt$. Plugging into (1.3.2) leads to the equation $p = m(s^2 + t^2)$, which means that m is a divisor of the prime p, giving a contradiction (recall that $1 < m < p$). The inequality

$$r = \frac{1}{m}(u^2 + v^2) \leq \frac{1}{m}\left(\frac{m^2}{4} + \frac{m^2}{4}\right) < m,$$

and the fact that $u^2 + v^2 > 0$, allow us to conclude that $0 < r < m$.

By multiplying together equations (1.3.2) and (1.3.4) and using identity (1.3.1), we get

$$m^2 rp = (x^2 + y^2)(u^2 + v^2) = (xu + yv)^2 + (xv - yu)^2. \tag{1.3.5}$$

From (1.3.3), we see that

$$xu + yv \equiv x^2 + y^2 \equiv 0 \pmod{m}$$

and

$$xv - yu \equiv xy - yx \equiv 0 \pmod{m}$$

and thus both $xu + yv$ and $xv - yu$ are multiples of m, say $xu + yv = mx_1$ and $xv - yu = my_1$. Plugging into (1.3.5) and then dividing by m^2, we have

$$rp = x_1^2 + y_1^2.$$

Since r is a natural number less than m for which rp is representable as the sum of two squares, then r may be taken to play the role of m_1 in the discussion above. The descent argument finally allows us to conclude that p itself is representable as a sum of two squares. □

CHAPTER II

BINARY QUADRATIC FORMS

2.1 Discriminants of Binary Quadratic Forms

Definition 2.1.1. *A "binary quadratic form" $F(x,y)$ is a degree two (quadratic) polynomial expression $F(x,y) = ax^2+bxy+cy^2$, where the coefficients a, b, and c are fixed integers and the two variables x and y (hence binary) are restricted to taking on integer values.*

We will often just say *form(s)* for brevity instead of *binary quadratic form(s)* as most forms discussed in detail in this thesis are of this type. Special cases of ternary quadratic forms will appear in Section 4.3. When the variables are not directly relevant to a discussion, a binary quadratic form is usually denoted by its name or ordered coefficients only: F or (a,b,c).

Definition 2.1.2. *A form (a,b,c) is said to be "primitive" if* $\gcd(a,b,c) = 1$*; otherwise, "imprimitive."*

The form $(2,6,5)$ is primitive, while $(4,12,10)$, where all three coefficients are divisible by 2, is an imprimitive form. As most results about imprimitive forms are reducible to questions about primitive forms, we will focus mainly on primitive forms.

The main inquiry driving the historic study of binary quadratic (and other) forms was — and still is — the question:

Which integers can be ***represented*** *by $ax^2+bxy+cy^2$ for a given triple of coefficients?*

This is a natural generalization of expressing numbers as sums of squares as we did in

Section 1.3 and other such classical problems as those discussed in Section 1.2. Thus, if $(x, y) = (1, 2)$, then $2 \cdot 1^2 + 6 \cdot 1 \cdot 2 + 5 \cdot 2^2 = 34$, so we have found a *representation* of 34 by the form $(2, 6, 5)$. As x and y are relatively prime, we have, in particular, found a *proper representation* of 34 by this specific form. More formally, we have

Definition 2.1.3. *Let $k \neq 0$. If $F(x, y) = k$ for integers x, y with $\gcd(x, y) = 1$, we say this representation of k by F is "proper." If x and y have a common divisor greater than 1, the representation is called "improper."*

As with primitive forms, it is often of more immediate interest to focus on proper representations.

Related useful terminology includes whether a form is *definite* or *indefinite.*

Definition 2.1.4. *A "definite" form is one for which all pairs $(x, y) \neq (0, 0)$ represent integers of the same sign, i.e., $F(x, y) > 0$ for all $(x, y) \neq (0, 0)$ or $F(x, y) < 0$ for all such pairs. More precisely, the form is called "positive definite" or "negative definite," respectively.*

Definition 2.1.5. *An "indefinite" form is one which with suitable x and y can represent both positive and negative integers.*

Deciding whether a form is definite or indefinite is greatly facilitated by the following crucial

Definition 2.1.6. *The discriminant d of the binary quadratic form (a, b, c) is defined as the value $b^2 - 4ac$.*

For the form $(2, 6, 5)$, we have discriminant $d = 6^2 - 4 \cdot 2 \cdot 5 = -4$. Positive discriminants are certainly possible (simply choose a sufficiently large b). For completeness, note that a discriminant of zero is also possible but usually disregarded as being less interesting or an impediment to the concise statement of elegant theorems even though Gauss does treat this case in Art. 215 of his *Disquisitiones* [Ga]. When the discriminant of a form $F(x, y)$ is zero or any perfect square, $d = b^2$, the form decomposes into a product of linear factors (see [La], p. 171), so these forms are certainly of less interest in general even if they do arise on occasion.

Consider now an arbitrary form $ax^2 + bxy + cy^2$ with negative discriminant. Then necessarily $a \neq 0$ (because b^2 cannot be negative). Multiplying by $4a$, we have

$$\begin{aligned} 4a(ax^2 + bxy + cy^2) &= 4a^2x^2 + 4abxy + 4acy^2 \\ &= (2ax + by)^2 + (4ac - b^2)y^2. \end{aligned}$$

As the discriminant is negative, $4ac - b^2$ is positive. This means that the last expression in the equations above is zero if and only if $x = 0$ and $y = 0$. Furthermore, if either x or y is nonzero, then the same expression must be positive. Hence on the left-hand-side of the first equation, for all $(x, y) \neq (0, 0)$, the signs of a and $ax^2 + bxy + cy^2$ must be the same. Thus (a, b, c) with negative discriminant is positive definite if and only if $a > 0$, and negative definite if and only if $a < 0$. It is customary to study such definite forms by considering the positive definite forms only since each of the latter forms can be changed into a corresponding negative definite form (or vice versa) simply by changing the signs on each of a, b, and c.

Now consider an arbitrary form $F(x, y) = ax^2 + bxy + cy^2$ with positive discriminant d and assume that d is not a perfect square (given the comments above, we generally avoid discriminants that are perfect squares). In this case we see again that $a \neq 0$. Note that $F(1, 0) = a$ and $F(b, -2a) = ab^2 - b \cdot 2ba + c \cdot 4a^2 = a(4ac - b^2) = -da$.

As these two numbers must be of opposite signs, such a form is indefinite, and we see that the discriminant allows us to decide immediately whether a form is definite or indefinite.

What are all the possible values that discriminants may take on? Not every integer is possible since $b^2 - 4ac \equiv b^2 \pmod 4$ and squares can only be congruent to 0 or 1 (mod 4). The list of possible discriminant values is thus limited to

$$\ldots, -19, -16, -15, -12, -11, -8, -7, -4, -3, 0, 1, 4, 5, 8, 9, 12, 13, 16, 17, \ldots.$$

Furthermore, each of these numbers actually is a discriminant because, for all $d \equiv 0 \pmod 4$, $(1, 0, -\frac{d}{4})$ has discriminant d, and, for all $d \equiv 1 \pmod 4$, $(1, 1, -\frac{d-1}{4})$ has discriminant d. Such a form where $a = 1$ and either $b = 0$ or $b = 1$ is called the *principal form* for its discriminant. Earlier it was noted that the discriminant of $(2, 6, 5)$ is -4, but here we see that the principal form of discriminant -4 is $(1, 0, 1)$.

Note that there are, in fact, an infinite number of forms for each discriminant value: For example, given (a, b, c) of discriminant d, we have $d = b^2 - 4ac = (b + 2)^2 - 4(b + 1 + ac)$, so $(a', b', c') = (1, b + 2, b + 1 + ac)$ also has discriminant d. Iterations of this process using (a', b', c'), etc., then produce new forms with larger b-values each time so that all of these forms are distinct. In light of this fact, it is natural to investigate whether some (or all) forms of a particular discriminant may have properties in common. Historically, the concept of "equivalence classes" and a full understanding of how linear transformations of the x and y variables can change one form into another have definitively resolved this question. This is the topic of the next section, but we first need to introduce two other types of discriminants and see how they relate to each other.

Definition 2.1.7. *An integer $d \in \mathbb{Z} \setminus \{0, 1\}$ which is congruent to* 0 *or* 1 *modulo* 4 *is called a "fundamental discriminant" if it is not divisible by the square of any odd prime number and is either odd or* $\equiv 8$ *or* $\equiv 12 \pmod{16}$.

Comment 2.1.8. *If d is a fundamental discriminant and t denotes the number of distinct prime divisors of d, then $t \geq 1$ and t is finite. This is easy to see since d is neither* 0 *nor* 1 *by definition and d is $\neq -1$ either since $-1 \not\equiv 1 \pmod{4}$. It is readily apparent that an odd fundamental discriminant is "square-free" (see Definition* 2.1.9 *below).*

Definition 2.1.9. *Given a prime number p and a nonzero integer a, we let $\mathrm{ord}_p(a)$ denote the exact power of p dividing a (note that $\mathrm{ord}_p(a)$ is uniquely defined by the FTA). A nonzero integer a is said to be "square-free" if $\mathrm{ord}_p(a) \leq 1$ for every prime number p.*

Simple examples of Definition 2.1.9 are: $\mathrm{ord}_2(-8) = 3$ and $\mathrm{ord}_5(75) = 2$.

Lemma 2.1.10. *If d is an even fundamental discriminant, then $4 \mid d$ (in other words, $\mathrm{ord}_2(d) \geq 2$) and either $\frac{d}{4} \equiv 2 \pmod{4}$ or $\frac{d}{4} \equiv 3 \pmod{4}$ (thus, $\mathrm{ord}_2(d) \leq 3$). In either case, the integer $\frac{d}{4}$ is square-free.*

Proof: If d is even, then either (i) $d = 8 + 16k$ or (ii) $d = 12 + 16l$. Either way, if d is even, it is divisible by 4. In case (ii), $\mathrm{ord}_2(d) = 2$ since $\frac{d}{4} = 3 + 4l$ is odd and indeed $\frac{d}{4} \equiv 3 \pmod{4}$. In case (i), d is divisible by 8 and $\mathrm{ord}_2(d) = 3$ since $\frac{d}{8} = 1 + 2k$ is odd. In case (i), $\frac{d}{4} \equiv 2 \pmod{4}$.

By definition of a fundamental discriminant, any odd prime divides $\frac{d}{4}$ to at most the first power. In case (ii), $\mathrm{ord}_2(\frac{d}{4}) = 0$. In case (i), $\mathrm{ord}_2(\frac{d}{4}) = 1$, and so in either case, $\frac{d}{4}$ is square-free. □

Comment 2.1.11. *Note that* 4 *is not a fundamental discriminant since* 4 *is neither congruent to* 8 *nor* 12 *modulo* 16*. On the other hand,* -4*,* -8*, and* 8 *are all fundamental discriminants. By Lemma* 2.1.10*, the only fundamental discriminants divisible only by the prime* 2 *are exactly these three.*

Lemma 2.1.12. *If* D *is a nonzero square-free integer and satisfies either* $D \equiv 2 \pmod 4$ *or* $D \equiv 3 \pmod 4$*, then* $4D$ *is a fundamental discriminant.*

Proof: First $D \neq 0$, and so $4D \neq 0$. Obviously, $4D \neq 1$ and $4D \equiv 0 \pmod 4$. Since D is square-free, it is not divisible by the square of an odd prime and neither is $4D$. We have either $D = 2 + 4k$ for some integer k, and so $4D = 8 + 16k$, or $D = 3 + 4k$ for some integer k, and thus $4D = 12 + 16k$. □

Lemma 2.1.13. *If* $D \equiv 1 \pmod 4$*,* $D \neq 1$*, and* D *is square-free, then* D *is a fundamental discriminant.*

Proof: Clearly, $D \in \mathbb{Z} \setminus \{0, 1\}$, $D \equiv 1 \pmod 4$, and D is odd and not divisible by the square of any odd prime number. □

Lemma 2.1.13 shows that any odd prime p congruent to 1 modulo 4 is a fundamental discriminant. This (infinite) list of fundamental discriminants starts out as $5, 13, 17, 29, \ldots$. Lemma 2.1.13 also shows that for any odd prime p congruent to 3 modulo 4, $-p$ is a fundamental discriminant. This (infinite) list of fundamental discriminants starts out as $-3, -7, -11, -19, \ldots$.

Definition 2.1.14. *A prime discriminant is a fundamental discriminant that is divisible by exactly one prime number.*

The prime discriminants are seen to be

$$\ldots, -19, -11, -8, -7, -4, -3, 5, 8, 13, 17, 29, \ldots,$$

that is, $-8, -4, 8$ and, for each odd prime p, exactly one of $\pm p$, where the sign chosen depends upon the congruence class of p modulo 4. If $p \equiv 1 \pmod 4$, then $+p$ is the corresponding prime discriminant; otherwise, $p \equiv 3 \pmod 4$ and the corresponding prime discriminant is $-p$.

We will mainly restrict ourselves in this thesis to working with binary quadratic forms whose discriminants are fundamental but we will find it necessary to loosen this restriction on occasion. The starting list for all negative fundamental discriminants is

$$-3, -4, -7, -8, -11, -15, -19, -20, -23, -24, -31, -35, -39, \ldots$$

and similarly for positive fundamental discriminants

$$5, 8, 12, 13, 17, 21, 24, 28, 29, 33, 37, 40, 41, 44, 53, 56, 57, \ldots.$$

The following theorem gives an elegant and important refinement to the FTA within the context of discriminants.

Theorem 2.1.15. *Let d be a fundamental discriminant. Then d can be written uniquely (up to order) as a product of prime discriminants.*

Proof: This is an induction proof on the number n of distinct prime divisors of d. By Comment 2.1.8, $n \geq 1$. If $n = 1$, then d is a prime discriminant by definition and the theorem clearly holds. Now assume that the theorem holds for fundamental discriminants divisible by $n \geq 1$ distinct primes. Assume that d is divisible by $n+1$ distinct primes. This means there is at least one odd prime p such that $p \mid d$, and let $d_p \equiv 1 \pmod 4$ be the corresponding prime discriminant. The theorem will be proved if we can show that $d' = d/d_p$ is a fundamental discriminant since d' has n distinct prime divisors.

Assume first that d is even. By Lemma 2.1.10, $d = 4D$, where $D \equiv 2 \pmod 4$ or $D \equiv 3 \pmod 4$ and D is square-free. Then $d' = 4 \cdot (D/d_p)$ ($d_p \mid D$ by Theorem 1.1.5), where (D/d_p) is a square-free integer and satisfies $(D/d_p) \equiv 2 \pmod 4$ or $(D/d_p) \equiv 3 \pmod 4$, respectively, since $d_p \equiv 1 \pmod 4$. In this case, d' is a fundamental discriminant by Lemma 2.1.12.

Now assume that d is odd, in which case $d \equiv 1 \pmod 4$. By assumption, d is divisible by $n+1 \geq 2$ distinct primes and since it is an odd fundamental discriminant, it is square-free. We conclude that $d' \equiv 1 \pmod 4$ since $d_p \equiv 1 \pmod 4$, and $d' \neq 1$ since d' is divisible by at least one (odd) prime. Clearly d' is square-free and thus d' is a fundamental discriminant by Lemma 2.1.13. □

Consider the fundamental discriminant -15. It is easily seen to be expressible as $(-3) \cdot 5$, where each of -3 and 5 is a prime discriminant. As $3 \equiv 3 \pmod 4$ and $5 \equiv 1 \pmod 4$, this sign placement is necessary; the expression $3 \cdot (-5)$ is not a product of prime discriminants (nor, in this case, of discriminants of any type for that matter). As another example, the fundamental discriminant -84 may be expressed as $(-7) \cdot (-4) \cdot (-3)$, where each of the three factors is a prime discriminant and this representation is unique up to order. One of the abilities of the PARI code prpdf in Appendix A is to find the unique factorization into prime discriminants of a given negative fundamental discriminant. On the other hand, note that there is no guarantee of such a unique factorization when the discriminant is not fundamental: $-64 = (-8) \cdot 8 = (-4) \cdot (-4) \cdot (-4)$. In fact, there are no factorizations into prime discriminants for some non-fundamental discriminants such as -12.

We will use Theorem 2.1.15 extensively in Chapter IV. The prime 2 must be handled with care since there are three prime discriminants divisible by 2. Given Theorem 2.1.15, there are 4 cases that need to be treated separately. (a) The fundamental discriminant d is odd and therefore $d \equiv 1 \pmod 4$. (b) The prime discriminant $d_2 = -4$ appears in the unique factorization of d. This happens if and only if $\frac{d}{4} \equiv 3 \pmod 4$ or $d \equiv 12 \pmod{16}$. (c) The prime discriminant $d_2 = -8$ appears in the unique factorization of d. In this case, $\frac{d}{4} \equiv 2 \pmod 4$, but this can be refined slightly. By Theorem 2.1.15, d/d_2 is either equal to 1 or is equal to a product of distinct odd prime discriminants which are all congruent to 1 (mod 4) and so $d/d_2 \equiv 1 \pmod 4$. We have $\frac{d}{-8} = 1 + 4k$ which implies that $d/4 = -2 - 8k$, so $\frac{d}{4} \equiv 6 \pmod 8$. (d) The prime discriminant $d_2 = 8$ appears in the unique factorization of d. Again $\frac{d}{4} \equiv 2 \pmod 4$, but using the same argument as above, $\frac{d}{8} = 1 + 4k$, so $\frac{d}{4} \equiv 2 \pmod 8$.

It is convenient in Case (a) to set $d_2 = 1$. We may now summarize the above classification with a definition that will prove to be useful later in this thesis.

Definition 2.1.16. *The prime discriminant contribution d_2 associated to a given fundamental discriminant d is defined as follows:*

(a) $d_2 = 1$ *if and only if* $d \equiv 1 \pmod 4$.

(b) $d_2 = -4$ *if and only if* $\frac{d}{4} \equiv 3 \pmod 4$.

(c) $d_2 = -8$ *if and only if* $\frac{d}{4} \equiv 6 \pmod 8$.

(d) $d_2 = 8$ *if and only if* $\frac{d}{4} \equiv 2 \pmod 8$.

One reason that forms whose discriminants are fundamental are nicer to work with is the following

Theorem 2.1.17. *If a binary quadratic form $F(x,y) = ax^2 + bxy + cy^2$ has discriminant $b^2 - 4ac$ equal to a fundamental discriminant d, then $F(x,y)$ is a primitive form.*

Proof: Assume on the contrary that there is a positive integer $e > 1$ such that $e \mid a$, $e \mid b$, and $e \mid c$. Then there exist integers a_1, b_1, and c_1 such that $d = b^2 - 4ac = (eb_1)^2 - 4(ea_1)(ec_1) = e^2(b_1^2 - 4a_1c_1)$. If p is an odd prime dividing e, then $p^2 \mid d$, which is a contradiction since a fundamental discriminant is not divisible by the square of any odd prime number. Since $e > 1$, then some prime must divide it and we are left with only one possibility, namely that $2 \mid e$, so $e = 2t$ for some $t \in \mathbb{N}$. We already know that t can not be divisible by an odd prime so we must have $t = 2^f$ with $f \geq 0$. If $f \geq 1$, then $\text{ord}_2(e^2) \geq 4$ and we know that d is not divisible by 2^4 so we must have $f = 0$ and $e = 2$. This implies that $d = 4(b_1^2 - 4a_1c_1)$, which is possible for a fundamental discriminant d as long as $\frac{d}{4} = b_1^2 - 4a_1c_1 \equiv 2 \text{ or } 3 \pmod 4$ (see Lemma 2.1.10). On the other hand, $b_1^2 - 4a_1c_1 \equiv b_1^2 \equiv 0 \text{ or } 1 \pmod 4$, which again leads to a contradiction so we conclude that $\gcd(a,b,c) = 1$ and that $F(x,y)$ is a primitive form. □

2.2 Equivalence of Forms

Recall that an *equivalence relation* $\sim$ is a relation on a non-empty set A with these properties:

(i) reflexive property: for all $a \in A$, $a \sim a$,

(ii) symmetric property: for all $a, b \in A$, if $a \sim b$, then b $\sim a$, and

(iii) transitive property: for all $a, b, c \in A$, if $a \sim b$ and $b \sim c$, then $a \sim c$.

An equivalence relation $\sim$ *partitions* the set A into *equivalences classes*, which are non-empty, disjoint classes having A as their union. This section describes how to define an equivalence relation on all forms of a given discriminant.

To define an equivalence relation on the forms, we first examine linear transformations of the forms' variables. At the outset, in the simplest cases we see that forms such as $(a, 0, c)$ and $(c, 0, a)$ ought to be considered equivalent as $ax^2 + cy^2$ and $cx^2 + ay^2$ really are the same since only the **independent** x and y variables need be interchanged to make this explicit. In effect, that interchange is to set $x = Y$ and $y = X$, where X and Y are taken as the names of the second form's variables. The important point, which is obvious in this case, is that as the pair X, Y takes on all pairs of integer values, so does the pair x, y (and the latter pair only takes on integer values). In finding exactly how to define equivalence of forms, we seek all possible substitutions of the form

$$x = rX + sY, \quad y = tX + uY \tag{2.2.1}$$

that have this same property of x and y taking on exactly all pairs of integer values. Assuming no specific conditions on r, s, t, u at first, we see immediately that they must all be integers since $X = 1, Y = 0$ imply $x = r$ and $y = t$ while $X = 0, Y = 1$ imply $x = s$ and $y = u$. Now that we know that these four coefficients are all integers, as X and Y run through integers only, the resulting x and y values must themselves always be integers as desired.

However, we need x and y to be integers if and only if X and Y are integers. To see how to ensure this, it is helpful to express X and Y in terms of x and y.

Multiplying the first equation in (2.2.1) by u and the second equation by s and then subtracting, we have

$$ux - sy = (ru - st)X.$$

Similarly, multiplying the second equation by r and the first by t and then subtracting, we have

$$-tx + ry = (ru - st)Y.$$

Now $ru - st \neq 0$ because, otherwise, $ux - sy$ and $-tx + ry$ would always be zero and x and y would not be independent variables. Let $e = ru - st$. Then, dividing the equations above by e, we obtain

$$X = \frac{u}{e}x - \frac{s}{e}y, \quad Y = -\frac{t}{e}x + \frac{r}{e}y.$$

These four coefficients must be integers also (as seen when x, y themselves are 0,1 and 1,0). This is definitely the case when $e = \pm 1$. No other values of e suffice: If all four coefficients are integers, then so also is the expression

$$\frac{r}{e}\frac{u}{e} - \frac{s}{e}\frac{t}{e},$$

which equals $\frac{1}{e}$, a fraction that is only an integer when $e = \pm 1$. This means the coefficients r, s, t, u used in the substitution must all be integers, and further, $ru - st$ must be ± 1 in order for the substitution to make the desired correspondences between pairs of integers.

The expression $ru-st$ in this context is called the *determinant* of the substitution. This terminology is consistent with the fact that the substitution in (2.2.1) above may be represented by the matrix of coefficients $\left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$, where the determinant of this matrix, denoted by $\left|\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right|$ or $\det\left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$, by definition equals $ru - st$. Further theory is simplified if determinants of substitutions are always restricted to $+1$ and it was Gauss himself who first recognized the importance of this restriction (we will elaborate more on this crucial matter in Section 3.1) when he proclaimed that equivalence among forms induced by such substitutions is "proper." *Unimodular* substitutions (or transformations) is the more modern terminology for such restricted substitutions.

Here then is the definition of equivalence of forms that has proved itself most useful.

Definition 2.2.1. *Two forms $F = (a, b, c)$ and $G = (a_1, b_1, c_1)$ are equivalent if and only if there exists a unimodular substitution $x = rX + sY$, $y = tX + uY$, with $r, s, t, u \in \mathbb{Z}$ and $ru - st = 1$, that transforms (a, b, c) into (a_1, b_1, c_1) as follows:*

$$\begin{aligned} F(x,y) &= a(rX+sY)^2 + b(rX+sY)(tX+uY) + c(tX+uY)^2 \\ &= a_1X^2 + b_1XY + c_1Y^2 = G(X,Y), \end{aligned}$$

where

$$a_1 = ar^2 + brt + ct^2, \tag{2.2.2}$$

$$b_1 = 2ars + b(ru+st) + 2ctu, \qquad \textit{and} \tag{2.2.3}$$

$$c_1 = as^2 + bsu + cu^2. \tag{2.2.4}$$

As this definition does, in fact, describe an equivalence relation (as demonstrated in [Da], pp. 132-133), the equivalence of these two forms is denoted by $(a, b, c) \sim (a_1, b_1, c_1)$.

We see from equation (2.2.2) that $a_1 = F(r, t)$ and from equation (2.2.4) that $c_1 = F(s, u)$, which means that a_1 and c_1 are both represented by F. As $ru - st = 1$ implies by Theorem 1.1.3 that $\gcd(r, t) = 1$ and that $\gcd(s, u) = 1$, we can further say that a_1 and c_1 are both properly represented by F (assuming they are nonzero).

Given the form $F(x, y) = ax^2 + bxy + cy^2$ as above, we say that the 2×2 matrix $\mathbf{M}(F) = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$ " belongs to F." To understand why this terminology is used, note that the matrix multiplication $\begin{pmatrix} x & y \end{pmatrix} \cdot \mathbf{M}(F) \cdot \begin{pmatrix} x \\ y \end{pmatrix}$ gives a 1×1 matrix whose single entry is the form $F(x, y)$. An equivalent statement is that $(F(x, y)) = \begin{pmatrix} x \\ y \end{pmatrix}^T \cdot \mathbf{M}(F) \cdot \begin{pmatrix} x \\ y \end{pmatrix}$. In addition, the above unimodular substitution $x = rX + sY$, $y = tX + uY$ can be written in matrix form as $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix}$. By taking the transpose, we have also $\begin{pmatrix} x & y \end{pmatrix} = \begin{pmatrix} X & Y \end{pmatrix} \begin{pmatrix} r & t \\ s & u \end{pmatrix}$. It may be easily checked that $\begin{pmatrix} X & Y \end{pmatrix} \begin{pmatrix} r & s \\ t & u \end{pmatrix}^T \cdot \mathbf{M}(F) \cdot \begin{pmatrix} r & s \\ t & u \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} X & Y \end{pmatrix} \cdot \mathbf{M}(G) \cdot \begin{pmatrix} X \\ Y \end{pmatrix} = (G(X, Y))$, where $\mathbf{M}(G)$ is the matrix belonging to the form $G(X, Y) = a_1X^2 + b_1XY + c_1Y^2$ above.

The set of all 2×2 matrices with integer entries and determinant 1 forms a nonabelian group of great importance in Number Theory. This group is denoted by $SL_2(\mathbb{Z})$, where "SL" stands for "special linear" since these matrices have deteminant 1, the subscript "2" denotes the size of the matrices, and the $\mathbb{Z}$ reminds us that all entries in these matrices are integers. In particular, note that the definition of a matrix $\begin{pmatrix} r & s \\ t & u \end{pmatrix}$ corresponding to a unimodular transformation of binary quadratic forms requires that this matrix be an element of $SL_2(\mathbb{Z})$. If the transformation represented by the matrix $\left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ takes the form F to the form G, we use the notation $F\left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) = G$ since $\left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)^T \cdot \mathbf{M}(F) \cdot \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) = \mathbf{M}(G)$.

The following theorems and proofs from [La] show two important facts: (i) equivalent forms have the same discriminant and (ii) equivalent forms represent the same integers.

Theorem 2.2.2. ([La], p. 173): *If $F = (a, b, c)$ has non-square discriminant d and $F \sim G = (a_1, b_1, c_1)$, then G also has discriminant d; moreover, if $d < 0$ and $a > 0$, then we also have $a_1 > 0$. This second part means, since F and a must have the same sign (except if $x = y = 0$) when $d < 0$, that if F is positive definite, then G is positive definite as well.*

Proof: By (2.2.2), (2.2.3), and (2.2.4) we see that $b_1^2 - 4a_1c_1 = (2ars + b(ru + st) + 2ctu)^2 - 4(ar^2 + brt + ct^2)(as^2 + bsu + cu^2) = a^2(4r^2s^2 - 4r^2s^2) + b^2(r^2u^2 + 2rstu + s^2t^2 - 4rstu) + c^2(4t^2u^2 - 4t^2u^2) + 4ab(r^2su + rs^2t - r^2su - rs^2t) + 4ac(2rstu - r^2u^2 - s^2t^2) + 4bc(rtu^2 + st^2u - rtu^2 - st^2u) = (b^2 - 4ac)(ru - st)^2 = b^2 - 4ac = d$. Note that even though we are assuming that $ru - st = 1$, the discriminants of F and G would still be equal if $ru - st = -1$. Now, if $d < 0$ and $a > 0$, F represents a_1 when $x = r$ and $y = t$, so $a_1 > 0$ since F is positive definite and since $r = t = 0$ is impossible because $ru - st = 1$. □

Theorem 2.2.3. ([La], p. 174): *Equivalent forms represent the same integers.*

Proof: By the definition of equivalent forms, if $F \sim G$ and $k = G(X, Y)$, then $k = F(rX + sY, tX + uY)$. □

The forms $(1, 0, 21)$ and $(3, 0, 7)$ each have discriminant -84. The number 1 is representable by $x^2 + 21y^2$ when taking $x = 1$ and $y = 0$. However, it is clear that

$3x^2+7y^2$ can never represent 1. By the contrapositive of Theorem 2.2.3, these forms are not equivalent. As it is therefore not true in general that all forms of the same discriminant are equivalent, it would be helpful to have a general method to determine whether two specific forms of the same discriminant are equivalent. Reduction theory (to be discussed in Sections 2.3 and 2.5) is a tool that makes this both possible and straightforward.

There is a tight connection between the proper representation of integers by binary quadratic forms and the equivalence theory we have developed in this Section. To quote Davenport ([Da], p. 136), the integers "that are properly representable by a form (a,b,c) are precisely those numbers which figure as first coefficients of forms equivalent to (a,b,c). At first sight, it may seem that this method of attacking the problem [of representing integers] is not likely to get one very far; nevertheless it is the basis on which the whole theory rests."

Theorem 2.2.4. *A nonzero integer m is properly representable by the form $F(x,y)$ if and only if $F(x,y)$ is equivalent to the form $G(X,Y)=mX^2+b_1XY+c_1Y^2$ for some $b_1,c_1\in\mathbb{Z}$.*

Proof: ($\Longrightarrow$) Assume that $m=F(r,t)$ for integers r,t with $\gcd(r,t)=1$. We know there exist integers u,s such that $ru-st=1$, so that $\det\left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)=1$. By definition, the form $G(X,Y)=F(rX+sY,tX+uY)$ is properly equivalent to $F(x,y)$. By equation (2.2.2), we have $G(X,Y)=a_1X^2+b_1XY+c_1Y^2$ with $a_1,b_1,c_1\in\mathbb{Z}$ and $a_1=F(r,t)=m$.
($\Longleftarrow$) Assume that $F(x,y)\sim G(X,Y)=mX^2+b_1XY+c_1Y^2$, where $\left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$ is the transformation matrix taking F to G. We have $F(r,t)=m$ and this representation is proper since $ru-st=1$. □

We also wish to tie in the proper representation of integers by binary quadratic forms with the theory of quadratic residues mentioned in Section 1.1. This connection will be developed much more extensively in Chapter IV.

Theorem 2.2.5. *Let d be a fundamental discriminant and $m \geq 3$ an odd integer relatively prime to d. Then m is properly representable by a (necessarily primitive) form of discriminant d if and only if d is a quadratic residue modulo m.*

Proof: ($\Longrightarrow$) Assume that m is properly representable by the form $F(x,y)$ of discriminant d. By Theorem 2.2.4, $F(x,y)$ is equivalent to the form $G(X,Y) = mX^2+b_1XY+c_1Y^2$, which has the same discriminant as $F(x,y)$ and so $d = b_1^2-4mc_1$. This implies that $b_1^2 \equiv d \pmod{m}$ and so d is a quadratic residue modulo m (note that $\gcd(d,m) = 1$ by assumption).
($\Longleftarrow$) Assume that d is a quadratic residue modulo m and let $b_1 \in \mathbb{Z}$ be chosen such that $b_1^2 \equiv d \pmod{m}$. If b_1 and d are of the same parity, we leave things as they are. If b_1 and d have opposite parity, then $b_1 + m$ and d have the same parity since m is odd. Since $(b_1 + m)^2 \equiv d \pmod{m}$, we see that we may choose $b \in \mathbb{Z}$ with the same parity as d such that $b^2 \equiv d \pmod{m}$. Since b and d have the same parity and $d \equiv 0$ or $1 \pmod{4}$, we see that $4 \mid (b^2 - d)$. Since $m \mid (b^2 - d)$ and $\gcd(4,m) = 1$, we see that $4m \mid (b^2 - d)$, so that $4mc = b^2 - d$ for some $c \in \mathbb{Z}$. The form $F(x,y) = mx^2 + bxy + cy^2$ has discriminant equal to d, it is primitive by Theorem 2.1.17, and m is properly representable by $F(x,y)$ since $F(1,0) = m$. □

2.3 Reduction Theory

The goal of reduction theory is to find a representative among all the equivalent forms in a given class that is in some sense simplest. In achieving that goal a method is simultaneously found to determine in a routine manner whether any two particular forms of the same discriminant are equivalent. Reduction theory for forms with negative discriminants was developed by Lagrange and is essentially standardized. Reduction theory for forms with positive discriminant has been developed in different ways and does not have the same degree of standardization. We will follow a method due to Zagier in Section 2.5.

Theorem 2.3.1. ([La], p. 175): *Every class of forms of non-square discriminant d contains a form (a, b, c) for which*

$$|b| \leq |a| \leq |c|.$$

Proof: Let the form (a_0, b_0, c_0) be a fixed element of the class. Let a be an integer with smallest positive absolute value which is representable by (a_0, b_0, c_0) (either a or $-a$ is acceptable if both are representable). Then

$$a = a_0 r^2 + b_0 rt + c_0 t^2$$

for some integers r and t. If $\gcd(r,t) \neq 1$, then $\frac{a}{(\gcd(r,t))^2}$ would be representable, but $0 < |\frac{a}{(\gcd(r,t))^2}| < |a|$, contrary to our choice of a. Thus $\gcd(r,t) = 1$, so there exist integers s and u by Theorem 1.1.3 such that

$$ru - st = 1.$$

Note that $\left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$ takes (a_0, b_0, c_0) into (a, b', c') by equation (2.2.2). For any integer h, the unimodular transformation $\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)$ in turn takes (a, b', c') into (a, b, c) by (2.2.2) and (2.2.3), where $b = 2ah + b'$. By an appropriate choice of h, the following inequality can be satisfied:

$$|b| \leq |a|.$$

Since $c \neq 0$ (because d is not a perfect square by assumption) and since c can be represented by (a, b, c) (with $x = 0$ and $y = 1$), we conclude that c can also be represented by (a_0, b_0, c_0) by use of Theorem 2.2.3. Because |a| is minimal, then $|a| \leq |c|$, completing the proof. □

For the rest of this section, we assume that $d < 0$. For the corresponding positive definite forms (we do not consider negative definite forms) having discriminant $= d$, we observe that necessarily $a > 0$ and $c > 0$. Hence the inequalities in Theorem 2.3.1 simplify to

$$|b| \leq a \leq c.$$

Now $(a, b, c) \sim (c, -b, a)$ by the unimodular transformation $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. Taking both this transformation and the transformation $\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)$ from the proof of Theorem 2.3.1 into account, any positive definite form is equivalent to one where a, b, and c satisfy

$$\left\{\begin{matrix} \text{either } c > a \text{ and } -a < b \leq a, \\ \text{or } c = a \text{ and } 0 \leq b \leq a. \end{matrix}\right\} \tag{2.3.1}$$

Definition 2.3.2. *A positive definite form* (a,b,c) *of discriminant* $d<0$ *whose coefficients satisfy the conditions in* (2.3.1) *is called a "reduced form."*

The following elegant theorem shows why Definition 2.3.2 is so important.

Theorem 2.3.3. *Given a positive definite form* F *of discriminant* $d<0$*, there is* **exactly one** *reduced form lying in the same equivalence class as* F*.*

We refer the reader to page 176 of [La] for a proof of this important theorem. This means that it can be determined whether two positive definite forms of the same discriminant are equivalent by converting each of them into a reduced form by a well-chosen sequence of tranformations. If the two reduced forms are identical, then the two original forms are equivalent. Otherwise, the original forms are not equivalent.

Recapping what has just been discussed, here is the complete procedure used to transform a given positive definite form into a reduced form: If the form (a,b,c) does not already meet the conditions (2.3.1), then either (i) $a>c$ or (ii) b is not in the proper range. We know that the transformations $\left(\begin{smallmatrix}0&1\\-1&0\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}1&h\\0&1\end{smallmatrix}\right)$ (for suitable h), address and correct for cases (i) and (ii), respectively. Furthermore, we know that the first transformation shown makes the new a a smaller positive integer (assuming $a>c$) but does not change the absolute value of b and that the second transformation adjusts the absolute value of b as necessary but does not change the value of a at all. This means that we can consecutively apply both types of transformations as many times as needed (usually alternately) and that the procedure must terminate after a finite number of steps, producing a form (a,b,c) satisfying conditions (2.3.1). For these same reasons, when cases (i) and (ii) simultaneously apply to a given form, the procedure works equally well no matter which type of transformation is applied first, both eventually producing the same reduced form.

Here is an example of the reduction of a positive definite form: The form $(41, 100, 61)$ of discriminant $d = 100^2 - 4 \cdot 41 \cdot 61 = -4$ is seen to be equivalent to $(41, 18, 2)$ by adding $2 \cdot 41 \cdot (-1)$ to 100, i.e., by taking $h = -1$, to obtain the new b value of 18, and recalculating the new $c = \frac{b^2-d}{4a} = 2$ from the unchanged a and d, and this new b. The latter form is equivalent to $(2, -18, 41)$ by reversing the first and third coefficients and changing the sign of the second. Next, take $h = 5$ and add $2 \cdot 2 \cdot 5$ to -18 and recalculate c to get the equivalent form $(2, 2, 1)$, then again reverse the new a and c and change the sign of b to get the equivalent form $(1, -2, 2)$. Finally, take $h = 1$ and add $2 \cdot 1 \cdot 1$ to -2 and recalculate c to get the reduced form $(1, 0, 1)$. This particular form reduction required five successive transformations of the two alternating types. This algorithm is very efficient and it is often the case that only two or three such transformations are needed to take a given form to an equivalent reduced form. See reduce_neg in Appendix A for an implementation of this algorithm, for which there is also sample output in Appendix B.

2.4 Class Number

For any given discriminant d, we know by the considerations of Section 2.2 that the forms of discriminant d can be partitioned into classes via a natural equivalence relation which is consistent with the main problem of representation (cf. Theorem 2.2.3). This of course begs the following question: How many classes of forms are there for a given discriminant d? There is an infinite number of distinct forms of discriminant d but is the *number of classes* finite? It is of crucial importance that the number of classes of forms of a fixed discriminant **is finite** and this provides key insights into the representation problem of integers by binary quadratic forms even though it does not provide a full resolution to the problem as we will see in Chapter IV.

Theorem 2.4.1. ([La], p. 176): *If d is a non-square discriminant and $h(d)$ denotes the number of classes of forms of discriminant d, then $1 \leq h(d) < \infty$, i.e., the class number is finite!*

Proof: Since d is not a perfect square, for any form (a_1, b_1, c_1) of discriminant d we know that $a_1 \neq 0$ and $c_1 \neq 0$. By Theorem 2.3.1, every class of forms of non-square discriminant d contains a form (a, b, c) for which

$$|b| \leq |a| \leq |c|. \tag{2.4.1}$$

1) If $d > 0$, we conclude from (2.4.1) that $4ac < 4ac + d = b^2 \leq |ac|$. The inequality $4ac < |ac|$ would not hold if ac were positive, so we must have $ac < 0$ since $ac \neq 0$. From this observation and (2.4.1), we obtain $4a^2 \leq 4|ac| = -4ac = d - b^2 \leq d$. Thus $|a| \leq \frac{\sqrt{d}}{2}$, and

$$|b| \leq |a| \leq \frac{\sqrt{d}}{2}. \tag{2.4.2}$$

From above, we see that every class of forms of discriminant d contains a form (a, b, c) where a and b are limited to a finite set of possible values by the bounds $|b| \leq \frac{\sqrt{d}}{2}$ and $|a| \leq \frac{\sqrt{d}}{2}$, and since $c = \frac{b^2-d}{4a}$, we see that c is also limited to a finite set of possible values. Since any form of discriminant d is equivalent to some form lying within a *finite* set, the number of classes $h(d)$ is finite.

2) If $d < 0$, and we restrict ourselves to positive definite forms as usual, then (2.4.1) simplifies to $|b| \leq a \leq c$ since $a > 0$ and $c > 0$. Thus, every class of forms of discriminant d contains a form (a, b, c) such that $4a^2 \leq 4ac = -d + b^2 = |d| + b^2 \leq$

$|d| + a^2$, and so

$$|b| \leq a \leq \sqrt{\frac{|d|}{3}}. \tag{2.4.3}$$

Again, a and b are restricted to a finite set of possible values, as well as c, and the finiteness of $h(d)$ follows exactly as in part 1). □

The bounds derived above in (2.4.2) and (2.4.3) will be of use to us later as well so it is worthwhile to place them within a broader context. Note that for the bound $\frac{\sqrt{d}}{2}$ in (2.4.2), we have $\frac{\sqrt{d}}{2} = \sqrt{\frac{d}{4}} < \sqrt{\frac{d}{3}}$, and thus for all non-square discriminants d (whether positive or negative), we may make the following more uniform statement: *Every class of forms of discriminant d contains a form (a, b, c) such that $|a| \leq \sqrt{\frac{|d|}{3}}$.* An identical statement can be made as well when $d = 0$ or $d = b^2$ for any $b \in \mathbb{N}$ (this may be extracted from doing exercises 8 and 9 on pages 61 and 62 of [Fl]), and thus this statement holds for *all* discriminants. Since the unimodular transformation $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ takes (a, b, c) to the equivalent (but generally different) form $(c, -b, a)$, we may also make the same statement as above with respect to the coefficient c. We summarize the above observations as

Comment 2.4.2. *Every class of forms associated to* **any** *given discriminant d contains a form (a, b, c) such that $|a| \leq \sqrt{\frac{|d|}{3}}$ and also contains a form (a_1, b_1, c_1) such that $|c_1| \leq \sqrt{\frac{|d|}{3}}$.*

This Comment will be used at a crucial juncture in the proof of Gauss's famous Duplication Theorem in Section 4.3.

Computing the class number $h(d)$ associated to a given negative discriminant $d < 0$ is particularly straightforward given Theorem 2.3.3. With the assistance of this

Theorem, we may calculate $h(d)$ by simply finding and counting *all* of the reduced forms corresponding to a given negative discriminant. Table 1 is the result of carrying out this method for each negative fundamental discriminant whose absolute value is less than 100. The PARI procedure prpdf (print positive definite forms) included in Appendix A and for which sample output is included in Appendix B, finds and returns in a vector all the reduced forms for any input negative fundamental discriminant.

In Table 1, there are several discriminants for which the class numbers are the same. In particular, $d = -39$ and $d = -84$ are just two of the discriminants having class number 4. It may be tempting initially to think that the algebra is entirely the same for all such discriminants with identical class numbers. This would be an oversimplification. In Chapter III we will see how the classes of forms associated to a given fundamental discriminant can be given the structure of a finite abelian group. We will find in Section 3.2 that the "class group" for $d = -39$ is cyclic and isomorphic to $\mathbb{Z}_4$, whereas the class group for $d = -84$ is noncyclic and therefore isomorphic to the Klein 4-group $\mathbb{Z}_2 \times \mathbb{Z}_2$. Distinct group structures may therefore exist for different fundamental discriminants even when the class numbers (group orders) are equal.

Table 1. Class Numbers and Reduced Forms for Fundamental Discriminants d with $-100 < d < 0$

$-d$	Class No.	Reduced Forms
3	1	$(1,1,1)$
4	1	$(1,0,1)$
7	1	$(1,1,2)$
8	1	$(1,0,2)$
11	1	$(1,1,3)$
15	2	$(1,1,4),(2,1,2)$
19	1	$(1,1,5)$
20	2	$(1,0,5),(2,2,3)$
23	3	$(1,1,6),(2,1,3),(2,-1,3)$
24	2	$(1,0,6),(2,0,3)$
31	3	$(1,1,8),(2,1,4),(2,-1,4)$
35	2	$(1,1,9),(3,1,3)$
39	4	$(1,1,10),(2,1,5),(2,-1,5),(3,3,4)$
40	2	$(1,0,10),(2,0,5)$
43	1	$(1,1,11)$
47	5	$(1,1,12),(2,1,6),(2,-1,6),(3,1,4),(3,-1,4)$
51	2	$(1,1,13),(3,3,5)$
52	2	$(1,0,13),(2,2,7)$
55	4	$(1,1,14),(2,1,7),(2,-1,7),(4,3,4)$
56	4	$(1,0,14),(2,0,7),(3,2,5),(3,-2,5)$
59	3	$(1,1,15),(3,1,5),(3,-1,5)$
67	1	$(1,1,17)$
68	4	$(1,0,17),(2,2,9),(3,2,6),(3,-2,6)$
71	7	$(1,1,18),(2,1,9),(2,-1,9),(3,1,6),(3,-1,6),(4,3,5),(4,-3,5)$
79	5	$(1,1,20),(2,1,10),(2,-1,10),(4,1,5),(4,-1,5)$
83	3	$(1,1,21),(3,1,7),(3,-1,7)$
84	4	$(1,0,21),(2,2,11),(3,0,7),(5,4,5)$
87	6	$(1,1,22),(2,1,11),(2,-1,11),(3,3,8),(4,3,6),(4,-3,6)$
88	2	$(1,0,22),(2,0,11)$
91	2	$(1,1,23),(5,3,5)$
95	8	$(1,1,24),(2,1,12),(2,-1,12),(3,1,8),(3,-1,8),(4,1,6),(4,-1,6),(5,5,6)$

A cursory glance at Table 1 shows that the class number $h(d)$ fluctuates somewhat erratically as a function of the discriminant d. This makes it all the more surprising that there does exist an elegant closed form expression for $h(d)$, $d < 0$, first announced by Jacobi in 1832. Jacobi had no proof, however, and it was Dirichlet who gave the first proof in 1838 using analytic techniques, which was rather a shock given the "discrete" nature of the class number $h(d)$ itself. After a search of almost 150 years, a purely algebraic proof of Dirichlet's analytic formula was finally obtained in 1978 by H. Orde [Or]. Even given the efforts of Orde, the most "natural" proofs are still considered those arrived at through analytic means.

Dirichlet's formula is easiest to state when d is a prime discriminant of the form $-p$, with $p > 3$ and $p \equiv 3 \pmod 4$.

Dirichlet's Formula: *Given a prime $p > 3$ with $p \equiv 3 \pmod 4$, the class number $h(-p)$ is equal to $(B - A)/p$, where A is equal to the sum of all quadratic residues modulo p and B is the sum of the quadratic nonresidues modulo p. By use of the Legendre symbol defined in* Section 1.1, *we may state this formula more compactly as*

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

As an example, let $p = 31$. The quadratic residues modulo 31 are $1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28$, and their sum is $A = 186$. The sum of the (remaining) quadratic nonresidues modulo 31 is $B = 279$, and thus $h(-31) = (279 - 186)/31 = 3$, as given in Table 1.

We already saw some interaction between the theories of quadratic residues and binary quadratic forms in Theorem 2.2.5. Dirichlet's formula shows an even more profound interaction. Dirichlet's formula as given above may be generalized to give an expression for $h(d)$ for **any** discriminant $d < 0$. This requires an extension of the Legendre symbol to a new symbol named in honor of Kronecker. Kronecker's symbol will be discussed in detail in Section 4.1 because of its importance to Genus Theory. We refer the reader to Landau's book ([La], p. 227) for a full statement of Dirichlet's formula valid for all negative fundamental discriminants, and for a slightly more involved formula derived by Dirichlet as well, for positive fundamental discriminants.

2.5 Reduction Theory when the Discriminant is Positive

In this section we are concerned only with indefinite forms of positive fundamental discriminant d. We follow the presentation of Zagier [Za] but with some slightly different conventions. Our source for this section was [Ta1].

Our transformations will use transformation matrices of the form

$$\mathbf{T_n} = \left(\begin{smallmatrix} 0 & -1 \\ 1 & n \end{smallmatrix}\right) \in SL_2(\mathbb{Z}),$$

where the integer n is chosen as described below. Such a transformation takes a form (a, b, c) whose discriminant is equal to $d = b^2 - 4ac$ to a form (a', b', c') whose coefficients are

$$\begin{aligned} a' &= c, \\ b' &= -b + 2cn, \quad \text{and} \\ c' &= a - bn + cn^2, \end{aligned}$$

where $(b')^2 - 4a'c' = d$. Given such an indefinite form (a, b, c), we apply $\mathbf{T_n}$ with n

chosen such that

$$n > \frac{b+\sqrt{d}}{2c} > n-1$$

(note that $c \neq 0$ since $d = b^2 - 4ac$ cannot be a perfect square). After obtaining the new form (a', b', c'), we iterate and continue in this way.

Definition 2.5.1. *We say an indefinite form* (a, b, c) *is "reduced" if* $a > 0$, $c > 0$, *and* $b > a + c$.

The form $(1, 10, 10)$ of discriminant 60 is not a reduced form. However, $\frac{10+\sqrt{60}}{2\cdot 10} \approx .887$ and $1 > .887 > 0$, so $n = 1$ and $\mathbf{T_1} = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)$, which takes $(1, 10, 10)$ to $(10, 10, 1)$, still an unreduced form. Iterating, $\frac{10+\sqrt{60}}{2\cdot 1} \approx 8.873$ and $9 > 8.873 > 8$, so $n = 9$ for this second transformation and $\mathbf{T_9} = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 9 \end{smallmatrix}\right)$, which takes $(10, 10, 1)$ to $(1, 8, 1)$. The form $(1, 8, 1)$, also of discriminant 60, is clearly a reduced form by this definition. We note in passing that the product of these two transformation matrices, namely, $\mathbf{T_1} \cdot \mathbf{T_9} = \left(\begin{smallmatrix} -1 & -9 \\ 1 & 8 \end{smallmatrix}\right)$, is a unimodular transformation that takes $(1, 10, 10)$ directly to the reduced form $(1, 8, 1)$. See zagierreduce in Appendix A for an implementation of this algorithm, for which there is also sample output in Appendix B.

Theorem 2.5.2. *Let* $d > 0$ *be a fundamental discriminant. Every form of discriminant* d *is taken by a* **finite** *number of transformations of the above type to a reduced form in the same equivalence class. There are only finitely many reduced forms of discriminant* d.

Proof: Let (a, b, c) be an arbitrary form of discriminant $d > 0$. Let

$$\frac{b+\sqrt{d}}{2c} = n - \theta \tag{2.5.1}$$

for a uniquely defined irrational number θ with $0 < \theta < 1$. We may rewrite this as $b + \sqrt{d} = 2cn - 2c\,\theta$, so

$$-\,b + 2cn = \sqrt{d} + 2c\,\theta. \tag{2.5.2}$$

The transformation $\mathbf{T_n}$ takes the form (a, b, c) to the form (a', b', c') with

$$a' = c, \tag{2.5.3}$$

$$b' = -b + 2cn = \sqrt{d} + 2c\,\theta \quad \text{(the second equality is just (2.5.2)),} \tag{2.5.4}$$

$$c' = a - bn + cn^2. \tag{2.5.5}$$

In order to obtain a more useful version of (2.5.5), we note that by (2.5.1)

$$n^2 = \left(\frac{b+\sqrt{d}}{2c}\right)^2 + \frac{(b+\sqrt{d})\theta}{c} + \theta^2, \quad \text{so}$$

$$n^2 = \frac{b^2 + 2b\sqrt{d} + d}{4c^2} + \frac{(b+\sqrt{d})\theta}{c} + \theta^2. \tag{2.5.6}$$

We find that

$$c' = a - b\left(\frac{b+\sqrt{d}}{2c}\right) - b\,\theta + \frac{b^2 + 2b\sqrt{d} + d}{4c} + (b+\sqrt{d})\theta + c\,\theta^2, \quad \text{so}$$

$$c' = c\theta^2 + \theta\sqrt{d} \tag{2.5.7}$$

since

$$\frac{4ac - 2b^2 - 2b\sqrt{d} + b^2 + 2b\sqrt{d} + d}{4c} = 0.$$

From (2.5.7) we note that if $c > 0$, then $c' > 0$. Since $0 < \theta^2 < 1$, if we assume that $c < 0$, then $0 > c\theta^2 > c$ and by (2.5.7) $c' > c\theta^2$, so $c' > c$ when $c < 0$. As c and c' are integers, this means that the "c coefficient" will become positive after a finite number of steps and then stay positive for every following step. Since $a' = c$ by (2.5.3), the same statement holds for the "a coefficient." Now assume that both a and c have become positive. The inequality $c' < c$ can only hold a finite number of consecutive steps. At some step, after c becomes positive, we must have a succeeding $c' \geq c$. This means

$$\begin{aligned} 0 \leq c' - c &= c\theta^2 + \theta\sqrt{d} - c \qquad \text{by (2.5.7)} \\ &= \theta\sqrt{d} - c(1 - \theta^2) \\ &< (1+\theta)(\sqrt{d} - c(1-\theta)) \\ &= \frac{1+\theta}{1-\theta}\left[\sqrt{d}(1-\theta) - c(1-\theta)^2\right]. \end{aligned}$$

The expression in square braces equals $\sqrt{d} - \theta\sqrt{d} - c + 2c\theta - c\theta^2$, which may be rewritten to obtain $\sqrt{d} + 2c\theta - (c\theta^2 + \theta\sqrt{d}) - c$, which equals $b' - c' - a'$ by (2.5.4), (2.5.7), and (2.5.3). Since $(1+\theta)/(1-\theta) > 0$, we conclude from above that $0 < b' - c' - a'$. This concludes the proof of the statement that an arbitrary form (a, b, c) of discriminant d is taken by a finite number of transformations of type $\mathbf{T_n}$ to a reduced form (each new form produced by a $\mathbf{T_n}$ is in the same equivalence class as the original form since $\det(\mathbf{T_n}) = 1$).

To prove that there are only finitely many reduced forms of discriminant d, let (a, b, c) be a reduced form and set $k = b - 2a$. Then $d - k^2 = b^2 - 4ac - (b - 2a)^2 = -4ac + 4ab - 4a^2$, so

$$d - k^2 = 4a(b - a - c) > 0 \tag{2.5.8}$$

because $a > 0$ and $b > a + c$. We conclude that $k^2 < d$ (remember that $d > 0$), so that

$$|k| < \sqrt{d}. \tag{2.5.9}$$

From above, $4ac = 4ab - 4a^2 - (d - k^2)$, so

$$c = k + a - \frac{d - k^2}{4a} \tag{2.5.10}$$

since $b - a = k + a$ and we note from (2.5.8) that $4a \mid (d - k^2)$. Also from (2.5.8) we see that $a \mid \frac{d-k^2}{4}$. Since $a > 0$ and $c > 0$, we have $d = b^2 - 4ac < b^2$ and so $\sqrt{d} < b$ (remember that $b > 0$). Since $b = k + 2a$, we conclude that

$$\frac{\sqrt{d} - k}{2} < a \quad (0 < \sqrt{d} - k \text{ by } (2.5.9)). \tag{2.5.11}$$

Combining the equations above, we conclude that a reduced form of discriminant d may be put into the shape $\left(a, k + 2a, k + a - \frac{d-k^2}{4a}\right)$, with $|k| < \sqrt{d}$, $k^2 \equiv d \pmod 4$, $a \mid \frac{d-k^2}{4}$, and $\frac{\sqrt{d}-k}{2} < a$. Only finitely many a's and k's can satisfy all of these conditions. Therefore, there are only finitely many reduced forms of discriminant d. $\square$

We illustrate Theorem 2.5.2 with the concrete example of positive fundamental discriminant $d = 60$. From the proof of the second part of the theorem we can find all reduced forms $\left(a, k + 2a, k + a - \frac{d-k^2}{4a}\right)$ for this discriminant as follows. First, we note that $\sqrt{60} \approx 7.746$. The conditions on k require $|k| < \sqrt{60}$ and $k^2 \equiv 60 \pmod 4$; this means the only possible values of k are $0, \pm 2, \pm 4, \pm 6$. Furthermore, conditions on a require a to divide $\frac{60-k^2}{4}$ and for a to be greater than $\frac{\sqrt{60}-k}{2}$. Beginning with $k = 0$, we see that a must divide 15 but the last condition requires $a > \frac{\sqrt{60}-0}{2} \approx 3.873$ so $a = 5$ or $a = 15$, producing the reduced forms $(5, 10, 2)$ and $(15, 30, 14)$, respectively. Similarly considering these conditions for other values of k, we now list each other pair (k, a) meeting all the criteria — followed by an arrow and the corresponding reduced form: $(2, 7) \to (7, 16, 7), (2, 14) \to (14, 30, 15), (-2, 7) \to (7, 12, 3), (-2, 14) \to (14, 26, 11), (4, 11) \to (11, 26, 14), (-4, 11) \to (11, 18, 6), (6, 1) \to (1, 8, 1), (6, 2) \to (2, 10, 5), (6, 3) \to (3, 12, 7), (6, 6) \to (6, 18, 11)$. Note that when $k = -6$, the condition $a > \frac{\sqrt{60}-(-6)}{2} \approx 6.873$ eliminates all divisors of 6. By Theorem 2.5.2, these 12 forms are exactly the reduced forms for $d = 60$ and every form of discriminant 60 is carried into one of these by the reduction method described earlier in this Section.

Although we do not prove it here, for a given positive discriminant the set of all reduced forms having that discriminant can always be partitioned into subsets that each comprise a "cycle." This partitioning results because the $\mathbf{T_n}$ transformations used at the beginning of this Section can also be applied to an already-reduced form to produce another "neighboring" reduced form. In the example above for $d = 60$, $(1, 8, 1)$ is transformed into itself and is thus part of a cycle of length one. The forms

$(2, 10, 5)$ and $(5, 10, 2)$ each transform into the other, giving a second cycle, this one of length two. The form $(7, 16, 7)$ is transformed into $(7, 12, 3)$, which is transformed into $(3, 12, 7)$, which finally is transformed into $(7, 16, 7)$, completing this cycle of length three. The remaining six forms comprise a fourth cycle. This cycle of length 6 is: $(11, 26, 14) \rightarrow (14, 30, 15) \rightarrow (15, 30, 14) \rightarrow (14, 26, 11) \rightarrow (11, 18, 6) \rightarrow (6, 18, 11) \hookleftarrow$, where the corresponding transformation matrices taking us from one form to the next are $\mathbf{T_2}, \mathbf{T_2}, \mathbf{T_2}, \mathbf{T_2}, \mathbf{T_3}, \mathbf{T_2}$, respectively. The last arrow indicates that the last transformation returns us to the beginning of this cycle, namely, back to $(11, 26, 14)$ (we will say more about this example in Section 2.7). Because each transformation is unimodular, each form in a cycle therefore belongs to the same equivalence class of forms and represents exactly the same integers. Finally, it may be proved that two reduced forms are equivalent to each other if and only if they belong to the same cycle. Thus the class number $h(d)$ associated to a given positive discriminant d is equal to the number of distinct cycles of reduced forms. In the example above, we have $h(60) = 4$. In general, any particular form in a given cycle can be used as a representative of the equivalence class associated to that cycle.

As we saw in Section 2.3, and in particular with Theorem 2.3.3, the situation with positive definite forms of negative discriminant is as simple as one could hope for: Exactly **one** reduced form lies in each equivalence class. For indefinite forms of positive discriminant, several reduced forms can all lie in the same equivalence class. Given this, it is not surprising that class numbers associated to positive discriminants grow much slower in size as a function of $|d|$ than class numbers associated to negative discriminants. It was proved by Stark and Baker in the 1960's that there are exactly 9 negative fundamental discriminants with associated class number equal to 1, namely, the discriminants $-3, -4, -7, -8, -11, -19, -43, -67$, and -163 (the first 8 of these are already included in our Table 1). A famous open conjecture posits that $h(d) = 1$ for infinitely many distinct positive fundamental discriminants d.

2.6 Abelian Groups

Let $G_1, G_2, \cdots, G_n$ be groups (not necessarily abelian or finite), with operations $\star_1, \star_2, \cdots, \star_n$, respectively. Recall that the *direct product* of the two groups G_1 and G_2 is the group denoted by $G_1 \times G_2$ and that this new group is the Cartesian product, the set $\{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2\}$, with the new group's operation $\star$ defined componentwise; namely, for $(g_1, g_2), (g_1', g_2') \in G_1 \times G_2$,

$$(g_1, g_2) \star (g_1', g_2') = (g_1 \star_1 g_1', g_2 \star_2 g_2').$$

Clearly, as $G_1 \times G_2$ is a group, the direct product $G_1 \times G_2 \times \cdots \times G_n$ can also be defined inductively for any $n > 2$ and is also a group, now with n components, and for each $1 \leq i \leq n$, $\star_i$ is the operation for the ith component. Two other facts are also clear: 1) If all the G_i are finite groups, then $G_1 \times G_2 \times \cdots \times G_n$ is a finite group whose order is equal to $|G_1||G_2| \cdots |G_n|$; and 2) if all the G_i are abelian groups, then $G_1 \times G_2 \times \cdots \times G_n$ is an abelian group as well. With this as background, we now state without proof the following important theorem.

Fundamental Theorem of Finite Abelian Groups: *Let G be a finite abelian group with $|G| > 1$. Then G is isomorphic to $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s}$ for some $s, n_1, n_2, \ldots, n_s \in \mathbb{N}$ satisfying $n_j \geq 2$ for all j and $n_{i+1} \mid n_i$ for $1 \leq i \leq s-1$. Furthermore, this expression for G is unique.*

Definition 2.6.1. *The integers $n_1, n_2, \ldots, n_s$ are called the "invariant factors of G." The description of G in the Fundamental Theorem is called the "invariant factor decomposition of G."*

Note that $|G| = n_1 n_2 \cdots n_s$, the product of the invariant factors. Since the expression in the theorem is uniquely determined, two finite abelian groups are isomorphic if and only if their lists of invariant factors are identical.

Definition 2.6.2. *Given the list $n_1, n_2, \ldots, n_s$ of invariant factors of a finite abelian group G, we say that G is of "type $(n_1, n_2, \ldots, n_s)$." The natural number s is said to be the "rank of G."*

If the rank of G is 1, then G is (isomorphic to) the cyclic group $\mathbb{Z}_{n_1}$; otherwise, G is (isomorphic to) a direct product of two or more cyclic groups.

Consider the finite abelian group H with invariant factors 108, 12, and 2. This means that H is the unique, up to isomorphism, finite abelian group of type $(108, 12, 2)$, so $H \cong \mathbb{Z}_{108} \times \mathbb{Z}_{12} \times \mathbb{Z}_2$, and the rank of H is 3. Also, $|H| = 2592$ since $108 \cdot 12 \cdot 2 = 2592$. Suppose we are interested in finding all finite abelian groups (again up to isomorphism) of a given order such as 2592. The theorem above gives us a methodical way to determine these: We must find all $s \in \mathbb{N}$ and all integer sequences $n_1, n_2, \ldots, n_s$ such that (1) $n_j \geq 2$ for all $j \in \{1, 2, \ldots, s\}$, (2) $n_{i+1} \mid n_i, 1 \leq i \leq s-1$, and (3) $n_1 n_2 \cdots n_s = n$.

In general, if $|G| = n = n_1 n_2 \cdots n_s$ as above, then each prime divisor of n must also divide some n_i. Because $n_{i+1} \mid n_i$ for $1 \leq i \leq s-1$, and by the transitivity of divisibility, each prime divisor of n must also divide the first invariant factor n_1. Therefore n_1 is greater than or equal to the product of n's distinct prime factors. Since $n_1 \mid n$, in the particular case when n is square-free it is also true that $n \mid n_1$, which means $n_1 = n$. As a result, the only possible list of invariant factors for a square-free n is simply $n_1 = n$, so the only abelian group of square-free order n is the cyclic group $\mathbb{Z}_n$.

For the current case $n = 2592 = 2^5 \cdot 3^4 = 6 \cdot 2^4 \cdot 3^3$, we see that $(2 \cdot 3) \mid n_1$, which means that the $(4+1)(3+1) = 20$ values of n_1 are thus 6, 12, 18, 24, 36, 48, 54, 72, 96, 108, 144, 162, 216, 288, 324, 432, 648, 864, 1296, and 2592. Keeping in mind that each list of invariant factors is nonincreasing and that within each list each subsequent n_i must divide the prior integer, it is not difficult to enumerate the full list of distinct finite abelian group types of order 2592: $(6,6,6,6,2)$, $(12,12,6,3)$, $(12,6,6,6)$, $(18,18,2,2,2)$, $(18,6,6,2,2)$, $(24,12,3,3)$, $(24,6,6,3)$, $(36,36,2)$, $(36,18,2,2)$, $(36,12,6)$, $(36,6,6,2)$, $(48,6,3,3)$, $(54,6,2,2,2)$, $(72,36)$, $(72,18,2)$, $(72,12,3)$, $(72,6,6)$, $(96,3,3,3)$, $(108,12,2)$, $(108,6,2,2)$, $(144,18)$, $(144,6,3)$, $(162,2,2,2,2)$, $(216,12)$, $(216,6,2)$, $(288,9)$, $(288,3,3)$, $(324,4,2)$, $(324,2,2,2)$, $(432,6)$, $(648,4)$, $(648,2,2)$, $(864,3)$, $(1296,2)$, and (2592). In summary, there are 35 distinct types for this specific order. We will calculate this number an easier way below.

The computer algebra system PARI uses this invariant factor method to specify finite abelian groups. Another way to classify finite abelian groups, in addition to the method given by the Theorem above, is the method from the following equivalent theorem which we also state without proof (proofs of both theorems and comments supporting their equivalence may be found in [DF]).

Theorem 2.6.3. *Let G be a finite abelian group of order $n > 1$ and let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ be the unique factorization of n into powers of distinct primes using the FTA. Then*

(1) *$G \cong A_1 \times A_2 \times \cdots \times A_k$, where $|A_i| = p_i^{\alpha_i}$;*

(2) *for each* $A_i \in \{A_1, A_2, \ldots, A_k\}$ *with* $|A_i| = p_i^{\alpha_i}$,

$$A_i \cong \mathbb{Z}_{p_i^{\beta_{i,1}}} \times \mathbb{Z}_{p_i^{\beta_{i,2}}} \times \cdots \times \mathbb{Z}_{p_i^{\beta_{i,t_i}}}$$

with $\beta_{i,1} \geq \beta_{i,2} \geq \cdots \geq \beta_{i,t_i} \geq 1$ *and* $\beta_{i,1} + \beta_{i,2} + \cdots + \beta_{i,t_i} = \alpha_i$ *;*

(3) *the decompositions in* (1) *and* (2) *are unique.*

Definition 2.6.4. *The prime powers* $p_i^{\beta_{i,j}}$ *described in Theorem* 2.6.3 *are called the "elementary divisors of* G*." The description of* G *in the first two parts of Theorem* 2.6.3 *is called the "elementary divisor decomposition of* G*."*

To determine all elementary divisor decompositions for abelian groups of a given order, we again use $n = 2592 = 2^5 \cdot 3^4$ as our example. The exponents in the prime power factorization will easily give the number of distinct decompositions. The $\beta_{i,j}$'s for each prime p_i in Theorem 2.6.3, a nonincreasing sequence of natural numbers, must add up to the corresponding α_i. Such a sequence is, by definition, called a *partition* of α_i. The α_i's here, the exponents above, are 5 and 4. There are 7 partitions of 5: $[5]$, $[4,1]$, $[3,2]$, $[3,1,1]$, $[2,2,1]$, $[2,1,1,1]$, and $[1,1,1,1,1]$. There are 5 partitions of 4: $[4]$, $[3,1]$, $[2,2]$, $[2,1,1]$, and $[1,1,1,1]$. As each partition of 5 can be matched with each partition of 4, there are $7 \cdot 5 = 35$ distinct finite abelian groups of this specific order, matching what we found earlier when counting invariant factor decompositions. Keeping in mind that these partitions are of the exponents, the abelian group corresponding to the third partition of 5 listed, $[3,2]$, and the second partition of 4 listed, $[3,1]$, is $\mathbb{Z}_{2^3} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_{3^3} \times \mathbb{Z}_{3^1} = \mathbb{Z}_8 \times \mathbb{Z}_4 \times \mathbb{Z}_{27} \times \mathbb{Z}_3$. The elementary divisors here are 8, 4; 27, 3, which corresponds to one of the entries in Table 2 on page 58 (we separate the prime powers of 2 from the prime powers of 3 by a semi-colon).

Recall the definition of a *Sylow p-subgroup*: If G is a group of order $p^\alpha m$, where $p \nmid m$, then a subgroup of order p^α is a Sylow p-subgroup of G. As the factorization of n in Theorem 2.6.3 guarantees that each $p_i^{\alpha_i}$ is relatively prime to the product, call it m, of the other factors, each A_i is isomorphic to a Sylow p_i-subgroup of G. A finite abelian group G contains exactly one Sylow p-subgroup for each distinct prime $p \mid |G|$, and G is isomorphic to an internal direct product of its Sylow p-subgroups. Since (2) in Theorem 2.6.3 actually gives the invariant factors of each A_i, namely, of each Sylow p_i-subgroup, the corresponding $t = t_i$ is the rank of that Sylow p_i-subgroup.

Definition 2.6.5. *Let G be a finite abelian group and p a prime. If $p \mid |G|$, and A is the (unique) Sylow p-subgroup of G, we define the "p-rank of G" to be the rank of A. If $p \nmid |G|$, the p-rank of G is defined to be zero.*

To take an invariant factor decomposition of a finite abelian group (as PARI gives) and convert it to the corresponding elementary divisor decomposition, simply factor each invariant factor into its prime powers. Each prime power $p_l^{\gamma_{kl}}$ (ignoring any for which $\gamma_{kl} = 0$) dividing an invariant factor n_k will correspond to a cyclic group $\mathbb{Z}_{p_l^{\gamma_{kl}}}$ that is a component of the resulting direct product. This process is best described with an example, so let us reexamine the finite abelian group H which has order $2592 = 2^5 \cdot 3^4$ and invariant factors 108, 12, and 2, and carry out this conversion. As stated earlier, $H \cong \mathbb{Z}_{108} \times \mathbb{Z}_{12} \times \mathbb{Z}_2$. Now, $108 = 2^2 \cdot 3^3$ and $12 = 2^2 \cdot 3$, so $\mathbb{Z}_{108} \cong \mathbb{Z}_4 \times \mathbb{Z}_{27}$ and $\mathbb{Z}_{12} \cong \mathbb{Z}_4 \times \mathbb{Z}_3$. This means $H \cong \mathbb{Z}_4 \times \mathbb{Z}_{27} \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_2$. We conclude that the elementary divisors of H are 4, 27, 4, 3, 2, which may be rearranged without affecting the isomorphism type so that all powers of the same prime are consecutive and nonincreasing: 4, 4, 2; 27, 3. From these elementary divisors, we see that $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2$ is isomorphic to the Sylow 2-subgroup of H, giving a 2-rank of 3, and that $\mathbb{Z}_{27} \times \mathbb{Z}_3$ is isomorphic to the Sylow 3-subgroup of H, giving a 3-rank of 2. To recapitulate, the group H of type $(108, 12, 2)$, as described by its invariant factors, is the same group (up to isomorphism) as the group described by the elementary divisors 4, 4, 2; 27, 3. Table 2 on page 58 gives the complete description of all 35 finite abelian groups of order 2592 in terms of their invariant factors and corresponding elementary divisors, along with their ranks, 2-ranks, and 3-ranks.

The main theme of this thesis is Genus Theory (dating back over two centuries to Gauss). Genus Theory gives an exact formula for the 2-rank r of the class group associated to a given fundamental discriminant d in terms of the number of distinct prime divisors t of the discriminant, namely, $r = t - 1$. This important relationship will be proved in Chapter III. Since there is no corresponding complete theory known doing the same for the 3-rank or, indeed, the p-rank of the class group for any prime $p > 2$, this contribution due to Gauss with respect to the prime $p = 2$ is our most powerful tool for partially describing class groups.

Table 2. Finite Abelian Groups of Order $2592 = 2^5 \cdot 3^4$

Type (Invariant Factors)	Rank	Elementary Divisors	2-Rank	3-Rank
$(6, 6, 6, 6, 2)$	5	2, 2, 2, 2, 2; 3, 3, 3, 3	5	4
$(12, 12, 6, 3)$	4	4, 4, 2; 3, 3, 3, 3	3	4
$(12, 6, 6, 6)$	4	4, 2, 2, 2; 3, 3, 3, 3	4	4
$(18, 18, 2, 2, 2)$	5	2, 2, 2, 2, 2; 9, 9	5	2
$(18, 6, 6, 2, 2)$	5	2, 2, 2, 2, 2; 9, 3, 3	5	3
$(24, 12, 3, 3)$	4	8, 4; 3, 3, 3, 3	2	4
$(24, 6, 6, 3)$	4	8, 2, 2; 3, 3, 3, 3	3	4
$(36, 36, 2)$	3	4, 4, 2; 9, 9	3	2
$(36, 18, 2, 2)$	4	4, 2, 2, 2; 9, 9	4	2
$(36, 12, 6)$	3	4, 4, 2; 9, 3, 3	3	3
$(36, 6, 6, 2)$	4	4, 2, 2, 2; 9, 3, 3	4	3
$(48, 6, 3, 3)$	4	16, 2; 3, 3, 3, 3	2	4
$(54, 6, 2, 2, 2)$	5	2, 2, 2, 2, 2; 27, 3	5	2
$(72, 36)$	2	8, 4; 9, 9	2	2
$(72, 18, 2)$	3	8, 2, 2; 9, 9	3	2
$(72, 12, 3)$	3	8, 4; 9, 3, 3	2	3
$(72, 6, 6)$	3	8, 2, 2; 9, 3, 3	3	3
$(96, 3, 3, 3)$	4	32; 3, 3, 3, 3	1	4
$(108, 12, 2)$	3	4, 4, 2; 27, 3	3	2
$(108, 6, 2, 2)$	4	4, 2, 2, 2; 27, 3	4	2
$(144, 18)$	2	16, 2; 9, 9	2	2
$(144, 6, 3)$	3	16, 2; 9, 3, 3	2	3
$(162, 2, 2, 2, 2)$	5	2, 2, 2, 2, 2; 81	5	1
$(216, 12)$	2	8, 4; 27, 3	2	2
$(216, 6, 2)$	3	8, 2, 2; 27, 3	3	2
$(288, 9)$	2	32; 9, 9	1	2
$(288, 3, 3)$	3	32; 9, 3, 3	1	3
$(324, 4, 2)$	3	4, 4, 2; 81	3	1
$(324, 2, 2, 2)$	4	4, 2, 2, 2; 81	4	1
$(432, 6)$	2	16, 2; 27, 3	2	2
$(648, 4)$	2	8, 4; 81	2	1
$(648, 2, 2)$	3	8, 2, 2; 81	3	1
$(864, 3)$	2	32; 27, 3	1	2
$(1296, 2)$	2	16, 2; 81	2	1
(2592)	1	32; 81	1	1

2.7 Automorphs

In this Section, we consider unimodular transformations that take a form $F = (a, b, c)$ into itself. We will see that such transformations have an easy to describe overall structure.

Definition 2.7.1. *Let $F = (a, b, c)$ be an arbitrary but fixed form of discriminant d. Let $\left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$ be a unimodular transformation that takes F into itself, namely, $F\left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) = F$. Then $\left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$ is called an "automorph of F" and we denote the set of all automorphs of F by $Aut(F)$.*

It is a straightforward exercise to show that $Aut(F)$, for any given form F, is a subgroup of $SL_2(\mathbb{Z})$. In this Section, we will give the exact structure of $Aut(F)$ and will find that $Aut(F)$ is an abelian group (which is not obvious since $SL_2(\mathbb{Z})$ is nonabelian) and also that $Aut(F)$ is the same group (up to isomorphism) for all forms of the same discriminant d.

The two unimodular transformations $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ are automorphs of every form F and some forms have no other automorphs than these two. Some forms, on the other hand, have an infinite number of automorphs. We will soon see that there is a concise formula giving all automorphs of a given form (a, b, c) in terms of a, b, and c. This formula also depends upon the discriminant d and the set of all solutions to a famous Diophantine equation known as "Pell's equation," whose study dates back to antiquity. The appellation "Pell's equation" has been applied to more than one specific equation, but the version of interest to us is the equation

$$t^2 - du^2 = 4, \tag{2.7.1}$$

where d is assumed to be a fundamental discriminant, and we seek all *integer* pair solutions (t, u) to this equation. We now quote several standard results concerning this equation, and refer the reader to Chapter VII of Part One of [La] for detailed proofs. The two "trivial" solution pairs $(t, u) = (\pm 2, 0)$ of equation (2.7.1) occur for all fundamental d. If $d < -4$, there can obviously be no other solutions. When $d = -4$, there are precisely two additional solutions, namely $(t, u) = (0, \pm 1)$. When $d = -3$, there are precisely four additional solutions, namely $(t, u) = (\pm 1, \pm 1)$. This covers all negative fundamental discriminants. Things are much more interesting for positive discriminants and for the next three theorems we assume additionally that $d > 0$. We will find that the solutions to equation (2.7.1) have an abelian group structure, and the following result shows how two solutions may be "multiplied" together to give a third solution.

Theorem 2.7.2. *If (t_1, u_1) and (t_2, u_2) are integer pair solutions of* (2.7.1)*, and if we set*

$$\frac{t_1 + u_1\sqrt{d}}{2} \cdot \frac{t_2 + u_2\sqrt{d}}{2} = \frac{t + u\sqrt{d}}{2} \quad (t, u \in \mathbb{Q}), \tag{2.7.2}$$

then t and u are integers and (t, u) is also a solution pair to (2.7.1).

Solving for t and u in equation (2.7.2), we find that $t = (t_1t_2 + du_1u_2)/2$ and $u = (t_1u_2 + t_2u_1)/2$, and so it is natural to define the following operation on integer solution pairs to Pell's equation:

$$(t_1, u_1) \circ (t_2, u_2) := \Big(\frac{t_1t_2 + du_1u_2}{2}, \frac{t_1u_2 + t_2u_1}{2}\Big). \tag{2.7.3}$$

It is easily verified that this operation is commutative. The identity element is the trivial solution pair $(2, 0)$, which we denote by $\mathbf{e}$. It is also an easy verification that the solution pair $(t_1, -u_1)$ is the inverse of the pair (t_1, u_1). Finally, associativity may be verified as well. The following theorem shows that there is at least one non-trivial solution to (2.7.1) when $d > 0$.

Theorem 2.7.3. *Pell's equation* (2.7.1) *has at least one solution with nonzero u (and hence at least one solution with $t > 0$ and $u > 0$).*

When $d > 0$, there are infinitely many distinct solution pairs to Pell's equation and the following theorem describes how all of these solutions are generated in a straightforward way in terms of the group operation defined in (2.7.3).

Theorem 2.7.4. *Let (t_1, u_1) be the unique solution pair of* (2.7.1) *for which u_1 has the smallest positive value and for which $t_1 > 0$ (uniqueness holds since if $u_1 = u_2$, then $t_1^2 = t_2^2 = du_1^2 + 4$). If $\mathbf{v} = (t_1, u_1)$ (this uniquely determined solution pair is called the "fundamental solution" to* (2.7.1)*), then every solution pair (t, u) to* (2.7.1) *is given in the form $\mathbf{v}_0^a \circ \mathbf{v}^n$, with $\mathbf{v}_0 = (-2, 0)$, where the two exponent possibilities $a \in \{0, 1\}$ and $n \in \mathbb{Z}$ are uniquely determined by the given pair (t, u).*

From the possible values for the exponents a and n, we see that this group structure is the same for all fundamental $d > 0$, namely, it is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}$.

We are now ready to state the main theorem of this section.

Theorem 2.7.5. *All automorphs of a form $F = (a, b, c)$ of fundamental discriminant d are given by the formula*

$$\begin{pmatrix} \frac{t-bu}{2} & -cu \\ au & \frac{t+bu}{2} \end{pmatrix}, \tag{2.7.4}$$

where (t, u) is an arbitrary solution pair of the Pellian equation $t^2 - du^2 = 4$.

Theorem 2.7.5 shows that a bijective map ψ exists whose domain is the set $P(d)$ of all solution pairs (t, u) of (2.7.1) and whose range is $Aut(F)$, given explicitly by $\psi((t,u)) = \begin{pmatrix} \frac{t-bu}{2} & -cu \\ au & \frac{t+bu}{2} \end{pmatrix}$ (Theorem 2.7.5 actually states that ψ is surjective but it is a straightforward check to see that ψ is injective as well). We noted earlier that $P(d)$ is an abelian group when $d > 0$, with respect to the operation defined in (2.7.3), and it is easy to check that ψ is actually an isomorphism in this case. Thus, we see that $Aut(F)$ is abelian when F is a form of discriminant $d > 0$ and that $Aut(F) \cong \mathbb{Z}_2 \times \mathbb{Z}$ in this case. When $d < -4$, then $Aut(F) = \{\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)\}$, since $(\pm 2, 0)$ are the only two solutions of $t^2 - du^2 = 4$ (Note: Theorem 2.7.5 is valid for all discriminants, positive or negative) and so $Aut(F) \cong \mathbb{Z}_2$ in this case. Even though we assumed that $d > 0$ when we developed the group law (2.7.3) for combining integer solution pairs to Pell's equation, it is valid also for $d < 0$. We saw earlier that there are four integer solution pairs when $d = -4$, and it is easy to check that $(0, 1)$ generates all other solution pairs and so $Aut(F) \cong \mathbb{Z}_4$ for any form F of discriminant -4. Recall that we use the notation $G = \langle g \rangle$ when G is a cyclic group and $g \in G$ is a generator of G. If $F = (a, b, c)$ has discriminant -4, then $Aut(F) = \langle \left(\begin{smallmatrix} -b/2 & -c \\ a & b/2 \end{smallmatrix}\right) \rangle$ by Theorem 2.7.5. Similar considerations lead us to conclude that $Aut(F) \cong \mathbb{Z}_6$ for any form F of discriminant -3.

The following theorem gives a full summary of the previous paragraph and covers all possible cases; this theorem will play an important rôle in Section 3.3.

Theorem 2.7.6. *Let F be a fixed binary quadratic form of fundamental discriminant d. The subset $Aut(F) \subset SL_2(\mathbb{Z})$ of automorphs of F forms an abelian group under matrix multiplication. Furthermore, the group structure is the same for all forms of* *the same discriminant. If $d < -4$, $Aut(F) \cong \mathbb{Z}_2$; if $d = -4$, $Aut(F) \cong \mathbb{Z}_4$; if $d = -3$, $Aut(F) \cong \mathbb{Z}_6$; if $d > 0$, $Aut(F) \cong \mathbb{Z}_2 \times \mathbb{Z}$.*

There is really nothing more to say about $Aut(F)$ when F has negative discriminant. For a fixed positive fundamental discriminant $d > 0$, however, the reduction theory developed in Section 2.5 is of crucial importance in determining the somewhat elusive fundamental solution to the Pellian equation $t^2 - du^2 = 4$. This is perhaps best illustrated by a concrete example. Recall from Section 2.5 that the form $(11, 26, 14)$ of discriminant 60 lies within a cycle of length 6. Beginning with $F = (11, 26, 14)$, the successive unimodular transformations $\mathbf{T_2}, \mathbf{T_2}, \mathbf{T_2}, \mathbf{T_2}, \mathbf{T_3}, \mathbf{T_2}$ take us successively to each form in the cycle and ultimately return us to $(11, 26, 14)$. This means that $\mathbf{T_2} \cdot \mathbf{T_2} \cdot \mathbf{T_2} \cdot \mathbf{T_2} \cdot \mathbf{T_3} \cdot \mathbf{T_2} = \left(\begin{smallmatrix} -9 & -14 \\ 11 & 17 \end{smallmatrix}\right)$ is a unimodular transformation which takes $(11, 26, 14)$ to itself, namely, it is an automorph of F. Comparing this matrix product to the matrix in Theorem 2.7.5, we find that $t = 8$ and $u = 1$, which is clearly a solution of $t^2 - 60u^2 = 4$. In fact, since $u = 1$, this pair $(8, 1)$ is the fundamental solution to the equation $t^2 - 60u^2 = 4$. This process works in general, namely, if we start with a reduced form $F = (a, b, c)$ of positive fundamental discriminant $d > 0$ and multiply together all $\mathbf{T_n}$ matrices as we go exactly once around the cycle and return to F, the fundamental solution $\mathbf{v} = (t_1, u_1)$ may be immediately read off from the product matrix. Going twice around corresponds to $\mathbf{v} \circ \mathbf{v}$ and going around backwards once corresponds to the inverse of $\mathbf{v}$. One might become overly optimistic from the example above since $4 + 60u^2$ with $u = 1$ immediately produces a square, namely 8^2, and it makes one wonder if a simple trial of setting $u = 1, 2, 3, \ldots$ might quickly produce a perfect square and the corresponding fundamental solution to $t^2 - du^2 = 4$. This optimism is, however, quickly dashed by experimenting with even fairly small values of d. For example, the fundamental solution to $t^2 - 376u^2 = 4$ is $(4286590, 221064)$, an answer which would be quite tedious to find by trial and error and yet is easily obtainable by the algorithm described above.

CHAPTER III

COMPOSITION OF FORMS AND CLASS GROUPS

3.1 Concordant Forms and Composition

One of Gauss's main accomplishments in the *Disquisitiones* [Ga] was to show how the equivalence classes of primitive forms for a fixed nonzero discriminant actually comprise an abelian group when a specific, useful kind of binary operation, known as "composition," is defined for combining these classes. The equivalence classes defined by Gauss were discussed at length in Section 2.2 and we were careful to emphasize that "proper" equivalence is defined by using transformation matrices $\left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ with determinant $ru - st = 1$. Lagrange and Legendre had more loosely allowed $ru - st = \pm 1$, but the associated classes (generally fewer in number) **do not** form a natural group structure. It was Gauss's crucial observation that a group structure is naturally obtained *only* when we restrict ourselves to equivalence classes defined via transformation matrices in $SL_2(\mathbb{Z})$. In order to define and explain the group operation of composition we first define the notion of two forms being "concordant." For ease of presentation, we work strictly with forms (a, b, c) whose discriminant is fundamental. Recall from Theorem 2.1.17 that all such forms are primitive and that both a and c are automatically nonzero.

Definition 3.1.1. *Two binary quadratic forms $F_1 = (a_1, b_1, c_1)$ and $F_2 = (a_2, b_2, c_2)$ having the same fundamental discriminant d are "concordant" if and only if the following two conditions are met:*

(i) $b_1 = b_2$, *as well as*

(ii) $a_2 \mid c_1$ *and* $a_1 \mid c_2$.

Comment 3.1.2. *It is very important to note that if* $\gcd(a_1, a_2) = 1$ *for the two forms in Definition* 3.1.1*, then condition* (ii) *automatically holds if condition* (i) *holds. This is seen as follows: We have* $b_1^2 - 4a_1c_1 = d = b_2^2 - 4a_2c_2$ *by assumption. If* $b_1 = b_2$*, then* $a_1c_1 = a_2c_2$*, and so* $a_1 \mid a_2c_2$ *and* $a_2 \mid a_1c_1$*. If* $\gcd(a_1, a_2) = 1$*, we conclude that* $a_1 \mid c_2$ *by Theorem* 1.1.3 *and also* $a_2 \mid c_1$*.*

Comment 3.1.3. *If two forms* $F_1 = (a_1, b_1, c_1)$ *and* $F_2 = (a_2, b_2, c_2)$ *are concordant, then* $a_1c_1 = a_2c_2$ *and* $a_2 \mid c_1$*, so that* $a_2c = c_1$ *for some* $c \in \mathbb{Z}$*. This implies that* $a_1a_2c = a_2c_2$*, so* $a_1c = c_2$*. This means that if* F_1 *and* F_2 *are concordant, they may be given the special form* $F_1 = (a_1, b, a_2c)$ *and* $F_2 = (a_2, b, a_1c)$ *for some fixed integer* c*, where* $b = b_1 = b_2$*.*

We first define the operation of composition, denoted by $*$, with respect to concordant forms. Since we ultimately wish to combine *equivalence classes* via composition, we will need to confirm below that if we are given any two classes $\mathcal{C}_1$ and $\mathcal{C}_2$, then forms $F_1 \in \mathcal{C}_1$ and $F_2 \in \mathcal{C}_2$ exist which are concordant with each other. We then define the composition product $\mathcal{C}_1 * \mathcal{C}_2$ of the two classes as being equal to the class $\mathcal{C}_3$ to which $F_1 * F_2$ belongs. Since this must all be consistent at the class level, we must also eventually check that the class $\mathcal{C}_3$ does not depend on the choices made for the concordant forms F_1 and F_2 within $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively.

Definition 3.1.4. *The composition* $F_1 * F_2$ *of two concordant forms* $F_1 = (a_1, b, a_2c)$ *and* $F_2 = (a_2, b, a_1c)$ *(see Comment* 3.1.3*) is defined to be the form* (a_1a_2, b, c)*.*

Comment 3.1.5. *Note that if* $F_1 = (a_1, b, a_2c)$ *and* $F_2 = (a_2, b, a_1c)$ *are concordant, then* F_2 *and* F_1 *are concordant as well, in reverse order, because of the symmetry* *inherent in Definition* 3.1.1. *Note also that* $F_1 * F_2 = (a_1a_2, b, c) = F_2 * F_1$ *because of the commutativity of multiplication among the integers.*

In Definition 3.1.4, we confirm immediately that the discriminant of the composite form (a_1a_2, b, c) is equal to the discriminant of the forms we are composing since $b^2 - 4a_1a_2c = b^2 - 4a_1c_1 = d$. This is a solid first step in the right direction but we now consider an even stiffer test. Recall from Fibonacci's identity (1.3.1) that if $m_1 = x_1^2 + y_1^2$ and $m_2 = x_2^2 + y_2^2$, then $m_1 \cdot m_2 = X^2 + Y^2$, where $X = x_1x_2 - y_1y_2$ and $Y = x_1y_2 + x_2y_1$. We saw that this identity was crucial to proving exactly which positive integers are representable by the binary quadratic form $x^2 + y^2$. As we already observed in Section 2.1, the representation problem of integers by forms is the driving force behind this whole subject. Is the operation of composition relevant to the representation problem? The answer is a resounding "yes" as we now demonstrate. Assume that $F_1(x, y) = a_1x^2 + bxy + a_2cy^2$ and $F_2(x, y) = a_2x^2 + bxy + a_1cy^2$ are concordant forms and that $m_1 = F_1(x_1, y_1)$ and $m_2 = F_2(x_2, y_2)$. One may easily verify that the following remarkable identity holds:

$$m_1 \cdot m_2 = F_1(x_1, y_1) \cdot F_2(x_2, y_2) = a_1a_2X^2 + bXY + cY^2, \tag{3.1.1}$$

where $X = x_1x_2 - cy_1y_2$ and $Y = a_1x_1y_2 + a_2x_2y_1 + by_1y_2$. Note that if we set $a_1 = 1 = a_2$, $b = 0$, and $c = 1$, we recover Fibonacci's identity above, so the identity in (3.1.1) provides a vast generalization of Fibonacci's identity and it may be employed to the same powerful effect towards the representation problem as the following theorem confirms.

Theorem 3.1.6. *If $F_1(x,y) = a_1x^2 + bxy + a_2cy^2$ and $F_2(x,y) = a_2x^2 + bxy + a_1cy^2$ are concordant forms and m_1, m_2 are integers representable by F_1 and F_2, respectively, then the integer $m_1 \cdot m_2$ is representable by the composite form $F_1 * F_2$.*

Proof: This follows immediately from the definition of the form $F_1 * F_2$ and identity (3.1.1). □

To verify that the composition of concordant forms leads to a well-defined operation at the class level, we will need to prove two lemmas first. The first demonstrates that a primitive form $F(x,y)$ represents a nonzero integer relatively prime to any previously fixed nonzero integer, which seems reasonable when one experimentally substitutes in various integer values for x and y. The second addresses the issue mentioned above: Given any two classes $\mathcal{C}_1$ and $\mathcal{C}_2$, show that forms $F_1 \in \mathcal{C}_1$ and $F_2 \in \mathcal{C}_2$ exist which are concordant with each other and which satisfy additional technical conditions as well.

Lemma 3.1.7. *If $F = (a,b,c)$ is a primitive form of non-square discriminant d and n is a nonzero integer, then F properly represents a nonzero integer m that is relatively prime to n.*

Proof: Let $p_1, \ldots, p_s$ denote the prime numbers that divide a, c, and n simultaneously and set $P = \prod_{i=1}^{s} p_i$ (if $s = 0$, we set $P = 1$; this convention is used for the quantities Q, R, and S defined below as well). Let $q_1, \ldots, q_t$ denote the primes that divide a and n but not c and let $Q = \prod_{i=1}^{t} q_i$. Let $r_1, \ldots, r_u$ denote the primes that divide c and n but not a and let $R = \prod_{i=1}^{u} r_i$. Finally, let $s_1, \ldots, s_v$ denote the remaining primes dividing n (these divide neither a nor c). Note that every prime dividing n appears in exactly one of these 4 lists. Clearly, $\gcd(Q, RS) = 1$. We claim that

$m = aQ^2 + bQ(RS) + c(RS)^2$ is relatively prime to n and note that this representation of m by F is proper assuming $m \neq 0$. Given p_i (if $s = 0$, we go straight to the next step of the proof), we note that this prime divides aQ^2 (we refer to this as the "first term") and it divides the third term $c(RS)^2$, but it does not divide the second term $bQ(RS)$ since it does not divide Q, R, or S and also not b since F is primitive; therefore, $p_i \nmid m$ by Theorem 1.1.5. Given q_i, note that it divides the first and second terms but not the third term and thus $q_i \nmid m$. A given r_i or s_i will divide the second and third terms but not the first so that $r_i \nmid m$ and $s_i \nmid m$. Since all primes dividing n are now accounted for, $\gcd(m, n) = 1$ as claimed. Is $m \neq 0$? If $|n| > 1$, then at least one prime number l divides n and we showed above that $l \nmid m$. If we did have $m = 0$, then we would have $l \mid m$, in contradiction to the above. If $n = \pm 1$, then $P = Q = R = S = 1$ and $m = a + b + c$, which is relatively prime to n but potentially zero. In this case, the following alternate argument suffices. Note that $m = a \neq 0$ is properly represented by $F(x, y)$ (just set $x = 1$ and $y = 0$) and $\gcd(m, n) = 1$. □

We now introduce a convention that will be used throughout the remainder of the thesis. Let $F = (a, b, c)$ be a form of non-square discriminant d, which implies that a and c are both nonzero. If d is given and $a, b \in \mathbb{Z}$ are specified as well, then $c = (b^2 - d)/4a$, and we will simply write $F = (a, b, \bullet)$, since the value of c is uniquely determined.

Lemma 3.1.8. *Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be equivalence classes of forms of fundamental discriminant d and let n be a nonzero integer. There exists a pair of concordant forms $F_1 = (a_1, b, \bullet) \in \mathcal{C}_1$ and $F_2 = (a_2, b, \bullet) \in \mathcal{C}_2$ such that $\gcd(a_1, a_2) = 1$ and $\gcd(a_1 a_2, n) = 1$.*

Proof: Let F be an arbitrary form in $\mathcal{C}_1$. By Theorem 2.1.17, we know that F is primitive and by Lemma 3.1.7 we know that there is a nonzero integer a_1 that is properly representable by F and such that $\gcd(a_1, n) = 1$. By Theorem 2.2.4, F is equivalent to the form $G_1 = (a_1, b_1, \bullet) \in \mathcal{C}_1$ for some $b_1 \in \mathbb{Z}$. Using the same method, we may construct a form $G_2 = (a_2, b_2, \bullet) \in \mathcal{C}_2$ such that $\gcd(a_2, a_1 n) = 1$. Theorem 1.1.3 implies that $\gcd(a_1, a_2) = 1$ and $\gcd(a_2, n) = 1$.

We now note that $e = (b_2 - b_1)/2 \in \mathbb{Z}$, since b_1 and b_2 have the same parity as d. Since $\gcd(a_1, a_2) = 1$, by Theorem 1.1.3 there exist integers s_1 and s_2 such that $a_1 s_1 - a_2 s_2 = 1$, and so $a_1 s_1 e - a_2 s_2 e = e$. If $n_1 = s_1 e$ and $n_2 = s_2 e$, we conclude that $b_1 + 2a_1 n_1 = b_2 + 2a_2 n_2$. Set $b = b_1 + 2a_1 n_1$. Recall from the proof of Theorem 2.3.1 that the unimodular transformation $\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)$ takes a form $(a, b_1, \bullet)$ to the form $(a, b, \bullet)$, where $b = b_1 + 2ah$. If we set $F_1 = G_1 \left(\begin{smallmatrix} 1 & n_1 \\ 0 & 1 \end{smallmatrix}\right)$ and $F_2 = G_2 \left(\begin{smallmatrix} 1 & n_2 \\ 0 & 1 \end{smallmatrix}\right)$, then $F_1 = (a_1, b, \bullet) \in \mathcal{C}_1$, $F_2 = (a_2, b, \bullet) \in \mathcal{C}_2$, with $\gcd(a_1, a_2) = 1$. By Comment 3.1.2, we see immediately that F_1 and F_2 are concordant. Since $\gcd(a_1, n) = 1$ and $\gcd(a_2, n) = 1$, we conclude that $\gcd(a_1 a_2, n) = 1$ by Theorem 1.1.3. □

The techniques used in the proof of Lemma 3.1.8 may be immediately employed to construct a straightforward algorithm for composing classes of forms. Assume that $G_1 = (a_1, b_1, c_1) \in \mathcal{C}_1$ and $G_2 = (a_2, b_2, c_2) \in \mathcal{C}_2$. If $\gcd(a_1, a_2) = 1$ (we refer to this below as the "first branch"), there is a very fast algorithm known as the Extended Euclidean Algorithm that outputs integers n_1 and n_2 such that $a_1 n_1 - a_2 n_2 = (b_2 - b_1)/2$. Using the unimodular transformations $\left(\begin{smallmatrix} 1 & n_1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & n_2 \\ 0 & 1 \end{smallmatrix}\right)$ as in the proof above immediately gives us the concordant forms $F_1 = (a_1, b, \bullet) \in \mathcal{C}_1$ and $F_2 = (a_2, b, \bullet) \in \mathcal{C}_2$, where $b = b_1 + 2a_1 n_1 = b_2 + 2a_2 n_2$. We next compute $F_3 = F_1 * F_2 = (a_1 a_2, b, \bullet)$ and if $F_3 \in \mathcal{C}_3$, we set $\mathcal{C}_3 = \mathcal{C}_1 * \mathcal{C}_2$ (the consistency of this last operation will be proved in Proposition 3.1.9 below). If $\gcd(a_1, a_2) > 1$ (second branch), start plugging in relatively prime pairs of integers (r, t) for (x, y) in $G_1(x, y)$. Once such a pair (r, t)

is found (usually very rapidly!) such that $\gcd(a_1' = G_1(r,t), a_2) = 1$, we again use the Extended Euclidean Algorithm to find $s, u \in \mathbb{Z}$ such that $ru - st = 1$. Now $G_1' = G_1\left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) = (a_1', b_1', \bullet)$, with $b_1' = 2a_1rs + b_1(ru + st) + 2c_1tu$, is a form with $G_1' \in \mathcal{C}_1$ and $\gcd(a_1', a_2) = 1$. The forms G_1' and G_2 are now ready to be run through the first branch of the algorithm to obtain the composite form $F_3 \in \mathcal{C}_3$, completing the overall algorithm. Note that the PARI code "compose" shown starting on page 167 in Appendix A implements a variation of the algorithm described above to compose two given forms of the same discriminant. Sample output from this implementation may be seen in Appendix B.

Proposition 3.1.9. *Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be equivalence classes of forms of fundamental discriminant d. Let $F_1 = (a_1, b, a_2c) \in \mathcal{C}_1$ and $F_2 = (a_2, b, a_1c) \in \mathcal{C}_2$ be a pair of concordant forms (see Comment* 3.1.3 *and Lemma* 3.1.8*) and let $G_1 = (a_1', b', a_2'c') \in \mathcal{C}_1$ and $G_2 = (a_2', b', a_1'c') \in \mathcal{C}_2$ be a pair of concordant forms. Then $F_1 * F_2 \sim G_1 * G_2$, proving that composition is a well-defined operation at the class level.*

Proof: We will carry out the proof in four stages.

Stage 1. Assume that $F_1 = G_1$ and that $\gcd(a_1, a_2') = 1$.

Note that $b = b'$ by assumption, and thus F_1 and G_2 are concordant by Comment 3.1.2. We will show that $F_1 * F_2 \sim F_1 * G_2$. Since $F_2 \sim G_2$, there exists a unimodular transformation $\mathbf{D} = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ such that $F_2\mathbf{D} = G_2$. Equivalently,

$$\begin{pmatrix} a_2 & b/2 \\ b/2 & a_1c \end{pmatrix} \mathbf{D} = (\mathbf{D}^T)^{-1} \begin{pmatrix} a_2' & b/2 \\ b/2 & a_1'c' \end{pmatrix}, \tag{3.1.2}$$

and

$$F_2(r,t) = a_2r^2 + brt + a_1ct^2 = a_2', \tag{3.1.3}$$

as well as

$$2a_2rs + b(ru + st) + 2a_1ctu = b. \tag{3.1.4}$$

Using the fact that $(\mathbf{D}^T)^{-1} = \left(\begin{smallmatrix} u & -t \\ -s & r \end{smallmatrix}\right)$, and equating the lower left entries in matrix equation (3.1.2), we find that $-ta_1c = sa_2'$. This implies that $a_1 \mid s$ since $\gcd(a_1, a_2') = 1$ by assumption. We set $s = a_1v$ for $v \in \mathbb{Z}$ and let $\mathbf{D}' = \left(\begin{smallmatrix} r & v \\ ta_1 & u \end{smallmatrix}\right)$, noting that $\mathbf{D}' \in SL_2(\mathbb{Z})$ since $ru - ta_1v = ru - st = 1$. Note that $F_1 * F_2 = (a_1a_2, b, c)$ and $F_1 * G_2 = (a_1a_2', b, \bullet)$, and we claim that $(F_1 * F_2)\mathbf{D}' = F_1 * G_2$. We are able to verify that $(F_1 * F_2)(r, ta_1) = a_1a_2r^2 + brta_1 + c(ta_1)^2 = a_1a_2'$ by (3.1.3), and $2a_1a_2rv + b(ru + ta_1v) + 2cta_1u = b$ by (3.1.4), confirming the claim, and completing the proof of Stage 1.

Stage 2. Assume that $b = b'$ and $\gcd(a_1, a_2') = 1$.

In this case, F_1 and G_2 are concordant. By applying Stage 1 twice, we obtain $F_1 * F_2 \sim F_1 * G_2 = G_2 * F_1 \sim G_2 * G_1 = G_1 * G_2$, where the two equalities hold by Comment 3.1.5.

Stage 3. Assume that $\gcd(a_1a_2, a_1'a_2') = 1$.

By the same argument as that used in the proof of Lemma 3.1.8, integers B, n, and n' may be chosen such that $b + 2a_1a_2n = b' + 2a_1'a_2'n' = B$ since $\gcd(a_1a_2, a_1'a_2') = 1$.

Note that

$$K_1 := F_1 \begin{pmatrix} 1 & a_2 n \\ 0 & 1 \end{pmatrix} = (a_1, B, e_1) \in \mathcal{C}_1,$$

and

$$K_2 := F_2 \begin{pmatrix} 1 & a_1 n \\ 0 & 1 \end{pmatrix} = (a_2, B, e_2) \in \mathcal{C}_2,$$

for some integers e_1 and e_2. We also define

$$H_1 := (F_1 * F_2) \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} = (a_1 a_2, B, \bullet)$$

and clearly $H_1 \sim F_1 * F_2$. The form H_1 has discriminant d and so $a_1 a_2$ divides the integer $(B^2 - d)/4$; we set $a_1 a_2 w = (B^2 - d)/4$ for $w \in \mathbb{Z}$. The discriminant equation of K_1 is $B^2 - 4a_1 e_1 = d$, from which we conclude that $a_2 w = e_1$. Similarly, we have $a_1 w = e_2$, and we deduce that the two forms K_1 and K_2 are concordant. Composing K_1 and K_2 gives $K_1 * K_2 = H_1$.

By the same argument,

$$L_1 := G_1 \begin{pmatrix} 1 & a_2' n' \\ 0 & 1 \end{pmatrix} = (a_1', B, \bullet) \in \mathcal{C}_1$$

and

$$L_2 := G_2 \begin{pmatrix} 1 & a_1' n' \\ 0 & 1 \end{pmatrix} = (a_2', B, \bullet) \in \mathcal{C}_2.$$

are concordant forms. We define

$$H_2 := (G_1 * G_2) \begin{pmatrix} 1 & n' \\ 0 & 1 \end{pmatrix} = (a_1' a_2', B, \bullet)$$

and note that $H_2 \sim G_1 * G_2$ as well as $L_1 * L_2 = H_2$. Since $\gcd(a_1a_2, a_1'a_2') = 1$, we have $\gcd(a_1, a_2') = 1$, and we conclude from Stage 2 that $K_1 * K_2 \sim L_1 * L_2$. Putting everything from above together, we have $F_1 * F_2 \sim H_1 = K_1 * K_2 \sim L_1 * L_2 = H_2 \sim G_1 * G_2$, completing the proof of Stage 3.

Stage 4. Assume full generality.

By Lemma 3.1.8, there exist concordant forms $J_1 = (a_1'', b'', \bullet) \in \mathcal{C}_1$ and $J_2 = (a_2'', b'', \bullet) \in \mathcal{C}_2$ such that $\gcd(a_1'', a_2'') = 1$ and $\gcd(a_1''a_2'', a_1a_2a_1'a_2') = 1$. This implies that $\gcd(a_1a_2, a_1''a_2'') = 1$ and by Stage 3 we conclude that $F_1 * F_2 \sim J_1 * J_2$. Similarly, we have $\gcd(a_1''a_2'', a_1'a_2') = 1$ and $J_1 * J_2 \sim G_1 * G_2$ by Stage 3. By transitivity, we finally conclude that $F_1 * F_2 \sim G_1 * G_2$. □

Before closing out this Section, we prove a refinement of Lemma 3.1.7.

Proposition 3.1.10. *Let $F(x, y) = ax^2 + bxy + cy^2$ be a form of fundamental discriminant d and assume that F is positive definite if $d < 0$. If n is a fixed positive integer, then F properly represents a positive integer m that is relatively prime to n.*

Proof: If $d < 0$, then every nonzero integer that F represents is positive since F is positive definite by assumption. Since d is fundamental, F is automatically primitive by Theorem 2.1.17. Therefore, a direct application of Lemma 3.1.7 completes the proof when $d < 0$.

We assume throughout the remainder of the proof that $d > 0$ and we recall from Section 2.1 that F is an indefinite form in this case. We first prove that F is equivalent to a form (a_1, b_1, c_1) with $a_1 > 0$. Since F is indefinite, there is a pair of integers $(x_1, y_1) \neq (0, 0)$ such that $F(x_1, y_1) = h_1 > 0$. If $e_1 = \gcd(x_1, y_1)$ and $r, t \in \mathbb{Z}$ are such that $re_1 = x_1$ and $te_1 = y_1$, then $\gcd(r, t) = 1$. We then have $F(x_1, y_1) = a(re_1)^2 + b(re_1)(te_1) + c(te_1)^2 = h_1$, so $e_1^2 \cdot F(r, t) = h_1$, which implies that $e_1^2 \cdot a_1 = h_1$ for some positive integer a_1. This implies that the positive integer a_1 is properly representable by the form $F(x, y)$ and so F is equivalent to the form (a_1, b_1, c_1) for some $b_1, c_1 \in \mathbb{Z}$ by Theorem 2.2.4. Since equivalent forms represent the same integers by Theorem 2.2.3, and properly represent the same integers as well, for the sake of proving the present result we may assume without loss of generality that $F(x, y) = ax^2 + bxy + cy^2$ with $a \in \mathbb{Z}^+$.

We are done immediately if $n = 1$, so assume that $n > 1$ and that $\{p_1, \ldots, p_k\}$, $k \geq 1$, is the set of all primes dividing n (the following argument works equally well whether d is positive or negative). A given p_i does not divide a, b, and c simultaneously since the form F is primitive. If $p_i \nmid a$, then the value $F(x_i, y_i)$ is not divisible by p_i when we choose x_i, y_i such that $x_i \equiv 1,\ y_i \equiv 0 \pmod{p_i}$. If $p_i \nmid c$, then again $p_i \nmid F(x_i, y_i)$ when $x_i \equiv 0,\ y_i \equiv 1 \pmod{p_i}$. If $p_i \mid a$ and $p_i \mid c$, then $p_i \nmid b$, and $p_i \nmid F(x_i, y_i)$ if x_i, y_i are chosen such that $x_i \equiv 1,\ y_i \equiv 1 \pmod{p_i}$. We conclude that we may choose an integer pair (x_i, y_i) for each i with $1 \leq i \leq k$ which satisfies certain congruence conditions modulo p_i ensuring that $p_i \nmid F(x_i, y_i)$. Using the CRT, we now choose integers x, y such that $x \equiv x_i \pmod{p_i}$ and $y \equiv y_i \pmod{p_i}$ for $1 \leq i \leq k$. The value $F(x, y)$ is then not divisible by any prime in the set $\{p_1, \ldots, p_k\}$ and is thus relatively prime to n. If $F(x, y) > 0$, then using the same argument from the previous paragraph, the form F is seen to properly represent a positive integer m that is in turn relatively prime to n. If $F(x, y) < 0$, we will now show that x may be replaced by an integer x' (we do not change the value of y) which still satisfies the same congruences as x above and yet $F(x', y) > 0$, which will complete the proof. Setting $x' = x + n \cdot z$ for any given $z \in \mathbb{Z}$ guarantees that $x' \equiv x_i \pmod{p_i}$ for $1 \leq i \leq k$ and so $F(x', y)$ is relatively prime to n. Recalling the identity

$$4aF(x', y) = (2ax' + by)^2 - dy^2$$

used on page 21 of this thesis, we see that if z is chosen to be a large enough positive integer, then the right hand side will be positive since a, b, d, and y are all fixed. Since $a > 0$, we see in this case that $F(x', y) > 0$. □

3.2 Class Groups

Definition 3.2.1. *If d is a fundamental discriminant, we let $\mathcal{H}(d)$ denote the set of equivalence classes of binary quadratic forms of discriminant d. It will be shown in Theorem* 3.2.3 *below that $\mathcal{H}(d)$ can be given the structure of a finite abelian group and for this reason we call $\mathcal{H}(d)$ the "class group of discriminant d."*

Definition 3.2.2. *Let d be a fixed fundamental discriminant. The form $F_0 = (1, 0, -\frac{d}{4})$ if $d \equiv 0 \pmod 4$, or $F_0 = (1, 1, \frac{1-d}{4})$ if $d \equiv 1 \pmod 4$, is called the "principal form" of discriminant d. The class $\mathcal{C}_0 \in \mathcal{H}(d)$ to which F_0 belongs is known as the "principal class" of discriminant d.*

Theorem 3.2.3. *If d is a fundamental discriminant, then $\mathcal{H}(d)$ forms a finite abelian group of order $h(d)$ and identity element $\mathcal{C}_0$ with respect to the binary operation of composition defined at the class level in Section* 3.1.

Proof: In Proposition 3.1.9, we proved that composition is a well-defined binary operation at the class level. We now verify all of the axioms which demonstrate that $\mathcal{H}(d)$ is an abelian group (we already proved that its order $h(d)$ is finite in Theorem 2.4.1).

Class composition is a commutative operation. This axiom follows immediately from Comment 3.1.5.

The element $\mathcal{C}_0$ acts as the identity element. Let $\mathcal{C}$ be a class in $\mathcal{H}(d)$ and $F = (a, b, \bullet) \in \mathcal{C}$. Let b_0 denote the b-coefficient of the principal form F_0. Since $b \equiv d \equiv b_0 \pmod 2$, there is an integer n such that $b = b_0 + 2n$, which means that $G_0 := F_0 \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right) = (1, b, \bullet) \in \mathcal{C}_0$. Clearly, G_0 and F are concordant and $G_0 * F$ lies in the class $\mathcal{C}_0 * \mathcal{C}$ by definition. But $G_0 * F = (a, b, \bullet) = F$, and so $\mathcal{C}_0 * \mathcal{C} = \mathcal{C}$, proving that $\mathcal{C}_0$ acts as the identity element for class composition.

The existence of an inverse element. Let $\mathcal{C}$ be a class in $\mathcal{H}(d)$ and $F = (a, b, c) \in \mathcal{C}$. The form $G = (c, b, a)$ also has discriminant d and F and G are clearly concordant. If $\mathcal{C}' \in \mathcal{H}(d)$ denotes the class in which G lies, then $F * G$ lies in the class $\mathcal{C} * \mathcal{C}'$ by definition. Note that $F * G = (ac, b, 1)$ and it only remains to show that $(ac, b, 1) \in \mathcal{C}_0$ to prove that $\mathcal{C}'$ acts as the inverse element of $\mathcal{C}$. Recall from Section 2.3 that $(ac, b, 1) \sim (1, -b, ac)$. Given that $-b \equiv b_0 \pmod{2}$, there is an integer n such that $b_0 = -b + 2n$. Therefore, $(1, -b, ac)\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right) = (1, b_0, \bullet) = F_0$, completing the proof.

Class composition is an associative operation. Let $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$ be any three given classes in $\mathcal{H}(d)$. Using the same argument as in the first paragraph of the proof of Lemma 3.1.8, we construct a form $G_3 = (a_3, b_3, \bullet) \in \mathcal{C}_3$ with a_3 an odd integer. Again, using Lemma 3.1.8, there exists a pair of concordant forms $G_1 = (a_1, b_1, \bullet) \in \mathcal{C}_1$ and $G_2 = (a_2, b_2, \bullet) \in \mathcal{C}_2$ such that $\gcd(a_1, a_2) = 1$ and $\gcd(a_1 a_2, 2a_3) = 1$. Note that $\gcd(a_1, a_3) = \gcd(a_2, a_3) = 1$ and a_1 and a_2 are each odd as well. By construction, the four nonzero integers $2, |a_1|, |a_2|$, and $|a_3|$ are all pairwise relatively prime. By the CRT, there exists an integer B that is a simultaneous solution to the four congruences $B \equiv b_0 \pmod{2}$, $B \equiv b_1 \pmod{|a_1|}$, $B \equiv b_2 \pmod{|a_2|}$, and $B \equiv b_3 \pmod{|a_3|}$. Since $b_0 \equiv d \pmod{2}$, we see that B has the same parity as b_1, b_2, and b_3. Since $2 \mid (B - b_1)$, $a_1 \mid (B - b_1)$, and $\gcd(2, a_1) = 1$, we conclude that $2a_1 \mid (B - b_1)$, which means $b_1 + 2a_1 n_1 = B$ for some $n_1 \in \mathbb{Z}$. Similarly, $b_2 + 2a_2 n_2 = B$ and $b_3 + 2a_3 n_3 = B$ for integers $n_2, n_3 \in \mathbb{Z}$. Now define $F_j := G_j \begin{pmatrix} 1 & n_j \\ 0 & 1 \end{pmatrix} = (a_j, B, \bullet) \in \mathcal{C}_j$ for $j = 1, 2, 3$, and note that F_1, F_2, and F_3 are all pairwise concordant. Finally, $(F_1 * F_2) * F_3 = (a_1 a_2, B, \bullet) * (a_3, B, \bullet) = ((a_1 a_2) a_3, B, \bullet) = (a_1 (a_2 a_3), B, \bullet) = (a_1, B, \bullet) * (a_2 a_3, B, \bullet) = F_1 * (F_2 * F_3)$, proving that class composition is an associative operation (note that associativity of multiplication among the integers provided a crucial step here). All group axioms are thus established, which allows us to finally conclude that $\mathcal{H}(d)$ forms a finite abelian group. □

The tables below exemplify class groups for various discriminants that exhibit different group structures. Of course, when the order of the class group is prime or square-free, the group must be cyclic. In the tables and elsewhere below we use the notation $[a, b, c]$ to refer to the equivalence class containing the form (a, b, c). As mentioned in Section 2.4, $\mathcal{H}(-39) \cong \mathbb{Z}_4$, and Table 3 shows that the class $[2, 1, 5]$ generates this class group.

Table 3. Class Group Table for Discriminant -39

$*$	$[1,1,10]$	$[2,1,5]$	$[3,3,4]$	$[2,-1,5]$
$[1,1,10]$	$[1,1,10]$	$[2,1,5]$	$[3,3,4]$	$[2,-1,5]$
$[2,1,5]$	$[2,1,5]$	$[3,3,4]$	$[2,-1,5]$	$[1,1,10]$
$[3,3,4]$	$[3,3,4]$	$[2,-1,5]$	$[1,1,10]$	$[2,1,5]$
$[2,-1,5]$	$[2,-1,5]$	$[1,1,10]$	$[2,1,5]$	$[3,3,4]$

As Table 4 shows, the class group of order 4 associated with $d = -84$ is the Klein 4-group since each class is its own inverse (recall that $\mathcal{C}_0 = [1, 0, 21]$ is the principal class and identity element for the class group of discriminant -84). Using the terminology from Section 2.6, this class group of order 4 is of type $(2, 2)$ and its 2-rank is 2.

Table 4. Class Group Table for Discriminant -84

$*$	$[1,0,21]$	$[2,2,11]$	$[3,0,7]$	$[5,4,5]$
$[1,0,21]$	$[1,0,21]$	$[2,2,11]$	$[3,0,7]$	$[5,4,5]$
$[2,2,11]$	$[2,2,11]$	$[1,0,21]$	$[5,4,5]$	$[3,0,7]$
$[3,0,7]$	$[3,0,7]$	$[5,4,5]$	$[1,0,21]$	$[2,2,11]$
$[5,4,5]$	$[5,4,5]$	$[3,0,7]$	$[2,2,11]$	$[1,0,21]$

In Table 5, we see that $\mathcal{H}(-87) = \langle [2,1,11] \rangle \cong \mathbb{Z}_6$.

Table 5. Class Group Table for Discriminant -87

$*$	$[1,1,22]$	$[2,1,11]$	$[4,-3,6]$	$[3,3,8]$	$[4,3,6]$	$[2,-1,11]$
$[1,1,22]$	$[1,1,22]$	$[2,1,11]$	$[4,-3,6]$	$[3,3,8]$	$[4,3,6]$	$[2,-1,11]$
$[2,1,11]$	$[2,1,11]$	$[4,-3,6]$	$[3,3,8]$	$[4,3,6]$	$[2,-1,11]$	$[1,1,22]$
$[4,-3,6]$	$[4,-3,6]$	$[3,3,8]$	$[4,3,6]$	$[2,-1,11]$	$[1,1,22]$	$[2,1,11]$
$[3,3,8]$	$[3,3,8]$	$[4,3,6]$	$[2,-1,11]$	$[1,1,22]$	$[2,1,11]$	$[4,-3,6]$
$[4,3,6]$	$[4,3,6]$	$[2,-1,11]$	$[1,1,22]$	$[2,1,11]$	$[4,-3,6]$	$[3,3,8]$
$[2,-1,11]$	$[2,-1,11]$	$[1,1,22]$	$[2,1,11]$	$[4,-3,6]$	$[3,3,8]$	$[4,3,6]$

We saw in Section 2.5 that $h(60) = 4$ and Table 6 shows that $\mathcal{H}(60) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Table 6. Class Group Table for Discriminant 60

$*$	$[1,8,1]$	$[2,10,5]$	$[3,12,7]$	$[11,18,6]$
$[1,8,1]$	$[1,8,1]$	$[2,10,5]$	$[3,12,7]$	$[11,18,6]$
$[2,10,5]$	$[2,10,5]$	$[1,8,1]$	$[11,18,6]$	$[3,12,7]$
$[3,12,7]$	$[3,12,7]$	$[11,18,6]$	$[1,8,1]$	$[2,10,5]$
$[11,18,6]$	$[11,18,6]$	$[3,12,7]$	$[2,10,5]$	$[1,8,1]$

In Table 7, we exhibit a class group isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_2$ corresponding to the fundamental discriminant $d = -260 = (-4)(5)(13)$. Since the number of distinct prime divisors t of d is 3, we expect from Genus Theory (see the last paragraph of Section 2.6) that the 2-rank r of $\mathcal{H}(-260)$ is $t - 1 = 2$, and this is confirmed in this example. The 2-ranks of $\mathcal{H}(-39)$, $\mathcal{H}(-84)$, $\mathcal{H}(-87)$, and $\mathcal{H}(60)$ are $1, 2, 1$, and 2, respectively, which again is consistent with the predictions of Genus Theory.

Table 7. Class Group Table for Discriminant -260

$*$	$[1,0,65]$	$[5,0,13]$	$[2,2,33]$	$[3,2,22]$	$[3,-2,22]$	$[6,2,11]$	$[6,-2,11]$	$[9,8,9]$
$[1,0,65]$	$[1,0,65]$	$[5,0,13]$	$[2,2,33]$	$[3,2,22]$	$[3,-2,22]$	$[6,2,11]$	$[6,-2,11]$	$[9,8,9]$
$[5,0,13]$	$[5,0,13]$	$[1,0,65]$	$[9,8,9]$	$[6,-2,11]$	$[6,2,11]$	$[3,-2,22]$	$[3,2,22]$	$[2,2,33]$
$[2,2,33]$	$[2,2,33]$	$[9,8,9]$	$[1,0,65]$	$[6,2,11]$	$[6,-2,11]$	$[3,2,22]$	$[3,-2,22]$	$[5,0,13]$
$[3,2,22]$	$[3,2,22]$	$[6,-2,11]$	$[6,2,11]$	$[9,8,9]$	$[1,0,65]$	$[5,0,13]$	$[2,2,33]$	$[3,-2,22]$
$[3,-2,22]$	$[3,-2,22]$	$[6,2,11]$	$[6,-2,11]$	$[1,0,65]$	$[9,8,9]$	$[2,2,33]$	$[5,0,13]$	$[3,2,22]$
$[6,2,11]$	$[6,2,11]$	$[3,-2,22]$	$[3,2,22]$	$[5,0,13]$	$[2,2,33]$	$[9,8,9]$	$[1,0,65]$	$[6,-2,11]$
$[6,-2,11]$	$[6,-2,11]$	$[3,2,22]$	$[3,-2,22]$	$[2,2,33]$	$[5,0,13]$	$[1,0,65]$	$[9,8,9]$	$[6,2,11]$
$[9,8,9]$	$[9,8,9]$	$[2,2,33]$	$[5,0,13]$	$[3,-2,22]$	$[3,2,22]$	$[6,-2,11]$	$[6,2,11]$	$[1,0,65]$

3.3 Ambiguous Classes and Ambiguous Forms

With all of the above preliminaries in place, we are now ready to take a detailed look at the class group $\mathcal{H}(d)$ itself and in particular try to say something about the 2-rank of its Sylow 2-subgroup. As already mentioned at the end of Section 2.6, Genus Theory is directly concerned with the 2-rank of $\mathcal{H}(d)$. We first define a certain subset of $\mathcal{H}(d)$ that plays a crucial role in these investigations. Recall that if G is a finite group and $a \in G$, then the "order" of a is the smallest positive integer n such that a^n is equal to the identity element in G. We denote the order of a within the group G by $|a|$ and recall that $|a| \mid |G|$.

Definition 3.3.1. *If d is a fundamental discriminant, the subset $\mathcal{A}(d)$ of $\mathcal{H}(d)$ consisting of all classes of order* 1 *or* 2 *within the group $\mathcal{H}(d)$ is known as the set of "ambiguous classes of discriminant d."*

It is a straightforward exercise to show that $\mathcal{A}(d)$ forms a subgroup of $\mathcal{H}(d)$. A more illuminating proof results from realizing these classes as the kernel of a homomorphic map that runs through the whole subject of Genus Theory: The so-called "squaring map."

Let G be an abelian group (finite or infinite) and consider the function $\varphi : G \to G$ defined by $\varphi(a) = a^2$ for all $a \in G$. This function φ, known as the "squaring map on G," is a homomorphism since $\varphi(ab) = (ab)^2 = abab = a^2b^2 = \varphi(a) \cdot \varphi(b)$ for all $a, b \in G$, where the abelian condition was used in the third equality. Recall from Group Theory that the kernel of a homomorphism φ, denoted by $\ker(\varphi)$, is the set of all elements $a \in G$ such that $\varphi(a) = e$, where e is the identity element in the codomain of φ, in the squaring map, G itself. It is well-known that $\ker(\varphi)$ is a normal subgroup of G. The image of φ, denoted by $\mathrm{im}(\varphi)$, is a subgroup of G, and the first isomorphism theorem (see page 97 of [DF]) states that the quotient group $G/\ker(\varphi)$ is isomorphic to $\mathrm{im}(\varphi)$. If G is a finite group, then $|G/\ker(\varphi)| = |G|/|\ker(\varphi)|$, a fact which we will have occasion to use often in the sequel.

As a first example of the squaring map, let $G = U_p$, the multiplicative group of reduced residue classes modulo a prime p, where we assume $p \geq 3$. Recall that $|G| = p - 1$. If $\varphi : G \to G$ is the squaring map, then $\ker(\varphi) = \{\overline{1}, \overline{-1}\}$, and $\mathrm{im}(\varphi)$ is the set of all square classes in U_p. We have $|\mathrm{im}(\varphi)| = (p-1)/2$ from above, and we let $\mathrm{im}(\varphi) = \{\overline{a_1}, \ldots, \overline{a_{(p-1)/2}}\}$, where we assume $1 \leq a_1 < \cdots < a_{(p-1)/2} \leq p - 1$ to ensure uniqueness. The integers $a_1, \ldots, a_{(p-1)/2}$ are exactly the $(p-1)/2$ quadratic residues (mod p) mentioned in part (iv) of Theorem 1.1.13.

Comment 3.3.2. *In this first example, G is a cyclic group (by the existence of a so-called "primitive root modulo p") of even order. If $G = \langle a \rangle$ is any finite cyclic group of even order $m \geq 2$, then the kernel of the squaring map φ on G consists of exactly two elements, namely, e and $a^{m/2}$ (note that G has exactly one element of order 2).*

Comment 3.3.3. *More generally, let G be any finite abelian group and φ the squaring map on G. If $T = \{a \in G \mid |a| = 1 \text{ or } 2\}$, we claim that $T = \ker(\varphi)$. Clearly, $T \subseteq \ker(\varphi)$. If $a \in G \setminus T$, then $|a| \geq 3$ and $a^2 \neq e$, which shows that $\ker(\varphi) \subseteq T$.*

By Comment 3.3.3, we see immediately that $\mathcal{A}(d)$ forms a normal subgroup of $\mathcal{H}(d)$. Later in this Section, we will give an exact formula for $|\mathcal{A}(d)|$ in terms of the number of distinct prime divisors t of the discriminant d. We will use this formula to obtain the following simple expression for the 2-rank r of $\mathcal{H}(d)$: $r = t - 1$. However, before we go further, we first consider another example of the squaring map which will be of service in proving the relationship $r = t - 1$.

Fix a binary quadratic form F of (fundamental) discriminant d and let $G = Aut(F)$. Recall from Theorem 2.7.6 that $Aut(F)$ is an abelian group which is cyclic of even order when $d < 0$, and is an infinite abelian group whose structure is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}$ when $d > 0$. If φ is the squaring map on G, set $J = \operatorname{im}(\varphi)$, and note that J is a normal subgroup of G since G is abelian.

Lemma 3.3.4. *In terms of the notation just introduced, the quotient group G/J is of order 2 if $d < 0$ and it is of order 4 if $d > 0$.*

Proof: We consider the fundamental discriminant d by cases. Section 2.7's notation for Pell equation solutions is summarized here and extended by also defining $\mathbf{g}$ and $\mathbf{h}$ for use below: $\mathbf{e} = (2, 0), \mathbf{g} = (0, 1), \mathbf{h} = (1, 1), \mathbf{v}_0 = (-2, 0)$, and $\mathbf{v} = (t_1, u_1)$ (see Theorem 2.7.4 and equation (2.7.3)).

Case i) $d < -4$. By Theorem 2.7.6, $G \cong \mathbb{Z}_2$, so $G \cong \langle \mathbf{v}_0 \rangle$ and $J = \operatorname{im}(\varphi) \cong \{\mathbf{e}\}$. Since $|G/J| = |G|/|J|$ for any finite group G and normal subgroup J, $|G/J| = 2/1 = 2$.

Case ii) $d = -4$. By Theorem 2.7.6, $G \cong \mathbb{Z}_4$, so $G \cong \langle \mathbf{g} \rangle \,(= \langle \mathbf{g}^3 = (0, -1) \rangle)$ and $J = \operatorname{im}(\varphi) \cong \{\mathbf{e}, \mathbf{g}^2\} (= \{\mathbf{e}, \mathbf{v}_0\})$. Thus $|G/J| = |G|/|J| = 4/2 = 2$.

Case iii) $d = -3$. By Theorem 2.7.6, $G \cong \mathbb{Z}_6$, so $G \cong \langle \mathbf{h} \rangle$ $(= \langle \mathbf{h}^5 = (1, -1) \rangle)$ and $J = \operatorname{im}(\varphi) \cong \{\mathbf{e}, \mathbf{h}^2, \mathbf{h}^4\}(= \{\mathbf{e}, (-1, 1), (-1, -1)\})$. Therefore $|G/J| = |G|/|J| = 6/3 = 2$. We see that in all cases with $d < 0$ the order of G/J is 2 as was to be shown.

Case iv) $d > 0$. By Theorem 2.7.6, $G \cong \mathbb{Z}_2 \times \mathbb{Z}$, so $\operatorname{im}(\varphi) \cong J := \{\mathbf{v}^{2n} | n \in \mathbb{Z}\}$. Let $\mathbf{g}_1 = \mathbf{e}, \mathbf{g}_2 = \mathbf{v}, \mathbf{g}_3 = \mathbf{v}_0$, and $\mathbf{g}_4 = \mathbf{v}_0 \circ \mathbf{v}$, so that $\mathbf{g}_1 J = \mathbf{e} J = J$, $\mathbf{g}_2 J = \{\mathbf{v}^{2n+1} | n \in \mathbb{Z}\}$, $\mathbf{g}_3 J = \{\mathbf{v}_0 \circ \mathbf{v}^{2n} | n \in \mathbb{Z}\}$, and $\mathbf{g}_4 J = \{\mathbf{v}_0 \circ \mathbf{v}^{2n+1} | n \in \mathbb{Z}\}$. Here the "$\circ$" operation is the one defined by equation (2.7.3). Clearly an arbitrary element $\mathbf{v}_0^j \circ \mathbf{v}^k$ of (a group isomorphic to) $\mathbb{Z}_2 \times \mathbb{Z}$ must be one of these 4 types depending upon the parity of j and k since $\mathbf{v}_0^2 = \mathbf{e}$. Then $G/J \cong \{\mathbf{g}_1 J = J, \mathbf{g}_2 J, \mathbf{g}_3 J, \mathbf{g}_4 J\}$. As these left cosets partition $\mathbb{Z}_2 \times \mathbb{Z}$ and each of these cosets is distinct, then the order of G/J is clearly 4 when $d > 0$. □

Definition 3.3.5. *If d is a fixed fundamental discriminant, we let φ_d denote the squaring map on $\mathcal{H}(d)$. We noted earlier in this Section that $\mathcal{A}(d) = \ker(\varphi_d)$ and we define $\mathcal{S}(d) = \operatorname{im}(\varphi_d)$, which is the set $\{\mathcal{C}^2 \mid \mathcal{C} \in \mathcal{H}(d)\}$ of all "square classes" in $\mathcal{H}(d)$ (note that $\mathcal{S}(d)$ is a normal subgroup of $\mathcal{H}(d)$ since $\mathcal{H}(d)$ is abelian).*

Proposition 3.3.6. *Let d be a fixed fundamental discriminant. If $\mathcal{H}(d)$, as a finite abelian group, has 2-rank equal to r, then $|\mathcal{A}(d)| = 2^r$.*

Proof: Clearly, if $h(d) = 1$ (the case when $\mathcal{H}(d)$ is the trivial group), then the 2-rank must be $r = 0$, so $|\mathcal{A}(d)| = 2^r = 2^0 = 1$ holds since $\mathcal{C}_0$ of order 1, the only class in $\mathcal{H}(d)$, is clearly ambiguous. Thus we assume that the order $h(d)$ of $\mathcal{H}(d)$ is $n > 1$ so that $\mathcal{H}(d)$ can be written (uniquely) in elementary divisor form by Theorem 2.6.3. Using the same notation as in Theorem 2.6.3, if we let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ be the unique factorization of n into powers of distinct primes using the FTA, then $\mathcal{H}(d) \cong$

$A_1 \times A_2 \times \cdots \times A_k$, where $|A_i| = p_i^{\alpha_i}$ and for each $A_i \in \{A_1, A_2, \ldots, A_k\}$ with $|A_i| = p_i^{\alpha_i}$, $A_i \cong \mathbb{Z}_{p_i^{\beta_{i,1}}} \times \mathbb{Z}_{p_i^{\beta_{i,2}}} \times \cdots \times \mathbb{Z}_{p_i^{\beta_{i,t_i}}}$ with $\beta_{i,1} \geq \beta_{i,2} \geq \cdots \geq \beta_{i,t_i} \geq 1$ and $\beta_{i,1} + \beta_{i,2} + \cdots + \beta_{i,t_i} = \alpha_i$. In particular, as the 2-rank equals r, there are exactly r component cyclic groups in the (fully expanded) direct product whose orders are positive powers of 2, namely, $A_1 \cong \mathbb{Z}_{2^{\beta_{1,1}}} \times \mathbb{Z}_{2^{\beta_{1,2}}} \times \cdots \times \mathbb{Z}_{2^{\beta_{1,r}}}$, provided r is nonzero. For each $1 \leq i \leq k$, let e_i be the identity element of A_i. Let us dispose of the case $r = 0$ first. In this case $|A_i|$ is odd for each $1 \leq i \leq k$. This means there is no element of order 2 in any of the A_i since the order of an element must divide the order of the group. In counting elements of $\mathcal{H}(d)$ of order 1 or 2, we see that $(e_1, e_2, \ldots, e_k)$ of order 1 is the only possible such element since any other coordinate $a_i \in A_i$ of this k-tuple, when squared, thus cannot be e_i. This means $|\mathcal{A}(d)| = 2^r = 2^0 = 1$ holds. When r is nonzero, we have $\mathcal{H}(d) \cong \mathbb{Z}_{2^{\beta_{1,1}}} \times \mathbb{Z}_{2^{\beta_{1,2}}} \times \cdots \times \mathbb{Z}_{2^{\beta_{1,r}}} \times A_2 \times \cdots \times A_k$. By Comment 3.3.2, each of the $\mathbb{Z}_{2^{\beta_{1,j}}}$ for $1 \leq j \leq r$ has exactly two elements of order 1 or 2, its identity e'_j and a generator g_j raised to the power $2^{\beta_{1,j}-1}$, respectively. Using a similar argument as before for the A_i, this time with $2 \leq i \leq k$, there is thus only one choice e_i for each of the $k-1$ coefficients of the $(r+k-1)$-tuple, but the first r coefficients now have exactly two choices each, e'_j and ${g_j}^{2^{\beta_{1,j}-1}}$. Therefore, there are exactly 2^r elements of $\mathcal{H}(d)$ which have order 1 or 2, completing the proof. □

Proposition 3.3.7. *If r is equal to the 2-rank of $\mathcal{H}(d)$, then the quotient group $\mathcal{H}(d)/\mathcal{S}(d)$ is isomorphic to $\mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$, with exactly r copies of $\mathbb{Z}_2$.*

Proof: As $\mathcal{S}(d)$ is the image of the squaring homomorphism φ_d, $\mathcal{S}(d)$ is a subgroup of $\mathcal{H}(d)$, and it is normal since it is a subgroup of an abelian group. This means it is legitimate to form the quotient group $\mathcal{H}(d)/\mathcal{S}(d)$. To determine the order of this quotient group, we begin by determining the order of a related quotient group,

$\mathcal{H}(d)/\mathcal{A}(d)$. As $\mathcal{A}(d)$ is the kernel of this same squaring map for which $\mathcal{S}(d)$ is the image, by the First Isomorphism Theorem (see [DF]) we have that $\mathcal{H}(d)/\mathcal{A}(d) \cong \mathcal{S}(d)$, so $|\mathcal{H}(d)/\mathcal{A}(d)| = |\mathcal{S}(d)|$. Thus $|\mathcal{H}(d)/\mathcal{A}(d)| = |\mathcal{H}(d)|/|\mathcal{A}(d)|$ implies that $|\mathcal{H}(d)/\mathcal{S}(d)| = |\mathcal{H}(d)|/|\mathcal{S}(d)| = |\mathcal{A}(d)|$. But $|\mathcal{A}(d)| = 2^r$ from Proposition 3.3.6, so we now know that $\mathcal{H}(d)/\mathcal{S}(d)$ is isomorphic to a finite abelian group of order 2^r.

Let $\mathcal{C} \in \mathcal{H}(d)$ be arbitrary so that $\mathcal{C}\mathcal{S}(d) \in \mathcal{H}(d)/\mathcal{S}(d)$. Then $\mathcal{C}\mathcal{S}(d) \cdot \mathcal{C}\mathcal{S}(d) = \mathcal{C}^2\mathcal{S}(d)$ by the definition of coset multiplication. As $\mathcal{C}^2 \in \mathcal{S}(d)$ (because $\mathcal{S}(d)$ contains the squares of all classes by definition), $\mathcal{C}^2\mathcal{S}(d) = \mathcal{S}(d)$. Since $\mathcal{C}\mathcal{S}(d)$ is an arbitrary element of $\mathcal{H}(d)/\mathcal{S}(d)$ and $\mathcal{C}\mathcal{S}(d)$ has order at most 2 by the above, $\mathcal{H}(d)/\mathcal{S}(d) \cong \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$, with exactly r copies of $\mathbb{Z}_2$, because all other finite abelian groups of order 2^r have an element of order greater than 2. (For completeness, note that if the 2-rank of $\mathcal{H}(d)$ is 0, then $\mathcal{H}(d)/\mathcal{S}(d)$ is isomorphic to the trivial group (of order $2^0 = 1$) and $\mathcal{S}(d) = \mathcal{H}(d)$ in this case.) □

We will prove in Chapter IV that the quotient group $\mathcal{H}(d)/\mathcal{S}(d)$ is isomorphic to the so-called "genus group" $\mathcal{G}(d)$ after having established the famous Duplication Theorem of Gauss. Proposition 3.3.7 then gives us the exact group structure of $\mathcal{G}(d)$.

We introduced ambiguous classes above and we now wish to define the related more concrete notion of a form being "ambiguous." In order to do this, it is expedient to work with a larger matrix group than $SL_2(\mathbb{Z})$.

Definition 3.3.8. *The set of all 2×2 matrices with integer entries having determinant equal to ± 1 is denoted by $GL_2(\mathbb{Z})$.*

It is easy to verify that $GL_2(\mathbb{Z})$ forms a nonabelian group under matrix multiplication which contains $SL_2(\mathbb{Z})$ as a proper subgroup. Let $\mathbf{I}_2$ denote the 2×2 identity matrix and let $-\mathbf{I}_2$ denote the matrix $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$.

Definition 3.3.9. *If $F = (a, b, c)$ is a form and $\mathbf{D} = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) \in GL_2(\mathbb{Z})$, then we define $F\mathbf{D}$ to be the form $G = (a_1, b_1, c_1)$, where $a_1, b_1,$ and c_1 are given by equations* (2.2.2), (2.2.3), *and* (2.2.4), *respectively.*

This Definition specializes to the same exact definition for $F\mathbf{D}$ as that given in Section 2.2 when $\mathbf{D}$ was restricted to being an element of $SL_2(\mathbb{Z})$. The exact argument used in the proof of Theorem 2.2.2 shows that the discriminant of G is equal to the discriminant of F. The following properties are easy to verify and will be used often in the sequel without further comment.

Proposition 3.3.10. *Let F be a form of fundamental discriminant d and let $\mathbf{D}$ and $\mathbf{E}$ be arbitrary elements in $GL_2(\mathbb{Z})$.*
(i) *If $F\mathbf{D} = G$, then the discriminant of G is equal to d.*
(ii) $F\mathbf{I}_2 = F$.
(iii) $(F\mathbf{D})\mathbf{E} = F(\mathbf{DE})$.

These properties may be summarized by saying that $GL_2(\mathbb{Z})$ induces a "right group action" on the set of all forms of discriminant d.

Everything needed to define an ambiguous form is now in place.

Definition 3.3.11. *A binary quadratic form F of fundamental discriminant d is "ambiguous" if there exists a matrix $\mathbf{D} \in GL_2(\mathbb{Z})$ such that $F\mathbf{D} = F$ and* $\det(\mathbf{D}) = -1$. *A matrix $\mathbf{D} \in GL_2(\mathbb{Z})$ having exactly these properties with respect to a fixed form F is called an "improper automorphism of F."*

Given our naming scheme, one would expect that ambiguous classes and ambiguous forms are somehow related to each other. This is indeed the case, as we now demonstrate.

Proposition 3.3.12. *A class $\mathcal{C} \in \mathcal{H}(d)$ is ambiguous if and only if it contains an ambiguous form. Indeed, a class $\mathcal{C} \in \mathcal{H}(d)$ either contains only ambiguous forms or no such forms at all.*

Proof: ($\Longrightarrow$) Suppose that $\mathcal{C} \in \mathcal{H}(d)$ is an ambiguous class. Then $\mathcal{C}$ has order 1 or order 2. In either case, $\mathcal{C}^2 = \mathcal{C}_0$, the principal class. This means that $\mathcal{C}$ is its own inverse. Let $(a,b,c) \in \mathcal{C}$. As was discussed in the proof of the existence of inverses in $\mathcal{H}(d)$, we thus have $(c,b,a) \in \mathcal{C}^{-1} = \mathcal{C}$. As $(a,b,c) \sim (c,b,a)$ there exists $\mathbf{E} \in SL_2(\mathbb{Z})$ such that $(c,b,a) = (a,b,c)\mathbf{E}$. Also $(c,b,a) = (a,b,c)\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, so $(a,b,c)\mathbf{E} = (a,b,c)\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Thus $(a,b,c)\mathbf{E}\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) = (a,b,c)\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) = (a,b,c)\mathbf{I}_2 = (a,b,c)$. Since $\mathbf{E}\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ is an element of $GL_2(\mathbb{Z})$ and $\det\left(\mathbf{E}\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)\right) = \det(\mathbf{E})\cdot\det\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) = 1\cdot(-1) = -1$, $\mathbf{E}\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ is an improper automorphism of (a,b,c), which means that (a,b,c) is an ambiguous form.

($\Longleftarrow$) Let $F = (a,b,c) \in \mathcal{C}$ be an ambiguous form. To show that $\mathcal{C}$ is an ambiguous class, it suffices to show that $\mathcal{C}^2 = \mathcal{C}_0$. As (a,b,c) is ambiguous, there exists an improper automorphism $\mathbf{D}$ so that $(a,b,c)\mathbf{D} = (a,b,c)$. We also have $(a,b,c)\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) = (c,b,a)$. This means that $(a,b,c)\mathbf{D}\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) = (a,b,c)\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) = (c,b,a)$. As $\det\left(\mathbf{D}\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)\right) = \det(\mathbf{D}) \cdot \det\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) = (-1)\cdot(-1) = 1$, $\mathbf{D}\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$, so $(a,b,c) \sim (c,b,a)$. As (a,b,c) and (c,b,a) are thus both elements of $\mathcal{C}$, it follows (again by comments in the proof of the existence of inverses in $\mathcal{H}(d)$), that $\mathcal{C}^2 = \mathcal{C}_0$. Therefore $\mathcal{C}$ is an ambiguous class.

The final statement of the proposition follows easily since a class that is not an ambiguous class must contain no ambiguous forms by what has already been proved. If, on the other hand, the class is ambiguous, the first part of the proof shows that every form in the class is ambiguous (since $(a,b,c) \in \mathcal{C}$ is completely arbitrary). $\square$

We have already found one way to count how many ambiguous classes there are in terms of the 2-rank r of $\mathcal{H}(d)$ (see Proposition 3.3.6). If t is the number of distinct prime divisors of the discriminant d, we mentioned earlier in this Section that $r = t - 1$ (the big and final result of this Section is a proof of this relationship). In order to relate $|\mathcal{A}(d)|$ to t, we will find it very useful to work with a special subset of ambiguous forms.

Definition 3.3.13. *A form F of fundamental discriminant d is "special ambiguous" if and only if either one of the following two conditions holds:*
(i) $F\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) = F$ *(equivalently, F is of the form $(a, 0, c)$), or*
(ii) $F\left(\begin{smallmatrix} 1 & 1 \\ 0 & -1 \end{smallmatrix}\right) = F$ *(equivalently, F is of the form (a, a, c)).*
Let Ω denote the set consisting of the two special matrices appearing in (i) *and* (ii).

Note that both matrices in Ω are members of $GL_2(\mathbb{Z})$ and have determinant equal to -1 and thus any special ambiguous form is clearly ambiguous. We also note that the principal form F_0 of discriminant d (see Definition 3.2.2) is special ambiguous.

As an illustration of Definition 3.3.13 and the results proved later in this Section, we now compute all special ambiguous forms of discriminant $d = 60$. Such forms of type $(a, 0, c)$ are easy to find since $d = -4ac = 60$ implies $ac = -15$. There are eight of these: $(1, 0, -15), (-1, 0, 15), (3, 0, -5), (-3, 0, 5), (5, 0, -3), (-5, 0, 3), (15, 0, -1)$, and $(-15, 0, 1)$. Finding the forms of type (a, a, c) is also easy since $d = a^2 - 4ac = a(a - 4c) = 60$ tells us that a (because it appears also as the b-coefficient) must be an even integer divisor of 60. There are also eight of this type: $(2, 2, -7), (-2, -2, 7)$, $(6, 6, -1), (-6, -6, 1), (10, 10, 1), (-10, -10, -1), (30, 30, 7)$, and $(-30, -30, -7)$. As $60 = 2^2 \cdot 3 \cdot 5$ and $60 \equiv 12 \pmod{16}$, Proposition 3.3.14 says there should be 2^3 special ambiguous forms of each of the two types, which we have confirmed in this example. Using the reduction theory described in Section 2.5, we find that these sixteen total special ambiguous forms are elements of the four classes in $\mathcal{H}(60)$ as follows: $(1, 0, -15), (-15, 0, 1), (-6, -6, 1), (10, 10, 1) \in [1, 8, 1]$, the principal class; $(-3, 0, 5), (5, 0, -3), (2, 2, -7), (-30, -30, -7) \in [2, 10, 5]$, the cycle of length 2; $(3, 0, -5), (-5, 0, 3), (-2, -2, 7), (30, 30, 7) \in [3, 12, 7]$, the cycle of length 3; and $(-1, 0, 15), (15, 0, -1), (6, 6, -1), (-10, -10, -1) \in [11, 18, 6]$, the cycle of length 6. As each class in $\mathcal{H}(60)$ contains special ambiguous forms, part (i) of Proposition 3.3.19 is certainly true in this example. Finally, since there are four special ambiguous forms in each class, this verifies part (ii) of Proposition 3.3.19.

It is also of interest to work out an example where $d < 0$. For $d = -84$, in looking for forms of type $(a, 0, c)$, we have $-4ac = -84$, so $ac = 21$. There are again eight: $(1, 0, 21), (-1, 0, -21), (3, 0, 7), (-3, 0, -7), (7, 0, 3), (-7, 0, -3), (21, 0, 1)$, and $(-21, 0, -1)$. Forms of type (a, a, c), since $a^2 - 4ac = a(a - 4c) = -84$ and a is an even divisor of the discriminant as before, include exactly the eight forms $(2, 2, 11), (-2, -2, -11), (6, 6, 5), (-6, -6, -5), (14, 14, 5), (-14, -14, -5), (42, 42, 11)$, and $(-42, -42, -11)$. As $-84 = -2^2 \cdot 3 \cdot 7$ and $-84 \equiv 12 \pmod{16}$, Proposition 3.3.14 says there should be 2^3 special ambiguous forms of each of the two types, which we have confirmed in this example also. Using the reduction theory described in Section 2.3 this time, we find that eight of these sixteen total special ambiguous forms are elements of the four classes in $\mathcal{H}(-84)$ as follows: $(1, 0, 21), (21, 0, 1) \in [1, 0, 21]$, the principal class; $(2, 2, 11), (42, 42, 11) \in [2, 2, 11]$; $(3, 0, 7), (7, 0, 3) \in [3, 0, 7]$; and $(6, 6, 5), (14, 14, 5) \in [5, 4, 5]$. The other eight, with negative a-coefficients, are negative definite forms and by definition are not elements of these classes of positive definite forms comprising the class group. As each class in $\mathcal{H}(-84)$ contains special ambiguous forms, part (i) of Proposition 3.3.19 is certainly true in this example also. Finally, since there are two special ambiguous forms in each class, this verifies part (ii) of Proposition 3.3.19.

It is clear from the above two examples that the set of special ambiguous forms of fixed discriminant d has only finitely many elements and we know that this set is nonempty since F_0 is special ambiguous. It is straightforward to extend the counts made in the two examples above to any given fundamental discriminant and the next result gives the answer in general.

Proposition 3.3.14. *The number of special ambiguous forms of fundamental discriminant d, broken down into the two different types, is given as in the table below, where t is the number of distinct prime divisors of d:*

d	$(a,0,c)$	(a,a,c)	Total
$d \equiv 1 \pmod 4$		2^{t+1}	2^{t+1}
$d \equiv 12 \pmod{16}$	2^t	2^t	2^{t+1}
$d \equiv 8 \pmod{16}$	2^{t+1}		2^{t+1}

Proof: First, we count the forms of fundamental discriminant d that are of type $(a,0,c)$. If d is odd, there are no forms of this type since the b-coefficient is 0, which is the opposite parity from d. Suppose that $d \equiv 0 \pmod 4$. Because $b = 0$ and d is a fundamental discriminant, $ac = -\frac{d}{4}$, where $\gcd(a,c) = 1$. As $\frac{d}{4}$ is square-free (since d is fundamental), let r be the number of necessarily distinct prime divisors of $\frac{d}{4}$. Then the number of choices for a is the number of subsets of this set of r primes, namely 2^r, times 2 (since the sign can be positive or negative), giving 2^{r+1}. As c is determined by the choice of a, the count of forms $(a,0,c)$ is also 2^{r+1}. If additionally $d \equiv 12 \pmod{16}$, then $r = t-1$ (because d is even) since all the prime factors of

$\frac{d}{4}$ are odd in this case, so the count is 2^t as desired. If additionally, instead, $d \equiv 8 \pmod{16}$, then $r = t$ since r includes the prime 2; hence the count here is 2^{t+1}, again as was to be shown.

Next, we count the forms of fundamental discriminant d that are of type (a, a, c). Suppose that d is odd. Any such form must have a such that $a \mid d$ since $d = a^2 - 4ac$, so let a be an arbitrary divisor of d. Then $d = ae$ for some $e \in \mathbb{Z}$. Hence $c = \frac{a^2-d}{4a} = \frac{a^2-ae}{4a}$. As $d = ae$ and $d \equiv 1 \pmod{4}$, either $a \equiv e \equiv 1 \pmod{4}$ or $a \equiv e \equiv 3 \pmod{4}$. In either case, $c = \frac{a-e}{4} \in \mathbb{Z}$. Thus the number of these forms is the number of (necessarily odd and square-free) divisors a of d of either sign. There are 2^{t+1} such divisors since d has t distinct (odd) prime divisors.

Suppose now that d is even. Because d is fundamental, (a, a, c) of discriminant d is primitive, so a is even (as it is the second coefficient which has the same parity as d) and c is odd. If $a = 2a'$, where a' is odd, then $d = a^2 - 4ac \equiv 12 \pmod{16}$. If, on the other hand, a' is assumed even, then $4 \mid a$ and $d = a^2 - 4ac \equiv 0 \pmod{32}$. However, this contradicts the fact that d is a fundamental discriminant since $\operatorname{ord}_2(d) \leq 3$ for all fundamental discriminants. Therefore, a' must be odd and there can be no forms of type (a, a, c) for an even fundamental discriminant d unless $d = a^2 - 4ac \equiv 12 \pmod{16}$.

So suppose further that $d \equiv 12 \pmod{16}$. We wish to count the forms $(2a', 2a', c)$ of discriminant d. (We know that c is odd.) As $\frac{d}{4a'} = a' - 2c$ is odd, a' is determined by its sign and its prime divisors, which may be any subset of the $t - 1$ necessarily odd prime divisors of $\frac{d}{4}$. There are 2^t altogether. □

We now need to establish several technical lemmas in order to be able to prove the final results of this Section.

Lemma 3.3.15. *If* $\mathbf{Y} = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) \in GL_2(\mathbb{Z})$ *is an improper automorphism of a form* F *of fundamental discriminant* d*, then* $r = -u$ *and* $\mathbf{Y}^2 = \mathbf{I}_2$*. Also, we have* $\mathbf{HYH} = \mathbf{Y}$ *for every* $\mathbf{H} \in Aut(F)$*.*

Proof: Let $\mathbf{Y}$ be an improper automorphism of such a form F. We have $ar^2 + brt + ct^2 = a$, so, after multiplying by u,

$$ar^2u + brtu + ct^2u = au. \tag{3.3.1}$$

By assumption $ru - st = -1$, so $st = ru + 1$. As $2ars + b(ru + st) + 2ctu = b$, thus $2ars + b(ru + ru + 1) + 2ctu = b$. Simplifying, $2ars + 2bru + 2ctu = 0$, so $ars + bru + ctu = 0$. Multiplying this last equation by t, then

$$arst + brtu + ct^2u = 0. \tag{3.3.2}$$

Subtracting equation (3.3.2) from equation (3.3.1), $ar^2u - arst = au$. As $a \neq 0$, $r^2u - rst = u$. This means $(ru - st)r = u$, so $(-1) \cdot r = u$ and $r = -u$ as desired. We then have $\mathbf{Y}^2 = \left(\begin{smallmatrix} -u & s \\ t & u \end{smallmatrix}\right)\left(\begin{smallmatrix} -u & s \\ t & u \end{smallmatrix}\right) = \begin{pmatrix} u^2+st & 0 \\ 0 & st+u^2 \end{pmatrix}$. But from above, $st = ru + 1$ implies $st = -u^2 + 1$, so $st + u^2 = 1$ and the product matrix is $\mathbf{I}_2$.

Now let $\mathbf{H} \in Aut(F)$ and let $\mathbf{Y}$ be an improper automorphism of F as before. Then $F\mathbf{H} = F$ and $F\mathbf{Y} = F$ by the definitions of automorphism and improper automorphism, so $F\mathbf{HY} = F\mathbf{Y} = F$. Also $\det(\mathbf{HY}) = -1$ as $\det(\mathbf{H}) = 1$ and $\det(\mathbf{Y}) = -1$. Hence $\mathbf{HY} \in GL_2(\mathbb{Z})$, so $\mathbf{HY}$ is an improper automorphism of F. By the first part of this proof, then $(\mathbf{HY})^2 = \mathbf{I}_2$. However, $(\mathbf{HY})(\mathbf{HY}) = \mathbf{I}_2$ implies $\mathbf{HYHYY} = \mathbf{Y}$, which, since $\mathbf{YY} = \mathbf{I}_2$, gives us $\mathbf{HYH} = \mathbf{Y}$ as desired. □

Lemma 3.3.16. *There does not exist a matrix* $\mathbf{C} \in GL_2(\mathbb{Z})$ *such that* $\mathbf{C}^{-1} \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \mathbf{C} = \left(\begin{smallmatrix} 1 & 1 \\ 0 & -1 \end{smallmatrix}\right)$.

Proof: Suppose that $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{Z})$ is such that $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)^{-1} \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & -1 \end{smallmatrix}\right)$. Using the well-known fact that for any invertible matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, its inverse is $\frac{1}{ad-bc} \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$, we have $\frac{1}{\pm 1} \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right) \left(\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\right) = \left(\begin{smallmatrix} \pm d & \mp b \\ \mp c & \pm a \end{smallmatrix}\right) \left(\begin{smallmatrix} a & b \\ -c & -d \end{smallmatrix}\right) = \left(\begin{smallmatrix} \pm(ad+bc) & \pm 2bd \\ \mp 2ac & \mp(ad+bc) \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & -1 \end{smallmatrix}\right)$. In particular, $\pm 2bd = 1$. This is a contradiction, however, since b and d are integers, so there can be no such matrix. □

Lemma 3.3.17. *If* $\mathbf{U} \in SL_2(\mathbb{Z})$ *commutes with either matrix in the set* Ω*, then* $\mathbf{U} = \pm \mathbf{I}_2$.

Proof: First, suppose that $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ commutes with $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. Then $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & -b \\ c & -d \end{smallmatrix}\right)$, which equals $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & b \\ -c & -d \end{smallmatrix}\right)$. Thus $b = -b$ and $c = -c$, so $b = c = 0$. As $\left|\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right| = ad - bc = ad = 1$, then either $a = d = 1$ or $a = d = -1$, so $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \pm \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Next, suppose that $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ commutes with $\left(\begin{smallmatrix} 1 & 1 \\ 0 & -1 \end{smallmatrix}\right)$. Then $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 & 1 \\ 0 & -1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & a-b \\ c & c-d \end{smallmatrix}\right)$, which equals $\left(\begin{smallmatrix} 1 & 1 \\ 0 & -1 \end{smallmatrix}\right) \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} a+c & b+d \\ -c & -d \end{smallmatrix}\right)$. Thus again $c = -c$ implies $c = 0$. We also have $a - b = b + d$. By the same argument as above, $a = d$ $(= \pm 1)$, so we find that $-b = b$, which again implies $b = 0$. We conclude that here also $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \pm \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. □

Lemma 3.3.18. *Let* $\mathbf{D} \in GL_2(\mathbb{Z})$ *be such that* $\det(\mathbf{D}) = -1$ *and* $\mathbf{D}^2 = \mathbf{I}_2$*. Then there exists* $\mathbf{U} \in SL_2(\mathbb{Z})$ *such that* $\mathbf{U}^{-1}\mathbf{D}\mathbf{U}$ *is equal to one of the two matrices in the set* Ω*.*

Proof: Let $\mathbb{Z}^2$ denote the set of all 2 entry column vectors $\left(\begin{smallmatrix} a_1 \\ a_2 \end{smallmatrix}\right)$ with $a_1, a_2 \in \mathbb{Z}$. Note that $\mathbf{Da} \in \mathbb{Z}^2$ if $\mathbf{a} \in \mathbb{Z}^2$, where $\mathbf{Da}$ denotes the usual product of matrices. Assume that $\mathbf{D} = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$. We claim there exists a vector $\mathbf{w} = \binom{w_1}{w_2} \in \mathbb{Z}^2$ such that $\mathbf{Dw} \neq -\mathbf{w}$. Assume on the contrary that $\mathbf{Dw} = -\mathbf{w}$ for all $\mathbf{w} \in \mathbb{Z}^2$. Then $rw_1 + sw_2 = -w_1$ and $tw_1 + uw_2 = -w_2$ for all $w_1, w_2 \in \mathbb{Z}$. Plugging in $\mathbf{w} = \binom{1}{0}$ tells us that $r = -1$ and $t = 0$ and plugging in $\mathbf{w} = \binom{0}{1}$ tells us that $s = 0$ and $u = -1$, which gives a contradiction since $\det\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) = 1$ and not -1. Let $\mathbf{w} \in \mathbb{Z}^2$ be a (necessarily nonzero) vector such that $\mathbf{Dw} \neq -\mathbf{w}$; note that $\mathbf{Dw} + \mathbf{w}$ is a nonzero vector in $\mathbb{Z}^2$ and set $\mathbf{e} = \binom{e_1}{e_2} = \mathbf{Dw}+\mathbf{w}$. We have $\mathbf{De} = \mathbf{D}^2\mathbf{w}+\mathbf{Dw} = \mathbf{w}+\mathbf{Dw} = \mathbf{e}$ since $\mathbf{D}^2 = \mathbf{I}_2$. If $c = \gcd(e_1, e_2)$, then $\mathbf{e} = \binom{ca_1}{ca_2}$, where $\gcd(a_1, a_2) = 1$. We finally set $\mathbf{a} = \binom{a_1}{a_2}$ and note that $\mathbf{a}$ is a nonzero vector in $\mathbb{Z}^2$, it satisfies $\mathbf{Da} = \mathbf{a}$, and $\gcd(a_1, a_2) = 1$. Using Theorem 1.1.3, choose $b_1, b_2 \in \mathbb{Z}$ such that $a_1b_2 - a_2b_1 = 1$ and set $\mathbf{b} = \binom{b_1}{b_2}$. Any element $\binom{x}{y} \in \mathbb{Z}^2$ can be written in the form $j_1\mathbf{a}+j_2\mathbf{b}$ for a uniquely determined pair of integers $j_1, j_2 \in \mathbb{Z}$ by solving the linear system $j_1a_1 + j_2b_1 = x$, $j_1a_2 + j_2b_2 = y$. We then have $\mathbf{Db} = j_1\mathbf{a} + j_2\mathbf{b}$ for some $j_1, j_2 \in \mathbb{Z}$. Applying $\mathbf{D}$ from the left on both sides leads to $\mathbf{D}^2\mathbf{b} = \mathbf{b} = j_1(1 + j_2)\mathbf{a} + j_2^2\mathbf{b}$, so $j_1(1 + j_2) = 0$ and $j_2^2 = 1$. If $j_2 = 1$, then $j_1 = 0$. We now show that this solution, tantamount to $\mathbf{Db} = \mathbf{b}$, leads to a contradiction. Combining $\mathbf{Da} = \mathbf{a}$ with $\mathbf{Db} = \mathbf{b}$ leads to the matrix equation $\mathbf{D}\left(\begin{smallmatrix} a_1 & b_1 \\ a_2 & b_2 \end{smallmatrix}\right) = \left(\begin{smallmatrix} a_1 & b_1 \\ a_2 & b_2 \end{smallmatrix}\right)$. Taking determinants of both sides leads to $(-1)(1) = 1$, a contradiction. Therefore, $\mathbf{Db} = j\mathbf{a}-\mathbf{b}$ for some uniquely determined $j \in \mathbb{Z}$. We may now choose $n \in \mathbb{Z}$ uniquely such that $j + 2n = 0$ or 1, depending on the parity of j, and we set $\mathbf{c} = \binom{c_1}{c_2} = n\mathbf{a} + \mathbf{b} = \binom{na_1+b_1}{na_2+b_2}$. We define $\mathbf{U} = \left(\begin{smallmatrix} a_1 & c_1 \\ a_2 & c_2 \end{smallmatrix}\right)$ and note that $\mathbf{U} \in SL_2(\mathbb{Z})$. Computing $\mathbf{Dc}$, we find that $\mathbf{Dc} = (j+2n)\mathbf{a}-\mathbf{c} = v\mathbf{a}-\mathbf{c}$, where $v = 0$ or 1. A straightforward matrix computation yields the equation $\mathbf{DU} = \mathbf{U}\left(\begin{smallmatrix} 1 & v \\ 0 & -1 \end{smallmatrix}\right)$, from which the final statement of the Theorem follows immediately upon multiplication on the left by $\mathbf{U}^{-1}$. □

Proposition 3.3.19. *Let d be a fundamental discriminant.*

(i) *Every equivalence class of forms of discriminant d that contains an ambiguous form must contain at least one special ambiguous form.*

(ii) *Every ambiguous class in $\mathcal{H}(d)$ contains exactly the same number of special ambiguous forms. That number is 2 if $d < 0$ and 4 if $d > 0$.*

Proof: (i) Let $\mathcal{C}$ be a class of forms of fundamental discriminant d and let $F \in \mathcal{C}$ be an ambiguous form. Then by Definition 3.3.11 there exists a matrix $\mathbf{D} \in GL_2(\mathbb{Z})$ such that $F\mathbf{D} = F$ and $\det(\mathbf{D}) = -1$. By Lemma 3.3.15, $\mathbf{D}^2 = \mathbf{I}_2$, so by Lemma 3.3.18, there exists $\mathbf{S} \in SL_2(\mathbb{Z})$ such that $\mathbf{S}^{-1}\mathbf{D}\mathbf{S} \in \Omega$. Then the form $F\mathbf{S} \in \mathcal{C}$ is special ambiguous by Definition 3.3.13 because $F\mathbf{S} \cdot \mathbf{S}^{-1}\mathbf{D}\mathbf{S} = (F\mathbf{D})\mathbf{S} = F\mathbf{S}$.

(ii) Let d be a fundamental discriminant and let $\mathcal{C} \in \mathcal{H}(d)$ be an ambiguous class. Then there exists an ambiguous form $F \in \mathcal{C}$ by Proposition 3.3.12. Let $J = \{\mathbf{E}^2 \mid \mathbf{E} \in Aut(F)\}$. By Lemma 3.3.4 $|Aut(F)/J| = 2$ if $d < 0$ and $|Aut(F)/J| = 4$ if $d > 0$. Thus we only need to demonstrate that the number of special ambiguous forms in $\mathcal{C}$ is equal to $|Aut(F)/J|$.

Let $\mathbf{Y}$ be a fixed improper automorphism of F. Let $\mathbf{E} \in Aut(F)$. As $\mathbf{YE}$ is an improper automorphism of F (because $\det(\mathbf{Y}) = -1$ and $\det(\mathbf{E}) = 1$), by Lemma 3.3.18 there exists $\mathbf{T} \in SL_2(\mathbb{Z})$ such that $\mathbf{A} = \mathbf{T}^{-1}\mathbf{YET} \in \Omega$. The form $F\mathbf{T}$ is a special ambiguous form in $\mathcal{C}$ by the same argument as in part (i). If also $\mathbf{S} \in SL_2(\mathbb{Z})$ with $\mathbf{B} = \mathbf{S}^{-1}\mathbf{YES} \in \Omega$, then by Lemma 3.3.16, it must be the case that $\mathbf{A} = \mathbf{B}$. (Otherwise, if we had $\mathbf{A} \neq \mathbf{B}$, then we could assume without loss of generality that $\mathbf{A} = \left(\begin{smallmatrix} 1 & 1 \\ 0 & -1 \end{smallmatrix}\right)$ and $\mathbf{B} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ (by swapping the names if necessary). Since $\mathbf{YE} = \mathbf{SBS}^{-1}$, we have $\mathbf{A} = \mathbf{T}^{-1}(\mathbf{SBS}^{-1})\mathbf{T} = (\mathbf{T}^{-1}\mathbf{S})\mathbf{B}(\mathbf{S}^{-1}\mathbf{T})$, which is a contradiction of Lemma 3.3.16 because $\mathbf{T}^{-1}\mathbf{S} = (\mathbf{S}^{-1}\mathbf{T})^{-1}$ and $\mathbf{S}^{-1}\mathbf{T} \in GL_2(\mathbb{Z})$ since $\mathbf{S}, \mathbf{T} \in SL_2(\mathbb{Z})$

and $SL_2(\mathbb{Z}) \subset GL_2(\mathbb{Z})$.) Therefore $(\mathbf{T}^{-1}\mathbf{S})^{-1} \cdot \mathbf{A} \cdot \mathbf{T}^{-1}\mathbf{S} = \mathbf{S}^{-1}\mathbf{YES} = \mathbf{B} = \mathbf{A}$, which follows since $\mathbf{YE} = \mathbf{TAT}^{-1}$. Thus, $\mathbf{A}(\mathbf{T}^{-1}\mathbf{S}) = (\mathbf{T}^{-1}\mathbf{S})\mathbf{A}$, and since $\mathbf{T}^{-1}\mathbf{S} \in SL_2(\mathbb{Z})$, by Lemma 3.3.17, we have that $\mathbf{T}^{-1}\mathbf{S} = \pm\mathbf{I}_2$. Hence $\mathbf{S} = \pm\mathbf{T}$, which means that $F\mathbf{T} = F\mathbf{S}$. This proves that the function ρ from $Aut(F)$ to the set of special ambiguous forms in $\mathcal{C}$ defined by $\rho(\mathbf{E}) = F\mathbf{T}$ is, in fact, well-defined.

We claim that the function ρ is surjective. To see this, let $G \in \mathcal{C}$ be a special ambiguous form. Then there exists $\mathbf{A} \in \Omega$ such that $G\mathbf{A} = G$. Let $\mathbf{T} \in SL_2(\mathbb{Z})$ with $F\mathbf{T} = G$. Then, for $\mathbf{E} = \mathbf{Y}^{-1}\mathbf{TAT}^{-1}$, we have $\rho(\mathbf{E}) = F\mathbf{T} = G$.

We claim that the function ρ is constant on cosets of J. To see this, let $\mathbf{E}, \mathbf{H} \in Aut(F)$. Let $\mathbf{T} \in SL_2(\mathbb{Z})$ be such that $\mathbf{A} = \mathbf{T}^{-1}\mathbf{YET} \in \Omega$ so that $\rho(\mathbf{E}) = F\mathbf{T}$. Note that $\mathbf{YE}$ is an improper automorphism of F (since $F\mathbf{Y} = F$ and $F\mathbf{E} = F$ imply $F\mathbf{YE} = F$ and since $\det(\mathbf{YE}) = -1$). Therefore, by Lemma 3.3.15, we have $\mathbf{HYEH} = \mathbf{YE}$, and so $\mathbf{A} = \mathbf{T}^{-1}\mathbf{HYEHT}$. Furthermore, $\mathbf{A} = \mathbf{T}^{-1}\mathbf{HYEHHH}^{-1}\mathbf{T} = (\mathbf{H}^{-1}\mathbf{T})^{-1}\mathbf{YEH}^2(\mathbf{H}^{-1}\mathbf{T})$, where $\mathbf{EH}^2 \in Aut(F)$ and $\mathbf{H}^{-1}\mathbf{T} \in SL_2(\mathbb{Z})$. Therefore, $\rho(\mathbf{EH}^2) = F\mathbf{H}^{-1}\mathbf{T}$ by the definition of ρ. However, as $\mathbf{H}^{-1} \in Aut(F)$, we see that $F\mathbf{H}^{-1}\mathbf{T} = F\mathbf{T}$, which demonstrates that $\rho(\mathbf{EH}^2) = \rho(\mathbf{E})$ as was to be shown.

We claim that the function ρ is also injective on cosets of J. Let $\mathbf{E}, \mathbf{H} \in Aut(F)$ be such that $\rho(\mathbf{E}) = \rho(\mathbf{H})$. Let $\mathbf{T}, \mathbf{S} \in SL_2(\mathbb{Z})$ be such that $\mathbf{A} = \mathbf{T}^{-1}\mathbf{YET}$, $\mathbf{B} = \mathbf{S}^{-1}\mathbf{YHS}$, and $\mathbf{A}, \mathbf{B} \in \Omega$. $\mathbf{A}$ is an improper automorphism of $\rho(\mathbf{E})$ as $\rho(\mathbf{E}) = F\mathbf{T}$ and $F\mathbf{TA} = F\mathbf{T}(\mathbf{T}^{-1}\mathbf{YET}) = F\mathbf{YET} = F\mathbf{T}$ (since, again, $\mathbf{YE}$ is an improper automorphism of F). An entirely similar argument shows that $\mathbf{B}$ is an improper automorphism of $\rho(\mathbf{E}) = \rho(\mathbf{H}) = F\mathbf{S}$. Since no (special ambiguous) form of fundamental discriminant can have both $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 1 \\ 0 & -1 \end{smallmatrix}\right)$ as improper automorphisms (see Definition 3.3.13), necessarily $\mathbf{A} = \mathbf{B}$. This gives $\mathbf{T}^{-1}\mathbf{YET} = \mathbf{S}^{-1}\mathbf{YHS}$, which implies that $\mathbf{E} = \mathbf{Y}^{-1}(\mathbf{TS}^{-1})\mathbf{YH}(\mathbf{ST}^{-1})$. As $F\mathbf{T} = F\mathbf{S}$ implies that $F\mathbf{ST}^{-1} = F$, then $\mathbf{ST}^{-1} \in Aut(F)$. By both parts of Lemma 3.3.15, we have (since $\mathbf{Y}^2 = \mathbf{I}_2$) that $\mathbf{Y}^{-1} = \mathbf{Y}$ is an improper automorphism of F and $\mathbf{Y}^{-1} = (\mathbf{ST}^{-1})\mathbf{Y}^{-1}(\mathbf{ST}^{-1})$, so $\mathbf{E} = (\mathbf{ST}^{-1})\mathbf{Y}^{-1}(\mathbf{ST}^{-1})(\mathbf{TS}^{-1})\mathbf{YH}(\mathbf{ST}^{-1}) = (\mathbf{ST}^{-1})\mathbf{H}(\mathbf{ST}^{-1})$. But $Aut(F)$ is abelian, so $\mathbf{E} = \mathbf{H}(\mathbf{ST}^{-1})^2$, where $(\mathbf{ST}^{-1})^2 \in J$. Therefore $\mathbf{E}$ and $\mathbf{H}$ are in the same J-coset of $Aut(F)$.

The function ρ is therefore a bijection from $Aut(F)/J$, the set of cosets of J in $Aut(F)$, onto the set of special ambiguous forms in $\mathcal{C}$. As the number of elements in each set is thus the same, this proves the desired result by use of Lemma 3.3.4 as mentioned above. □

Theorem 3.3.20. *If t is the number of distinct prime divisors of the fundamental discriminant d, then $|\mathcal{A}(d)| = 2^{t-1}$. Combined with Proposition 3.3.6, we conclude that $r = t - 1$.*

Proof: Let t and d be as stated above. To determine $|\mathcal{A}(d)|$, the number of ambiguous classes in $\mathcal{H}(d)$, we use Proposition 3.3.19(ii) which says that every ambiguous class contains the same number of special ambiguous forms, namely 2 if $d < 0$ and 4 if $d > 0$. By Proposition 3.3.14 we know that there are 2^{t+1} special ambiguous forms of fundamental discriminant d (regardless of d's sign). If $d > 0$, since each of the 2^{t+1} special ambiguous forms is in some class in $\mathcal{H}(d)$, we only need to divide 2^{t+1} by $4 = 2^2$ to find that there are $2^{t+1-2} = 2^{t-1}$ ambiguous classes. If $d < 0$, we must remember that only half of the 2^{t+1} special ambiguous forms, i.e. 2^t, are each in some class in $\mathcal{H}(d)$ because, by definition, the class group only includes classes containing positive definite forms (with the equinumerous negative definite forms excluded). Hence in this case we find there are $2^t/2 = 2^{t-1}$ ambiguous classes also, so $|\mathcal{A}(d)| = 2^{t-1}$.

Finally, under the assumption and result of Proposition 3.3.6 that if $\mathcal{H}(d)$ has 2-rank equal to r, then $|\mathcal{A}(d)| = 2^r$, we conclude that $2^r = 2^{t-1}$, giving $r = t - 1$. □

CHAPTER IV

GENUS THEORY

4.1 Dirichlet Characters and the Kronecker Symbol

Before we can define and discuss the notion of *genus* (plural, *genera*) in detail, the concept of "character" must be introduced. The characters we use are based upon a special symbol named in honor of Kronecker that is related to the Legendre symbol introduced in Section 1.1. Our source for this section was [Ta2].

A famous theorem in Number Theory, first proved by Dirichlet around 1840, states that if a and m are positive integers that are relatively prime then the arithmetic sequence $\{a+km \mid k \in \mathbb{Z}^{\geq 0}\}$ contains an infinite number of prime numbers. Dirichlet's proof uses analysis in a crucial way and certain number-theoretic functions called "Dirichlet characters" that are interesting in their own right.

Definition 4.1.1. *A complex-valued function $\psi : \mathbb{Z}^+ \to \mathbb{C}$ is said to be a "Dirichlet character modulo m" (m is a fixed positive integer; a and b below are arbitrary positive integers) if*

(a)

$$\psi(a) \begin{cases} = 0 & \textit{if } \gcd(a,m) \neq 1 \\ \neq 0 & \textit{if } \gcd(a,m) = 1. \end{cases}$$

(b) *If $a \equiv b \pmod{m}$, then $\psi(a) = \psi(b)$.*

(c) $\psi(ab) = \psi(a)\psi(b)$.

A simple example, when $m = 2$, is the following:

a	1	2	3	4	5	6	7	8	...
$\psi(a) =$	1	0	1	0	1	0	1	0	

For obvious reasons, this particular character is called the "trivial character modulo 2." If a Dirichlet character ψ takes on a single value other than 0 and 1 we say that it is a "nontrivial character." Given a fundamental discriminant $d \in \mathbb{Z}$, we will define a corresponding function $\chi_d : \mathbb{Z}^+ \to \{-1, 0, 1\}$ known as the "Kronecker symbol with respect to d" and show that χ_d is a nontrivial Dirichlet character modulo $|d|$.

Throughout the remainder of this Section, we will rely heavily upon several important properties of the Jacobi symbol (see Section 1.1 for the definition of this symbol). For the convenience of the reader, we collect here all of the properties of the Jacobi symbol used throughout this Section. For proofs of all of these properties, we refer the reader to Landau's book [La].

Theorem 4.1.2. *Let m and n be fixed odd positive integers and let $a, b \in \mathbb{Z}$.*
(a) *If $a \equiv b \pmod m$ and $\gcd(a, m) = 1$, then $(\frac{a}{m}) = (\frac{b}{m})$.*
(b) *If $\gcd(a, m) = \gcd(a, n) = 1$, then $(\frac{a}{m})(\frac{a}{n}) = (\frac{a}{mn})$.*
(c) *If $\gcd(a, m) = \gcd(b, m) = 1$, then $(\frac{ab}{m}) = (\frac{a}{m})(\frac{b}{m})$.*
(d) *$(\frac{-1}{m}) = (-1)^{(m-1)/2}$.*
(e) *$(\frac{2}{m}) = (-1)^{(m^2-1)/8}$.*

The similarities of these properties with the corresponding properties of the Legendre symbol are quite striking: 4.1.2(a) generalizes 1.1.13(i), 4.1.2(c) generalizes 1.1.13(iii), and (d) and (e) here extend parts (i) and (ii), respectively, of the QRL.

Property 4.1.2(b) has no analogue to any property of the Legendre symbol. The added flexibility of the Jacobi symbol makes it easier to work with than the Legendre symbol, both theoretically and numerically. Finally, part (iii) of the QRL may also be generalized to the Jacobi symbol.

Theorem 4.1.3. *Assume $m, n \in \mathbb{Z}$ are odd and relatively prime. Then*

$$\left(\frac{m}{|n|}\right)\left(\frac{n}{|m|}\right) = \begin{cases} -(-1)^{[(m-1)(n-1)]/4} & \textit{if } m < 0 \textit{ and } n < 0, \\ (-1)^{[(m-1)(n-1)]/4} & \textit{otherwise.} \end{cases}$$

Let d be a fixed fundamental discriminant throughout the following discussion. Our first goal is to define a function χ_d on the positive integers that takes on only three values: $-1, 0,$ and 1. The strategy is simple: We set $\chi_d(1) = 1$ and then uniquely specify χ_d at every prime number p. Once that is done, we extend the function χ_d to all positive integers multiplicatively using the Fundamental Theorem of Arithmetic. For example, if $\chi_d(3) = 1$ and $\chi_d(7) = -1$, then we define $\chi_d(21) = \chi_d(3 \cdot 7) := \chi_d(3) \cdot \chi_d(7) = (1)(-1) = -1$. The method for defining χ_d at the prime numbers $p \geq 2$ is the following:

Definition 4.1.4. $p = 2:$ $\quad \chi_d(2) = 0$ *if* $2 \mid d$*, or equivalently, if* $d \equiv 0 \pmod 4$.

$$\chi_d(2) = \begin{cases} 1 & \textit{if } d \equiv 1 \pmod 8 \\ -1 & \textit{if } d \equiv 5 \pmod 8. \end{cases}$$

Since $d \equiv 0$ or $1 \pmod 4$, this covers all possibilities. If d is odd, then the Jacobi symbol $\left(\frac{2}{|d|}\right)$ is defined since $|d|$ is a positive odd integer and $\gcd(2, |d|) = 1$, and we have

$$\chi_d(2) = \left(\frac{2}{|d|}\right) = (-1)^{(|d|^2-1)/8}. \tag{4.1.1}$$

The second equality here is just Theorem 4.1.2(e). If $d \equiv 1 \pmod 8$, then $|d| \equiv 1$ or $7 \pmod 8$ and the expression $\frac{(|d|^2-1)}{8}$ is even, which verifies the first equality in (4.1.1) when $d \equiv 1 \pmod 8$. If $d \equiv 5 \pmod 8$, then $|d| \equiv 3$ or $5 \pmod 8$ and the expression $\frac{(|d|^2-1)}{8}$ is odd, which completes the proof of the first equality in (4.1.1).

Definition 4.1.5. *p = odd prime:* $\quad \chi_d(p) = 0$ *if $p \mid d$.*

$$\chi_d(p) = \left(\tfrac{d}{p}\right) \text{ (}\leftarrow \textit{Legendre symbol) if } p \nmid d.$$

Definition 4.1.6. *If $a \geq 2$ and $a = \prod_{j=1}^{t} p_j$ is the unique factorization of a into a product of primes, then we define*

$$\chi_d(a) = \prod_{j=1}^{t} \chi_d(p_j), \tag{4.1.2}$$

which gives χ_d as a uniquely defined function on all of $\mathbb{Z}^+$.

Given that χ_d takes on values of only $0, 1$, and -1 on the primes, it is clear that the range of the function χ_d is $\{-1, 0, 1\}$. We illustrate these ideas with a specific example.

Example 4.1.7. $d = 60$.

$\chi_{60}(1) = 1$.

$\chi_{60}(2) = 0$ since d is even.

$\chi_{60}(3) = 0$ since $3 \,|\, 60$.

$\chi_{60}(4) = \chi_{60}(2) \cdot \chi_{60}(2) = 0$ (it should be clear that $\chi_d(a) = 0$ for all even $a \in \mathbb{Z}^+$).

$\chi_{60}(5) = 0$ since $5 \,|\, 60$.

$\chi_{60}(6) = 0$.

$\chi_{60}(7) = 1$ since $60 \equiv 4 \pmod 7$ and $\left(\frac{4}{7}\right) = 1$.

$\chi_{60}(8) = 0$.

$\chi_{60}(9) = \chi_{60}(3) \cdot \chi_{60}(3) = 0$.

$\chi_{60}(10) = 0$.

$\chi_{60}(11) = 1$ since $60 \equiv 5 \pmod{11}$ and $\left(\frac{5}{11}\right) = 1$.

$\chi_{60}(12) = 0$.

$\chi_{60}(13) = -1$ since $60 \equiv 8 \pmod{13}$ and $\left(\frac{8}{13}\right) = -1$.

$\vdots$

From this example, it should be clear in general that if $a \geq 2$ and $\gcd(a, d) \neq 1$, i.e. there is at least one prime $p \geq 2$ such that $p \,|\, a$ and $p \,|\, d$, then $\chi_d(a) = 0$. If $a \geq 1$ and $\gcd(a, d) = 1$, then it should also be clear that $\chi_d(a) = 1$ or -1 and in particular is nonzero. We now summarize these observations.

Theorem 4.1.8. *The function* $\chi_d : \mathbb{Z}^+ \to \{-1, 0, 1\}$ *satisfies part* (*a*) *of Definition* 4.1.1 *for being a Dirichlet character modulo* $|d|$ (*of course,* $\gcd(a, d) = \gcd(a, |d|)$ *for all* $a \in \mathbb{Z}^+$).

Recall that the Jacobi symbol $\left(\frac{d}{1}\right)$ is defined to be equal to 1, and $\chi_d(1) = 1$ by definition, so $\chi_d(1) = \left(\frac{d}{1}\right)$. We now verify that $\chi_d(a)$ is equal to the Jacobi symbol

$\left(\frac{d}{a}\right)$ whenever $a > 1$ is an odd integer and $\gcd(a, d) = 1$ (note that this Jacobi symbol is only defined under these circumstances). In this case, the prime factorization $a = \prod_{j=1}^{t} p_j$ is such that none of the p_j divide d. The Jacobi symbol $\left(\frac{d}{a}\right)$ is then defined by

$$\left(\frac{d}{a}\right) = \prod_{j=1}^{t} \left(\frac{d}{p_j}\right) \tag{4.1.3}$$

(since a is odd, each p_j is an odd prime and all symbols on the right side of (4.1.3) are Legendre symbols). Since p_j is odd and $p_j \nmid d$ for $j = 1, \ldots, t$, we have $\chi_d(p_j) = \left(\frac{d}{p_j}\right)$ (Legendre symbol) for $j = 1, \ldots, t$ and we conclude by equation (4.1.2) that

$$\chi_d(a) = \left(\frac{d}{a}\right) \tag{4.1.4}$$

when $a \geq 1$ is odd and $\gcd(a, d) = 1$.

Theorem 4.1.9. *If $a, b \in \mathbb{Z}^+$ are arbitrary positive integers, then*

$$\chi_d(ab) = \chi_d(a)\chi_d(b), \tag{4.1.5}$$

namely, χ_d satisfies part (c) *of Definition* 4.1.1 *for being a Dirichlet character modulo* $|d|$.

Proof: This statement is obvious if either a or b is $= 1$ so we assume that $a, b \geq 2$. Write $a = \prod_{j=1}^{t} p_j$ and $b = \prod_{k=1}^{r} q_k$ in terms of their unique factorizations into primes. Then by equation (4.1.2) we obtain

$$\chi_d(ab) = \chi_d(\prod_{j=1}^{t} p_j \prod_{k=1}^{r} q_k) = \prod_{j=1}^{t} \chi_d(p_j) \cdot \prod_{k=1}^{r} \chi_d(q_k) = \chi_d(a)\chi_d(b). \qquad \square$$

We set $m = |d| \geq 3$ throughout the rest of this section.

Theorem 4.1.10. *If $a \in \mathbb{Z}^+$ and $\gcd(a, d) = 1$, then*

i) *for d odd, we have*

$$\chi_d(a) = \left(\frac{a}{m}\right) (\leftarrow \textit{Jacobi symbol});$$

ii) *for d even, if 2 goes into d exactly c times, so that $d = 2^c u$ and u is odd, and if we set $v = |u|$, then*

$$\chi_d(a) = \left(\frac{2}{a}\right)^c (-1)^{\frac{(u-1)}{2} \cdot \frac{(a-1)}{2}} \left(\frac{a}{v}\right)$$

(*note that a must be odd here since d is even and* $\gcd(a, d) = 1$*; both symbols on the right side here are Jacobi symbols*).

Before we prove Theorem 4.1.10, we note that all that remains to prove that χ_d is a Dirichlet character modulo m is that part (b) of Definition 4.1.1 holds, namely,

Theorem 4.1.11. *If $a, b \in \mathbb{Z}^+$ are such that $a \equiv b \pmod{m}$, then*

$$\chi_d(a) = \chi_d(b). \tag{4.1.6}$$

We will assume Theorem 4.1.10 holds and show that Theorem 4.1.11 follows as a corollary of it. After completing the proof of Theorem 4.1.11, we will return to the proof of Theorem 4.1.10.

Proof of Theorem 4.1.11 based upon Theorem 4.1.10:

If $\gcd(a, d) = \gcd(a, m) > 1$, then $\gcd(b, d) > 1$ since $a \equiv b \pmod{m}$ and so $\chi_d(a) = 0 = \chi_d(b)$, verifying (4.1.6) in this case. We will assume for the remainder of the proof that $\gcd(a, d) = \gcd(a, m) = 1$ and so $\gcd(b, d) = 1$ since $a \equiv b \pmod{m}$. In this case, both $\chi_d(a)$ and $\chi_d(b)$ are nonzero (actually either 1 or -1). There are two cases.

Case 1: Assume d is odd so that $d \equiv 1 \pmod{4}$. We have $\chi_d(a) = \left(\frac{a}{m}\right) = \left(\frac{b}{m}\right) = \chi_d(b)$, with the first and third equalities holding by part i) of Theorem 4.1.10 and the second equality holding by Theorem 4.1.2(a).

Case 2: Assume d is even so that $d \equiv 0 \pmod{4}$. By part ii) of Theorem 4.1.10, we have

$\chi_d(a) = \left(\frac{2}{a}\right)^c (-1)^{\frac{(u-1)}{2} \cdot \frac{(a-1)}{2}} \left(\frac{a}{v}\right)$ and $\chi_d(b) = \left(\frac{2}{b}\right)^c (-1)^{\frac{(u-1)}{2} \cdot \frac{(b-1)}{2}} \left(\frac{b}{v}\right)$.

Note that $\gcd(a, v) = \gcd(b, v) = 1$ and $a \equiv b \pmod{v}$ since $v \mid m$. Again, by Theorem 4.1.2(a), we conclude that $\left(\frac{a}{v}\right) = \left(\frac{b}{v}\right)$.

We claim that $(-1)^{\frac{(u-1)}{2} \cdot \frac{(a-1)}{2}} = (-1)^{\frac{(u-1)}{2} \cdot \frac{(b-1)}{2}}$. Both a and b here are odd since they are both relatively prime to the even number d. It is easy to see that $\frac{(a-1)}{2}$ is even if $a \equiv 1 \pmod{4}$ and $\frac{(a-1)}{2}$ is odd if $a \equiv 3 \pmod{4}$. To establish the claim, we just need to verify that $a \equiv b \pmod{4}$. Since $d \equiv 0 \pmod{4}$, we have $c = 2$ or 3 in part ii) of Theorem 4.1.10 (the fact that c is at most 3 follows from the assumption that d is a fundamental discriminant). Therefore, $4 \mid m$ and since $a \equiv b \pmod{m}$, we conclude that $a \equiv b \pmod{4}$.

If $c = 2$, then $\left(\frac{2}{a}\right)^c = 1 = \left(\frac{2}{b}\right)^c$ and the proof of Case 2 is complete. In order to complete the proof of Case 2, we just need to prove that $\left(\frac{2}{a}\right)^c = \left(\frac{2}{b}\right)^c$ when $c = 3$. If $c = 3$, then $8 \mid m$ and so $a \equiv b \pmod{8}$. Theorem 4.1.2(e) shows that if a and b are positive odd integers congruent to each other modulo 8, then the two Jacobi symbols $\left(\frac{2}{a}\right)$ and $\left(\frac{2}{b}\right)$ are equal. This completes the proof of the equality in equation (4.1.6) in all cases. □

We now return to the

Proof of Theorem 4.1.10: Part i): Assume d is odd so that $d \equiv 1 \pmod{4}$. We may write a in the form $a = 2^l w$, where $l \geq 0$ and w is an odd positive integer. We have

$$\chi_d(a) = \chi_d(2^l w) = [\chi_d(2)]^l \cdot \chi_d(w) = \left(\frac{2}{m}\right)^l \cdot \chi_d(w),$$

where the second equality holds by Theorem 4.1.9 and the third equality holds by equation (4.1.1). Furthermore, $\chi_d(a) = \left(\frac{2}{m}\right)^l \cdot \left(\frac{d}{w}\right)$ by equation (4.1.4) since $w \geq 1$ is odd and $\gcd(w, d) = 1$. We now apply Theorem 4.1.3 to see that

$$\left(\frac{d}{w}\right) \cdot \left(\frac{w}{m}\right) = \left(\frac{d}{w}\right) \cdot \left(\frac{w}{|d|}\right) = (-1)^{\frac{(d-1)}{2} \cdot \frac{(w-1)}{2}} \qquad \text{since } w > 0.$$

The expression on the far right above is equal to 1 since $\frac{(d-1)}{2}$ is even (remember $d \equiv 1 \pmod{4}$). Since $\left(\frac{d}{w}\right) \cdot \left(\frac{w}{m}\right) = 1$, that means either $\left(\frac{d}{w}\right) = 1 = \left(\frac{w}{m}\right)$ or $\left(\frac{d}{w}\right) = -1 = \left(\frac{w}{m}\right)$;

in either case, $\left(\frac{d}{w}\right) = \left(\frac{w}{m}\right)$. We conclude that

$$\chi_d(a) = \left(\frac{2}{m}\right)^l \left(\frac{w}{m}\right) = \left(\frac{2^l w}{m}\right) = \left(\frac{a}{m}\right),$$

the second equality holding by Theorem 4.1.2(c), completing the proof of part i).

Part ii): Assume that d is even so that $d \equiv 0 \pmod 4$. Recall that $a \in \mathbb{Z}^+$ is odd and $\gcd(a, d) = \gcd(a, m) = 1$ in part ii) of Theorem 4.1.10. We have

$$\chi_d(a) = \left(\frac{d}{a}\right) = \left(\frac{2^c u}{a}\right) = \left(\frac{2}{a}\right)^c \left(\frac{u}{a}\right), \tag{4.1.7}$$

where the first equality holds by equation (4.1.4) and the third equality holds by Theorem 4.1.2(c). We now apply Theorem 4.1.3 again to obtain

$$\left(\frac{u}{a}\right)\left(\frac{a}{v}\right) = \left(\frac{u}{a}\right)\left(\frac{a}{|u|}\right) = (-1)^{\frac{(u-1)}{2}\cdot\frac{(a-1)}{2}} \qquad \text{since } a > 0. \tag{4.1.8}$$

Since $\left(\frac{a}{v}\right) \cdot \left(\frac{a}{v}\right) = 1$ (recall that either $\left(\frac{a}{v}\right) = 1$ or $\left(\frac{a}{v}\right) = -1$), we may multiply both sides of (4.1.8) by $\left(\frac{a}{v}\right)$ and combine with (4.1.7) to obtain

$$\chi_d(a) = \left(\frac{2}{a}\right)^c (-1)^{\frac{(u-1)}{2}\cdot\frac{(a-1)}{2}} \left(\frac{a}{v}\right),$$

completing the proof of part ii) and of Theorem 4.1.10. □

We summarize our progress thus far with the following important

Corollary 4.1.12. *For a fixed fundamental discriminant d, the corresponding Kronecker symbol χ_d is a Dirichlet character modulo $m = |d|$.*

Proof: We simply combine Theorems 4.1.8, 4.1.9, and 4.1.11. □

Now that we know that χ_d is a Dirichlet character modulo $m = |d|$, we wish to prove that it is nontrivial as well, namely, that the following theorem holds:

Theorem 4.1.13. *There exists some $a \in \mathbb{Z}^+$ such that*

$$\chi_d(a) = -1. \tag{4.1.9}$$

Proof: Case 1: Assume that d is odd. As an odd fundamental discriminant, d is square-free and $m = |d| \geq 3$. Because of this, there exists an odd prime p such that $m = pg$ and $p \nmid g$ (note that $g \in \mathbb{Z}^+$ and g is odd as well). Let s be an integer in the range $1 \leq s \leq p-1$ chosen such that s is a quadratic nonresidue mod p, which is possible by Theorem 1.1.13(iv). We have $\left(\frac{s}{p}\right) = -1$ by definition. Since $\gcd(p, g) = 1$, by the Chinese Remainder Theorem there exists a positive integer a that is a simultaneous solution to the two congruences $a \equiv s \pmod{p}$ and $a \equiv 1 \pmod{g}$. Since a is relatively prime to both p and g, it is relatively prime to m. We have

$$\chi_d(a) = \left(\frac{a}{m}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{g}\right) = \left(\frac{s}{p}\right)\left(\frac{1}{g}\right) = (-1)(1) = -1,$$

where the first equality holds by part i) of Theorem 4.1.10, the second by Theorem 4.1.2(b), the third by a double application of Theorem 4.1.2(a), and the fourth by construction, which completes the proof of case 1.

Case 2: Assume that d is even and that $c = 3$ in the notation of part ii) of Theorem 4.1.10. We have $m = |d| = 8|u| = 8v$ (again, in terms of the notation of part ii)) with $\gcd(8, v) = 1$. By the Chinese Remainder Theorem, there exists a positive integer a

that is a simultaneous solution to the two congruences

$$a \equiv 5 \pmod{8} \leftarrow \text{(this implies } a \text{ is odd)},$$

$$a \equiv 1 \pmod{v}.$$

Since a is relatively prime to both 8 and v, it is relatively prime to m. By part ii) of Theorem 4.1.10 we have $\chi_d(a) = \left(\frac{2}{a}\right)^3 (-1)^{\frac{(u-1)}{2}\cdot\frac{(a-1)}{2}} \left(\frac{a}{v}\right)$. By Theorem 4.1.2(e), we have $\left(\frac{2}{a}\right) = -1$. Since $a \equiv 1 \pmod{4}$, $\frac{(a-1)}{2}$ is even and so $(-1)^{\frac{(u-1)}{2}\cdot\frac{(a-1)}{2}} = 1$. By Theorem 4.1.2(a), $\left(\frac{a}{v}\right) = \left(\frac{1}{v}\right) = 1$. For this choice of $a \in \mathbb{Z}^+$, we obtain $\chi_d(a) = -1$.

We finally assume that d is even and $c = 2$, so that $d = 4u$, with u being odd. By Lemma 2.1.10, we see that u is square-free and $u \equiv 3 \pmod{4}$. Since $\gcd(4, v) = 1$ (note that $v = |u|$ is odd), by the Chinese Remainder Theorem there exists a positive integer a that is a simultaneous solution to the two congruences

$$a \equiv 3 \pmod{4} \leftarrow \text{(this implies } a \text{ is odd)},$$

$$a \equiv 1 \pmod{v}.$$

Since a is relatively prime to both 4 and v, it is relatively prime to $m = 4v$. By part ii) of Theorem 4.1.10 we have $\chi_d(a) = \left(\frac{2}{a}\right)^2 (-1)^{\frac{(u-1)}{2}\cdot\frac{(a-1)}{2}} \left(\frac{a}{v}\right)$. Since $u \equiv a \equiv 3 \pmod{4}$, $\frac{(u-1)}{2}$ and $\frac{(a-1)}{2}$ are both odd so $(-1)^{\frac{(u-1)}{2}\cdot\frac{(a-1)}{2}} = -1$. By Theorem 4.1.2(a), $\left(\frac{a}{v}\right) = \left(\frac{1}{v}\right) = 1$. For this choice of $a \in \mathbb{Z}^+$, we obtain $\chi_d(a) = -1$. This completes the proof of Theorem 4.1.13 for all possible cases. □

Our next goal is to look carefully at the Kronecker symbol χ_d when d is a prime discriminant. Recall that a fundamental discriminant is called a "prime discriminant" if it is divisible by exactly one prime number. Recall from Comment 2.1.11 that there are exactly three prime discriminants divisible only by the prime 2, namely, -4, -8, and 8. All other prime discriminants are in one-to-one correspondence with the odd prime numbers. If q is an odd prime, then $d_q = (-1)^{(q-1)/2}q \equiv 1 \pmod 4$ is the corresponding prime discriminant.

Recall from Theorem 2.1.15 that if d is a fundamental discriminant, then d can be written uniquely (up to order) as a product of prime discriminants. When we decompose a fundamental discriminant in this way, only one prime discriminant corresponding to a given prime can appear in the product and that one only to the first power. For example, not both 8 and -4 can appear in a given decomposition of a fundamental discriminant. For Example 4.1.7, we considered $d = 60$, and $60 = (-4)(-3)\cdot 5$ is the prime discriminant decomposition.

We now consider the Kronecker symbol associated to each prime discriminant.

Proposition 4.1.14. *Given an odd prime $q \equiv 1 \pmod 4$, with $d = q > 0$, we have $\chi_q(a) = \left(\frac{a}{q}\right) \leftarrow$ (Legendre symbol) for all $a \in \mathbb{Z}^+$ with $\gcd(a,q) = 1$ (by Theorem 4.1.8 we have $\chi_q(a) = 0$ for all $a \in \mathbb{Z}^+$ such that $q \mid a$).*

Proof: Since $\left(\frac{1}{q}\right) = 1$, we have $\chi_q(1) = 1 = \left(\frac{1}{q}\right)$. Note that $q \equiv 1 \pmod 8$ or $q \equiv 5 \pmod 8$. By the Second Supplement of the QRL, we see that

$$\left(\frac{2}{q}\right) = \begin{cases} 1 & \text{if } q \equiv 1 \pmod 8 \\ -1 & \text{if } q \equiv 5 \pmod 8. \end{cases}$$

Comparing to Definition 4.1.4, $\chi_q(2) = \left(\frac{2}{q}\right)$. If, finally, p is an odd prime such that $p \neq q$, then $\chi_q(p) = \left(\frac{q}{p}\right)$ by Definition 4.1.5. Noting that $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$ by part (iii) of the QRL since $q \equiv 1 \pmod 4$, we conclude that $\chi_q(p) = \left(\frac{p}{q}\right)$ in this case.

The Proposition has now been established for $a = 1$ and a equal to any prime number not equal to q. Given $a \geq 2$ with $\gcd(a, q) = 1$, if $a = \prod_{j=1}^{t} p_j$ is the unique factorization of a into a product of primes, then by Definition 4.1.6 we have $\chi_q(a) = \prod_{j=1}^{t} \chi_q(p_j) = \prod_{j=1}^{t} \left(\frac{p_j}{q}\right)$. By Theorem 1.1.13(iii), the last product is equal to $\left(\frac{a}{q}\right)$, which completes the proof. □

Proposition 4.1.15. *Given an odd prime* $q \equiv 3 \pmod 4$, *with* $d = -q < 0$, *we have* $\chi_{-q}(a) = \left(\frac{a}{q}\right) \leftarrow$ *(Legendre symbol) for all* $a \in \mathbb{Z}^+$ *with* $\gcd(a, q) = 1$ *(by Theorem* 4.1.8 *we have* $\chi_{-q}(a) = 0$ *for all* $a \in \mathbb{Z}^+$ *such that* $q \mid a$*).*

Proof: We have $\chi_{-q}(1) = 1 = \left(\frac{1}{q}\right)$. By the Second Supplement of the QRL,

$$\left(\frac{2}{q}\right) = \begin{cases} -1 & \text{if } q \equiv 3 \pmod 8 \leftarrow \text{here } d \equiv 5 \pmod 8 \\ 1 & \text{if } q \equiv 7 \pmod 8 \leftarrow \text{here } d \equiv 1 \pmod 8, \end{cases}$$

and so $\chi_{-q}(2) = \left(\frac{2}{q}\right)$ by Definition 4.1.4. If, finally, p is an odd prime such that $p \neq q$, then $\chi_{-q}(p) = \left(\frac{-q}{p}\right)$ by Definition 4.1.5. Using parts (i) and (iii) of the QRL, we see that $\left(\frac{-q}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{q}{p}\right) = 1 \cdot \left(\frac{p}{q}\right)$ when $p \equiv 1 \pmod 4$ and that $\left(\frac{-q}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{q}{p}\right) = (-1)(-1)\left(\frac{p}{q}\right) = \left(\frac{p}{q}\right)$ when $p \equiv 3 \pmod 4$, since $q \equiv 3 \pmod 4$. In either case, $\chi_{-q}(p) = \left(\frac{p}{q}\right)$, and the Proposition is established for $a = 1$ and a equal to any prime number not equal to q. We complete the proof for all positive a relatively prime to q as we did in Proposition 4.1.14. □

Proposition 4.1.16. *If $d = -4$, then $\chi_{-4}(1) = 1$, $\chi_{-4}(2) = 0$, $\chi_{-4}(3) = -1$, $\chi_{-4}(4) = 0$, and this pattern repeats itself mod 4.*

Proof: This follows simply by knowing that χ_{-4} is a nontrivial Dirichlet character mod 4. Of course, it is easy enough to check that $\chi_{-4}(3) = \left(\frac{-4}{3}\right) = \left(\frac{2}{3}\right) = -1$. It is also instructive to apply part ii) of Theorem 4.1.10 here as well. In the notation used there: $c = 2$, $u = -1$, $v = 1$, and a is a positive odd integer. Then

$$\chi_{-4}(a) = \left(\frac{2}{a}\right)^2 \cdot (-1)^{\frac{-2}{2}\cdot\frac{(a-1)}{2}} \cdot \left(\frac{a}{1}\right) = 1 \cdot (-1)^{\frac{(a-1)}{2}} \cdot 1 = (-1)^{\frac{(a-1)}{2}},$$

which matches the pattern described in this Proposition. □

Proposition 4.1.17. *If $d = 8$, then $\chi_8(1) = 1$, $\chi_8(2) = 0$, $\chi_8(3) = -1$, $\chi_8(4) = 0$, $\chi_8(5) = -1$, $\chi_8(6) = 0$, $\chi_8(7) = 1$, $\chi_8(8) = 0$, and this pattern repeats itself mod 8.*

Proof: Most of this follows simply by knowing that χ_8 is a Dirichlet character mod 8. We do need to check, however, by use of Definition 4.1.5 and basic properties of the Legendre symbol that $\chi_8(3) = \left(\frac{8}{3}\right) = \left(\frac{2}{3}\right) = -1$, $\chi_8(5) = \left(\frac{8}{5}\right) = \left(\frac{3}{5}\right) = -1$, and $\chi_8(7) = \left(\frac{8}{7}\right) = \left(\frac{1}{7}\right) = 1$. Again, with regard to part ii) of Theorem 4.1.10 with $c = 3$, $u = 1 = v$, and a being a positive odd integer, we find that

$$\chi_8(a) = \left(\frac{2}{a}\right)^3 \cdot (-1)^0 \cdot \left(\frac{a}{1}\right) = \left(\frac{2}{a}\right) = \begin{cases} 1 & \text{if } a \equiv 1 \pmod 8 \\ -1 & \text{if } a \equiv 3 \pmod 8 \\ -1 & \text{if } a \equiv 5 \pmod 8 \\ 1 & \text{if } a \equiv 7 \pmod 8, \end{cases}$$

where the final expression on the far right holds by Theorem 4.1.2(e). Again, this matches the pattern described in this Proposition. □

Proposition 4.1.18. *If $d=-8$, then $\chi_{-8}(1)=1$, $\chi_{-8}(2)=0$, $\chi_{-8}(3)=1$, $\chi_{-8}(4)=0$, $\chi_{-8}(5)=-1$, $\chi_{-8}(6)=0$, $\chi_{-8}(7)=-1$, $\chi_{-8}(8)=0$, and this pattern repeats itself mod* 8*.*

Proof: Most of this follows simply by knowing that χ_{-8} is a Dirichlet character mod 8. We may confirm by use of Definition 4.1.5 and basic properties of the Legendre symbol that $\chi_{-8}(3)=\left(\frac{-8}{3}\right)=\left(\frac{1}{3}\right)=1$, $\chi_{-8}(5)=\left(\frac{-8}{5}\right)=\left(\frac{2}{5}\right)=-1$, and $\chi_{-8}(7)=\left(\frac{-8}{7}\right)=\left(\frac{6}{7}\right)=-1$. With regard to part ii) of Theorem 4.1.10 with $c=3$, $u=-1$, $v=1$, and a being a positive odd integer, we find that

$$\chi_{-8}(a)=\left(\frac{2}{a}\right)^{3}(-1)^{\frac{-2}{2}\cdot\frac{(a-1)}{2}}\cdot\left(\frac{a}{1}\right)=\left(\frac{2}{a}\right)(-1)^{\frac{(a-1)}{2}}=\begin{cases}1 & \text{if } a\equiv 1 \pmod 8\\ 1 & \text{if } a\equiv 3 \pmod 8\\ -1 & \text{if } a\equiv 5 \pmod 8\\ -1 & \text{if } a\equiv 7 \pmod 8,\end{cases}$$

where the final expression on the far right holds by Theorem 4.1.2(e), and, again, this matches the pattern described in this Proposition. □

Comment 4.1.19. *An important thing to notice from these last three Propositions is that when d is a prime discriminant divisible only by* 2 *and we write d in the form $2^c u$, with $u=\pm 1$, and assume a is a positive odd integer, then*

$$\chi_d(a)=\left(\frac{2}{a}\right)^{c}(-1)^{\frac{(u-1)}{2}\cdot\frac{(a-1)}{2}},$$

namely, the right side matches exactly the complicated expression appearing on the right side of part ii) of Theorem 4.1.10 *coming before and excluding the Jacobi symbol $\left(\frac{a}{v}\right)$. This observation will be of importance to us in the proof of the next theorem,*

Theorem 4.1.20.

Assume now that d is a fundamental discriminant whose unique decomposition into prime discriminants via Theorem 2.1.15 has the form

$$d = d_1 \cdots d_t, \quad \text{with } t \geq 1, \tag{4.1.10}$$

where each d_j is a prime discriminant and no two of the d_j's correspond to the same prime number. Our next goal is to prove the following important result.

Theorem 4.1.20. *Given the assumptions above,*

$$\chi_d(a) = \chi_{d_1}(a) \cdots \chi_{d_t}(a) \qquad \textit{for all } a \in \mathbb{Z}^+. \tag{4.1.11}$$

Proof: Let $a \in \mathbb{Z}^+$ and also set $m = |d|$ as before. If $\gcd(a, m) > 1$, then the left side of equation (4.1.11) is equal to 0 by Theorem 4.1.8 and the right side will also be zero since $\gcd(a, d_j) > 1$ for at least one j with $1 \leq j \leq t$. We therefore assume throughout the remainder of the proof that a is a fixed positive integer with $\gcd(a, m) = 1$ and thus $\gcd(a, d_j) = 1$ for all j with $1 \leq j \leq t$.

Case 1: Assume that the fundamental discriminant d is odd. Then $\chi_d(a) = \left(\frac{a}{m}\right)$, the Jacobi symbol, by part i) of Theorem 4.1.10. Note that $m = |d_1 \cdots d_t| = |d_1| \cdots |d_t|$, which is a product of odd primes since d is odd. Therefore, by the definition of the Jacobi symbol, $\left(\frac{a}{m}\right) = \left(\frac{a}{|d_1|}\right) \cdots \left(\frac{a}{|d_t|}\right)$, a product of Legendre symbols. In turn, this Legendre symbol product equals $\chi_{d_1}(a) \cdots \chi_{d_t}(a)$ by Propositions 4.1.14 and 4.1.15.

Case 2: Assume that the fundamental discriminant d is even. First, note that if $d \in \{-8, -4, 8\}$, then $t = 1$, $d = d_1$, $\chi_d(a) = \chi_{d_1}(a)$, and we are finished, so assume that $t > 1$. As exactly one $d_j \in \{-8, -4, 8\}$, reorder and renumber if necessary so that d_1 is this even prime discriminant. By part ii) of Theorem 4.1.10, we have $\chi_d(a) = \left(\frac{2}{a}\right)^c (-1)^{\frac{(u-1)}{2}\cdot\frac{(a-1)}{2}} \left(\frac{a}{v}\right)$, where each symbol on the right is a Jacobi symbol and d has been written as $2^c u$ with u odd and $v = |u|$. By Comment 4.1.19, this may be rewritten as $\chi_d(a) = \chi_{d_1}(a) \cdot \left(\frac{a}{v}\right)$. Since $v = |d/d_1|$ is a positive odd integer, by the same argument as in Case 1, we have that $\left(\frac{a}{v}\right) = \left(\frac{a}{|d_2|}\right) \cdots \left(\frac{a}{|d_t|}\right) = \chi_{d_2}(a) \cdots \chi_{d_t}(a)$. Thus, by combining these equations, we have again $\chi_d(a) = \chi_{d_1}(a) \cdots \chi_{d_t}(a)$. □

The Kronecker symbol χ_d has the positive integers as its domain but for our purposes in Genus Theory it is important to consider a related function $\overline{\chi}_d$ whose domain is a finite abelian group. We first extend the standard notion of congruence defined in Section 1.1. If $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$, and $a, b \in \mathbb{Z}$, we write $a \equiv b \pmod{n}$ if $n \mid (a-b)$. This reduces to the usual definition when $n \geq 2$. The set of all multiples of n forms an "ideal" in $\mathbb{Z}$, which we denote by $(n) := \{kn \mid k \in \mathbb{Z}\}$. The quotient ring $\mathbb{Z}/(n)$ has exactly $|n|$ elements, and we denote the group of units (or invertible elements) within this quotient ring by U_n (if $n \geq 2$, this group coincides with the multiplicative group of reduced residue classes modulo n discussed in Section 1.1). A typical element in the finite abelian multiplicative group U_n is a coset $a + (n)$, where a may be taken in the range $1 \leq a < |n|$ with $\gcd(a, n) = 1$. There are exactly $\varphi(|n|)$ elements in U_n, and we usually write $\overline{a}$ instead of $a + (n)$ for a typical element in U_n, where the bar is understood to mean "modulo n," with n considered as the fixed modulus throughout. As an example, assuming $n = -84$, we have $U_{-84} = \{\overline{1}, \overline{5}, \overline{11}, \overline{13}, \overline{17}, \overline{19}, \overline{23}, \overline{25}, \overline{29}, \overline{31}, \overline{37}, \overline{41}, \overline{43}, \overline{47}, \overline{53}, \overline{55}, \overline{59}, \overline{61}, \overline{65}, \overline{67}, \overline{71}, \overline{73}, \overline{79}, \overline{83}\}$, and the group U_{-84} has $\varphi(|-84|) = 24$ elements as expected.

Let d be a fixed fundamental discriminant, positive or negative. We consider d to be our fixed modulus throughout the following discussion. The function $\overline{\chi}_d$ alluded to above is defined on the group U_d as follows:

Definition 4.1.21. *Given $a \in \mathbb{Z}^+$ with $\gcd(a,d) = 1$, we set $\overline{\chi}_d(\overline{a}) := \chi_d(a)$.*

This function is well-defined on the domain U_d by Theorem 4.1.11 since $\overline{a} = \overline{b}$ (for $a, b \in \mathbb{Z}^+$ with $\gcd(a,d) = \gcd(b,d) = 1$) holds precisely when $a \equiv b \pmod{|d|}$. The codomain of this function is the set $\{1, -1\}$ by Theorem 4.1.8. In terms of our example, $\overline{\chi}_{-84}$ takes on the value 1 on the cosets $\overline{1}, \overline{5}, \overline{11}, \overline{17}, \overline{19}, \overline{23}, \overline{25}, \overline{31}, \overline{37}, \overline{41}, \overline{55}, \overline{71}$ and it takes on the value -1 on the remaining 12 cosets in U_{-84}. Using Theorem 4.1.9, it is straightforward to check that the map $\overline{\chi}_d : U_d \to \{1, -1\}$ is a homomorphism from the multiplicative group U_d to the multiplicative group $\{1, -1\}$ (we usually denote this latter group by $\mathbb{Z}_2$, even though it was defined as an additive group in Section 1.1). By Theorem 4.1.13, the map $\overline{\chi}_d : U_d \to \{1, -1\}$ is surjective, a fact of crucial importance in the following considerations. The kernel of the map $\overline{\chi}_d$, denoted by $\ker(\overline{\chi}_d)$, is a normal subgroup of U_d.

Definition 4.1.22. *If d is a fixed fundamental discriminant, we set $K_d := \ker(\overline{\chi}_d)$.*

Theorem 4.1.23. *The quotient group U_d/K_d is isomorphic to $\mathbb{Z}_2$.*

Proof: This follows immediately from the First Isomorphism Theorem and the surjectivity of the map $\overline{\chi}_d$. □

Now let $d = d_1 \cdots d_t$, $t \geq 1$, be the unique decomposition of d into a product of prime discriminants as in equation (4.1.10). For each j with $1 \leq j \leq t$, the Kronecker symbol χ_{d_j} is a nontrivial Dirichlet character modulo $|d_j|$, and we wish to define a corresponding function $\overline{\chi}_{d_j}$ for each j whose domain is U_d (the bar here again means that we are working mod d). Given $a \in \mathbb{Z}^+$ with $\gcd(a,d) = 1$, we set $\overline{\chi}_{d_j}(\overline{a}) := \chi_{d_j}(a)$.

This is again well-defined since if $a, b \in \mathbb{Z}^+$ with $\gcd(a, d) = \gcd(b, d) = 1$ and $\overline{a} = \overline{b}$, then $a \equiv b \pmod{|d_j|}$ since $d_j \mid d$ for each j with $1 \leq j \leq t$. For the same reasons as above, each function $\overline{\chi}_{d_j}$ defines a homomorphism from U_d to $\{1, -1\}$. In terms of our example above, the decomposition of the fundamental discriminant $d = -84$ is $-84 = (-3)(-4)(-7)$. We note that:

$\overline{\chi}_{-3}$ takes on the value 1 on the cosets $\overline{1}, \overline{13}, \overline{19}, \overline{25}, \overline{31}, \overline{37}, \overline{43}, \overline{55}, \overline{61}, \overline{67}, \overline{73}, \overline{79}$ and -1 on the remaining 12 cosets of U_{-84};

$\overline{\chi}_{-4}$ takes on the value 1 on the cosets $\overline{1}, \overline{5}, \overline{13}, \overline{17}, \overline{25}, \overline{29}, \overline{37}, \overline{41}, \overline{53}, \overline{61}, \overline{65}, \overline{73}$ and -1 on the remaining 12 cosets of U_{-84};

$\overline{\chi}_{-7}$ takes on the value 1 on the cosets $\overline{1}, \overline{11}, \overline{23}, \overline{25}, \overline{29}, \overline{37}, \overline{43}, \overline{53}, \overline{65}, \overline{67}, \overline{71}, \overline{79}$ and -1 on the remaining 12 cosets of U_{-84}.

As a direct consequence of Theorem 4.1.20, we have the following

Corollary 4.1.24. *Given the assumptions and conventions above,*

$$\overline{\chi}_d(\overline{a}) = \overline{\chi}_{d_1}(\overline{a}) \cdots \overline{\chi}_{d_t}(\overline{a}) \qquad \text{for all } \overline{a} \in U_d. \tag{4.1.12}$$

Definition 4.1.25. *Given the assumptions and conventions above, we set*

$$B_d := \cap_{j=1}^{t} \ker(\overline{\chi}_{d_j}),$$

and note that B_d is a normal subgroup of U_d.

In terms of our example above, $B_{-84} = \{\overline{1}, \overline{25}, \overline{37}\}$.

Theorem 4.1.26. *If t is the number of distinct prime divisors of the fundamental discriminant d, then the quotient group U_d/B_d has order 2^t and is isomorphic to $\mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$, with exactly t copies of $\mathbb{Z}_2$.*

Proof: Let $d = d_1 \cdots d_t$ be the factorization of d into a product of prime discriminants as given in equation (4.1.10). Let A denote the finite abelian group $\mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$, with exactly t copies of $\mathbb{Z}_2$ (we consider $\mathbb{Z}_2$ as $\{1, -1\}$, using multiplicative notation). Clearly, $|A| = 2^t$. For $a \in \mathbb{Z}^+$ with $\gcd(a, d) = 1$, we define the map $\psi : U_d \to A$ by $\psi(\overline{a}) = (\overline{\chi}_{d_1}(\overline{a}), \ldots, \overline{\chi}_{d_t}(\overline{a}))$. The map ψ is a homomorphism since for all $a, b \in \mathbb{Z}^+$ with $\gcd(a, d) = \gcd(b, d) = 1$, we have

$$\begin{aligned}
\psi(\overline{a} \cdot \overline{b}) = \psi(\overline{ab}) &= (\overline{\chi}_{d_1}(\overline{ab}), \ldots, \overline{\chi}_{d_t}(\overline{ab})) \\
&= (\overline{\chi}_{d_1}(\overline{a}) \cdot \overline{\chi}_{d_1}(\overline{b}), \ldots, \overline{\chi}_{d_t}(\overline{a}) \cdot \overline{\chi}_{d_t}(\overline{b})) \\
&= (\overline{\chi}_{d_1}(\overline{a}), \ldots, \overline{\chi}_{d_t}(\overline{a})) \cdot (\overline{\chi}_{d_1}(\overline{b}), \ldots, \overline{\chi}_{d_t}(\overline{b})) \\
&= \psi(\overline{a}) \cdot \psi(\overline{b}).
\end{aligned}$$

Note that $\ker(\psi) = B_d$ since the identity element of A is $(1, \ldots, 1)$.

We claim that the map ψ is surjective. To see this, let $(c_1, \ldots, c_t)$ be an arbitrary element in A. Recall that χ_{d_j} is a nontrivial Dirichlet character modulo $|d_j|$ for each j with $1 \leq j \leq t$ by Corollary 4.1.12 and Theorem 4.1.13. This implies that we can choose $y_j \in \mathbb{Z}^+$ with $\gcd(y_j, d_j) = 1$ such that $\chi_{d_j}(y_j) = c_j$ for each j with $1 \leq j \leq t$. Since the d_j are pairwise relatively prime, we may apply the Chinese Remainder

Theorem to find an integer $a \in \mathbb{Z}^+$ such that

$$\begin{aligned} a &\equiv y_1 \pmod{|d_1|} \\ &\vdots \\ a &\equiv y_t \pmod{|d_t|}. \end{aligned}$$

By Theorem 1.1.9, we have $\gcd(a, d_j) = \gcd(y_j, d_j) = 1$ for all j with $1 \leq j \leq t$ and so $\gcd(a, d) = 1$. Finally, we have $\psi(\overline{a}) = (\overline{\chi}_{d_1}(\overline{a}), \ldots, \overline{\chi}_{d_t}(\overline{a})) = (\chi_{d_1}(a), \ldots, \chi_{d_t}(a)) = (\chi_{d_1}(y_1), \ldots, \chi_{d_t}(y_t)) = (c_1, \ldots, c_t)$, which shows that ψ is surjective. By the First Isomorphism Theorem, $U_d/\ker(\psi) \cong \psi(U_d)$, and thus $U_d/B_d \cong A$. □

Theorem 4.1.27. *If t is the number of distinct prime divisors of the fundamental discriminant d, then B_d is a normal subgroup of K_d and the quotient group K_d/B_d has order 2^{t-1} and is isomorphic to $\mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$, with exactly $t-1$ copies of $\mathbb{Z}_2$.*

Proof: Let $d = d_1 \cdots d_t$ be the factorization of d into a product of prime discriminants as given in equation (4.1.10). We first show that B_d is a subset of K_d. If $a \in \mathbb{Z}^+$ with $\gcd(a, d) = 1$, then $\overline{a} \in B_d$ if and only if $\overline{\chi}_{d_1}(\overline{a}) = \cdots = \overline{\chi}_{d_t}(\overline{a}) = 1$, and thus if $\overline{a} \in B_d$, then $\overline{\chi}_d(\overline{a}) = 1$ by equation (4.1.12), which implies that $\overline{a} \in K_d$. Since K_d and B_d are both subgroups of the abelian group U_d, B_d is a normal subgroup of K_d. By standard group index computations, we have $|U_d/B_d| = |U_d/K_d||K_d/B_d|$, so $2^t = 2 \cdot |K_d/B_d|$ by Theorems 4.1.26 and 4.1.23, so that $|K_d/B_d| = 2^{t-1}$ as claimed. We saw in Theorem 4.1.26 that every element in the quotient group U_d/B_d is of order 1 or 2 and since K_d/B_d is a subgroup of U_d/B_d, the same holds for K_d/B_d, which implies that K_d/B_d is isomorphic to $\mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$, with exactly $t-1$ copies of $\mathbb{Z}_2$. □

The quotient group K_d/B_d, which we now have a precise knowledge of by Theorem 4.1.27 (note that almost every result from the present Section was ultimately involved in the proof of this Theorem), will play a crucial role in Section 4.2.

When $d = -84$, we computed the subgroup B_{-84} above and it is easy to see that the $4 = 2^{3-1}$ cosets in the quotient group K_{-84}/B_{-84} are $B_{-84} = \{\overline{1}, \overline{25}, \overline{37}\}$, $\{\overline{5}, \overline{17}, \overline{41}\}$, $\{\overline{11}, \overline{23}, \overline{71}\}$, and $\{\overline{19}, \overline{31}, \overline{55}\}$.

4.2 Genera

Genus Theory is a subject that has been an object of careful study for over 200 years and it therefore comes as no surprise that there are several ways to both view and approach this subject. In keeping with the classical line of approach taken throughout this thesis, we follow Gauss and view this subject in terms of the positive integers that are represented by forms of a fixed fundamental discriminant d. We first consider the principal form F_0 of discriminant d (see Definition 3.2.2). We will find below (see Corollary 4.2.4) that if we consider the set of all positive integers represented by F_0 (whether properly or improperly) that are relatively prime to d (this set is nonempty by Proposition 3.1.10), and look at the classes in U_d that are "hit" when we reduce these positive integers modulo d, we obtain precisely the classes in the set B_d defined in Definition 4.1.25. In terms of the example $d = -84$ we worked through in Section 4.1, every positive integer represented by $F_0 = (1, 0, 21)$ that is relatively prime to -84 is congruent to either 1, 25, or 37 modulo 84 and there is a positive integer represented by F_0 that is congruent to any given one of these three integers. When we consider the positive integers relatively prime to 84 represented by the other three reduced forms $(2, 2, 11)$, $(3, 0, 7)$, and $(5, 4, 5)$ of discriminant -84, we find that $(2, 2, 11)$ hits precisely the congruence classes $\{\overline{11}, \overline{23}, \overline{71}\}$, $(3,0,7)$ hits precisely $\{\overline{19}, \overline{31}, \overline{55}\}$, and $(5,4,5)$ hits precisely $\{\overline{5}, \overline{17}, \overline{41}\}$. These four distinct subsets of U_{-84} should look familiar, they are indeed the four cosets in the quotient group K_{-84}/B_{-84}. None of this is coincidental; a large portion of Genus Theory is illustrated by these observations! It is interesting to note that the only elements in U_{-84} that are hit by any form of discriminant -84 all lie in K_{-84}. This is a special instance of the following theorem, whose proof we borrow from [Ta3].

Theorem 4.2.1. *Let d be a fundamental discriminant and assume that n is a positive integer relatively prime to d. If n is represented by a form of discriminant d, then $\overline{n} \in K_d$.*

Proof: We are assuming there is a form $F(x,y) = ax^2+bxy+cy^2$ whose discriminant is d and $s, u \in \mathbb{Z}$ such that $n = F(s,u)$. Assume that $\gcd(s,u) = e \geq 1$. Then there exist integers r and t with $er = s$ and $et = u$ and $\gcd(r,t) = 1$. We have $n = a(er)^2 + b(er)(et) + c(et)^2 = e^2F(r,t)$. Note that the integer $m = F(r,t)$ is positive ($n = e^2m$ and $n \in \mathbb{Z}^+$) and $\gcd(m,d) = 1$ since $\gcd(n,d) = 1$ (note that $\gcd(e,d) = 1$ as well). We have $\overline{\chi}_d(\overline{n}) = \chi_d(n) = \chi_d(e^2m) = [\chi_d(e)]^2 \cdot \chi_d(m)$. Since $\gcd(e,d) = 1$, we have $\chi_d(e) = \pm 1$ and conclude that $\overline{\chi}_d(\overline{n}) = \overline{\chi}_d(\overline{m})$. Our goal is to prove that $\overline{\chi}_d(\overline{n}) = 1$ and therefore it suffices to prove that $\overline{m} \in K_d$ when $m \in \mathbb{Z}^+$, $\gcd(m,d) = 1$, and m is *properly* represented by a form $F(x,y)$ of discriminant d. These assumptions are made about m throughout the remainder of the proof. The $(\Longrightarrow)$ direction of the proof of Theorem 2.2.5 shows that there exists an integer b_1 such that ${b_1}^2 \equiv d \pmod{m}$ (this direction of the proof does not invoke the assumption in Theorem 2.2.5 that m be odd). Since $\overline{\chi}_d(\overline{m}) = \chi_d(m)$, our goal is to prove that $\chi_d(m) = 1$. There are two cases:

i) m is odd. Recall from equation (4.1.4) that if m is an odd positive integer with $\gcd(m,d)=1$ that $\chi_d(m)=\left(\frac{d}{m}\right)$, with the right side a Jacobi symbol. From above, we know there exist integers b_1 and k such that ${b_1}^2-d=km$, so $d={b_1}^2-km$. Therefore,

$$\chi_d(m)=\left(\frac{d}{m}\right)=\left(\frac{{b_1}^2-km}{m}\right)=\left(\frac{{b_1}^2}{m}\right)=\left(\frac{b_1}{m}\right)\left(\frac{b_1}{m}\right)=1,$$

where the third equality holds by Theorem 4.1.2(a), the next equality holds by Theorem 4.1.2(c), and the final equality holds because $\left(\frac{b_1}{m}\right)=\pm1$. We conclude that $\chi_d(m)=1$ when m is odd.

ii) m is even. In this case we must have $d\equiv 1 \pmod 4$ since if $4\mid d$ then m and d are not relatively prime. By Theorem 2.2.4, since m is properly represented by the form $F(x,y)$, then $F(x,y)$ is properly equivalent to the form $G(X,Y)=mX^2+b_1XY+c_1Y^2$ with the same discriminant $d={b_1}^2-4mc_1$. Since m is even, we have $d\equiv {b_1}^2 \pmod 8$. Since $1\equiv d\equiv {b_1}^2 \pmod 4$, b_1 is odd. For any odd integer b_1 we have ${b_1}^2\equiv 1 \pmod 8$ and so $d\equiv 1 \pmod 8$. By Definition 4.1.4, we have $\chi_d(2)=1$ since $d\equiv 1 \pmod 8$. We now write $m=2^rm'$, with r chosen such that m' is odd. Note that $m'\in\mathbb{Z}^+$ and that $\gcd(m',d)=1$ since $\gcd(m,d)=1$. If $m'=1$, we can go directly to the equalities in the last line below to complete the proof, so we assume that $m'\geq 3$ from now on. From above, $d={b_1}^2-4mc_1={b_1}^2-4\cdot 2^rm'\cdot c_1$ and so ${b_1}^2\equiv d \pmod{m'}$, which implies that d is a quadratic residue modulo m'. By Theorem 2.2.5, m' is properly represented by a form of discriminant d. Since m' satisfies all of the conditions as in Case i) above, we conclude that $\chi_d(m')=1$. Finally, we have, by Theorem 4.1.9,

$$\chi_d(m)=\chi_d(2^rm')=[\chi_d(2)]^r\cdot\chi_d(m')=1^r\cdot 1=1. \qquad \square$$

Proposition 4.2.2. *If d is a fundamental discriminant and F_0 is the principal form of discriminant d, then F_0 represents positive integers that fall into every congruence class within the subset $B_d \subset U_d$.*

Proof: Assume that m is a positive integer such that $\gcd(m, d) = 1$ and $\overline{m} \in B_d$. We wish to prove that there exists a positive integer n that is representable by F_0 such that $\overline{n} = \overline{m}$, and we consider four different cases (the notation introduced in Definition 2.1.16 will be employed here).

i) $\underline{d_2 = 1}$. Let $d = d_1 \cdots d_t$ be the factorization of d into a product of prime discriminants and note in this case that each d_j is of the form $(-1)^{(p_j-1)/2}p_j$, for some odd prime p_j (there should be no confusion between what d_2 might be here versus the value of d_2, defined with respect to the prime number 2, used to distinguish the four cases in this proof). By definition, the condition that $\overline{m} \in B_d$ is equivalent to the following Legendre symbol equalities: $\left(\frac{m}{p_1}\right) = \cdots = \left(\frac{m}{p_t}\right) = 1$. This follows from Propositions 4.1.14 and 4.1.15 and amounts to $m \in \mathbb{Z}^+$ being a quadratic residue with respect to each p_j for $1 \le j \le t$. This means there are integers $x_1, \ldots, x_t$ such that $x_j^2 \equiv m \pmod{p_j}$ for each j with $1 \le j \le t$. We now use the CRT to obtain a positive integer x such that $x \equiv x_j \pmod{p_j}$ for $1 \le j \le t$, and set $n = x^2 = F_0(x, 0)$. The positive integer n is representable by F_0 and $n \equiv m \pmod{p_j}$ for $1 \le j \le t$, which implies that $n \equiv m \pmod{d}$, and completes the proof in this case.

ii) $\underline{d_2 = -4}$. Assume that the first prime discriminant d_1 in the factorization of d above is equal to -4. We replace the congruences $x_1^2 \equiv m \pmod{p_1}$ and $x \equiv x_1 \pmod{p_1}$ in case i) by instead $1^2 \equiv m \pmod{4}$ (see Proposition 4.1.16; thus, $x_1 = 1$) and $x \equiv 1 \pmod{4}$, respectively, and then proceed as in case i) to complete the proof.

iii) $\underline{d_2 = -8}$. This time we set $d_1 = -8$. We replace the congruences $x_1^2 \equiv m \pmod{p_1}$

and $x \equiv x_1 \pmod{p_1}$ in case i) by instead $1^2 \equiv m \pmod 8$ (again, $x_1 = 1$) and $x \equiv 1 \pmod 8$, respectively. If $m \equiv 1 \pmod 8$ (see Proposition 4.1.18), then $n = F_0(x, 0)$ is a positive integer representable by F_0 with $n \equiv m \pmod d$, exactly as desired. If $m \equiv 3 \pmod 8$ (the other possibility in Proposition 4.1.18), we choose $x_1 = 1$ again, and use the CRT again to find a positive integer x simultaneously satisfying the relevant congruences, but we also make sure to pick x large enough so that $x^2 - \frac{d}{4} > 0$. We now set $n = F_0(x, 1) = x^2 - \frac{d}{4}$ (the principal form of discriminant d is $F_0 = x^2 - \frac{d}{4}y^2$ in the present case) and note that n is a positive integer representable by F_0. We also note that $n \equiv 1 - \frac{d}{4} \equiv 1 - 6 \equiv 3 \equiv m \pmod 8$ (recall from Definition 2.1.16 that $\frac{d}{4} \equiv 6 \pmod 8$ in the present case) and $n \equiv m \pmod{p_j}$ for $2 \leq j \leq t$ since $p_j \mid \frac{d}{4}$ for each such odd prime p_j. Therefore, $n \equiv m \pmod d$, which completes the proof in this case.

iv) $\underline{d_2 = 8}$. Here we set $d_1 = 8$. The required argument follows the same exact pattern as in case iii). This time $m \equiv 1 \pmod 8$ and $m \equiv 7 \pmod 8$ are the two possibilities that arise in Proposition 4.1.17. If $m \equiv 1 \pmod 8$, we again set $n = F_0(x, 0)$ and proceed as above. If $m \equiv 7 \pmod 8$, we again set $n = F_0(x, 1)$, and note in the present case that $\frac{d}{4} \equiv 2 \pmod 8$, so that $n \equiv m \pmod 8$. The rest of the details work out exactly as above, completing the overall proof. □

Theorem 4.2.3. *Let d be a fixed fundamental discriminant and $\mathcal{C}$ a given class in $\mathcal{H}(d)$. If m, n are positive integers relatively prime to d that are both representable by a form $F \in \mathcal{C}$, then $\overline{m}$ and $\overline{n}$ lie in the same coset of the quotient group K_d/B_d.*

Proof: Let $d = d_1 \cdots d_t$ be the factorization of d into a product of prime discriminants, and if $d \equiv 0 \pmod 4$, we assume that the prime discriminants are numbered such that $d_1 \in \{-4, -8, 8\}$. By Theorem 4.2.1, we know that $\overline{m}$ and $\overline{n}$ are both elements of the group K_d. Let $\overline{x} = \overline{m} \cdot \overline{n}^{-1} \in K_d$. To show that $\overline{m}$ and $\overline{n}$ are in the same coset of K_d/B_d, we need to demonstrate that $\overline{m} \cdot B_d = \overline{n} \cdot B_d$, or equivalently, that $\overline{x} \in B_d$. We have $\overline{m} = \overline{x} \cdot \overline{n}$, and so $\overline{m} \cdot \overline{n} = \overline{x} \cdot \overline{n}^2$. Note that $\overline{n}^2 \in B_d$ since $\overline{\chi}_{d_j}(\overline{n}^2) = \left[\overline{\chi}_{d_j}(\overline{n})\right]^2 = (\pm 1)^2 = 1$ for each j with $1 \leq j \leq t$. It therefore suffices to show that $\overline{m} \cdot \overline{n} \in B_d$.

Let $F = (a, b, c)$ be any given form in the class $\mathcal{C}$, and let $r, s, t, u \in \mathbb{Z}$ be such that $F(r, t) = m$ and $F(s, u) = n$. Let $\mathbf{D} = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$, and note that $F\mathbf{D} = (m, l, n)$ for some $l \in \mathbb{Z}$ (the form $F\mathbf{D}$ may be defined exactly as in Definition 3.3.9; this new form will not have the same discriminant as F if $\mathbf{D} \notin GL_2(\mathbb{Z})$). We have

$$\mathbf{D}^T \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \mathbf{D} = \begin{pmatrix} m & l/2 \\ l/2 & n \end{pmatrix},$$

and taking determinants of all matrices, and setting $v = \det(\mathbf{D})$, we obtain

$$v^2 \left(ac - \frac{b^2}{4} \right) = \left(mn - \frac{l^2}{4} \right).$$

Multiplying both sides by -4 gives $(b^2 - 4ac)v^2 = l^2 - 4mn$, and thus $l^2 - 4mn = dv^2$. For each odd prime discriminant factor d_j of d, the congruence $l^2 \equiv 4mn \pmod{|d_j|}$ holds. Since $|d_j|$ is an odd prime, there exists an integer e_j such that $2e_j \equiv 1 \pmod{|d_j|}$ by Theorem 1.1.3. It follows that $(le_j)^2 \equiv mn \pmod{|d_j|}$ for each j with d_j being odd, which shows that mn is a quadratic residue with respect to each such $|d_j|$. By Propositions 4.1.14 and 4.1.15, we conclude that $\overline{\chi}_{d_j}(\overline{m} \cdot \overline{n}) = 1$ for each odd prime discriminant d_j dividing d.

If $d \equiv 1 \pmod 4$, we may already conclude that $\overline{m} \cdot \overline{n} \in B_d$. If $d \equiv 0 \pmod 4$, all that remains to prove is that $\overline{\chi}_{d_1}(\overline{m} \cdot \overline{n}) = 1$, where $d_1 \in \{-4, -8, 8\}$. From above,

$l^2 - 4mn = dv^2$, and so $l^2 = 4mn + dv^2$, where both terms on the right side of the second equation are even, which implies that l^2 is even, and so l is even as well. Let $l = 2k$ for some integer k, and thus $4k^2 = 4mn + dv^2$, and furthermore $k^2 = mn + \frac{dv^2}{4}$, where $\frac{d}{4} \in \mathbb{Z}$. Since m and n are relatively prime to d, which is even by assumption, the product mn is odd and positive. We now consider three separate cases.

i) $\underline{d_1 = -4}$. From above, we write $mn = k^2 - \frac{d}{4} \cdot v^2$. From Definition 2.1.16, we see that $\frac{d}{4} \equiv 3 \pmod 4$ in this case and so $mn \equiv k^2 + v^2 \pmod 4$. If both k and v are even or they are both odd, then this last congruence will not hold since mn is an odd integer. This implies either that $k^2 \equiv 0 \pmod 4$ and $v^2 \equiv 1 \pmod 4$ or that $k^2 \equiv 1 \pmod 4$ and $v^2 \equiv 0 \pmod 4$. In either event, $mn \equiv 1 \pmod 4$, and we then have $\overline{\chi}_{-4}(\overline{m} \cdot \overline{n}) = 1$ by Proposition 4.1.16, completing the proof.

ii) $\underline{d_1 = -8}$. Again, we start with $mn = k^2 - \frac{d}{4} \cdot v^2$. From Definition 2.1.16, we see that $\frac{d}{4} \equiv 6 \pmod 8$ in this case and so $mn \equiv k^2 + 2v^2 \pmod 8$. If k is even, then this last congruence will not hold since mn is an odd integer, and thus k must be odd so that $k^2 \equiv 1 \pmod 8$. If v is even, then $v^2 \equiv 0$ or $4 \pmod 8$, which implies $mn \equiv 1 + 0 \equiv 1 \pmod 8$ (because $2v^2 \equiv 0 \pmod 8$ in either event). If v is also odd, then $v^2 \equiv 1 \pmod 8$, and $mn \equiv 1 + 2 \cdot 1 \equiv 3 \pmod 8$. Since either $mn \equiv 1$ or $3 \pmod 8$, we have $\overline{\chi}_{-8}(\overline{m} \cdot \overline{n}) = 1$ by Proposition 4.1.18, completing the proof.

iii) $\underline{d_1 = 8}$. We start with $mn = k^2 - \frac{d}{4} \cdot v^2$. From Definition 2.1.16, we see that $\frac{d}{4} \equiv 2 \pmod 8$ in this case and so $mn \equiv k^2 - 2v^2 \pmod 8$. As in the previous case, this is not possible when k is even. If k is odd and v is even, $mn \equiv 1 - 0 \equiv 1 \pmod 8$. If both k and v are odd, then $mn \equiv 1 - 2 \cdot 1 \equiv -1 \equiv 7 \pmod 8$. Since either $mn \equiv 1$ or $7 \pmod 8$, we have $\overline{\chi}_8(\overline{m} \cdot \overline{n}) = 1$ by Proposition 4.1.17, which completes the overall proof. □

Corollary 4.2.4. *If d is a fundamental discriminant and F_0 is the principal form of discriminant d, then the positive integers relatively prime to d that are represented by F_0 cover precisely the classes in the set B_d upon reduction modulo d.*

Proof: We already know from Proposition 4.2.2 that every element in B_d is "hit" by positive integers representable by F_0 upon reduction modulo d. We know that $\overline{1}$ is one of the elements hit since $F_0(1,0) = 1$. If $\overline{m}$ is any other element in K_d that is hit by F_0, then by Theorem 4.2.3 we must have $\overline{m} \cdot B_d = \overline{1} \cdot B_d$, which implies that $\overline{m} \in B_d$, completing the proof. □

Theorem 4.2.3 allows us to uniquely define a map from the group $\mathcal{H}(d)$ to the quotient group K_d/B_d. Given a class $\mathcal{C} \in \mathcal{H}(d)$, every form $F \in \mathcal{C}$ represents exactly the same integers by Theorem 2.2.3 and any such F represents a positive integer m relatively prime to d by Proposition 3.1.10. If $n \in \mathbb{Z}^+$ is relatively prime to d and n is representable by F, then $\overline{m} \cdot B_d = \overline{n} \cdot B_d$ by Theorem 4.2.3, which shows that the following map, named in honor of Gauss, is well-defined:

Definition 4.2.5. *Given the notation introduced just above, the Gauss map $\omega_d : \mathcal{H}(d) \to K_d/B_d$ is defined by sending $\mathcal{C} \mapsto \overline{m} \cdot B_d$.*

Note that once we know a single positive integer m, with $\gcd(m, d) = 1$, represented by a form F of discriminant d, then we know that $\mathcal{C} \mapsto \overline{m} \cdot B_d$, where $\mathcal{C}$ is the class to which F belongs. In terms of the example $d = -84$ worked out in Section 4.1, and using the notation introduced in Section 3.2, we have:

$\omega_{-84}(\mathcal{C}_0) = \overline{1} \cdot B_{-84}$,

$\omega_{-84}([2, 2, 11]) = \overline{11} \cdot B_{-84}$,

$\omega_{-84}([3, 0, 7]) = \overline{19} \cdot B_{-84}$, and

$\omega_{-84}([5,4,5]) = \overline{5} \cdot B_{-84}$.

Note that all 4 cosets in K_{-84}/B_{-84} are "hit" under the Gauss map. In order to gain a better understanding of the Gauss map, we now revisit the other four examples covered in Section 3.2. We will verify in each example that the Gauss map is surjective. The surjectivity of the Gauss map is one of the key features of Genus Theory and will be proved in Theorem 4.2.18.

Example 4.2.6. $\underline{d = -39}$. The Gauss map ω_{-39} sends both $[1,1,10]$ and $[3,3,4]$ to $\overline{1} \cdot B_{-39} = \{\overline{1}, \overline{4}, \overline{10}, \overline{16}, \overline{22}, \overline{25}\}$ and it sends both $[2,1,5]$ and $[2,-1,5]$ to $\overline{2} \cdot B_{-39} = \{\overline{2}, \overline{5}, \overline{8}, \overline{11}, \overline{20}, \overline{32}\}$. By Theorem 4.1.27, the group K_{-39}/B_{-39} is of order 2, confirming that the Gauss map is onto.

Example 4.2.7. $\underline{d = -87}$. The Gauss map ω_{-87} sends $[1,1,22]$, $[4,3,6]$, and $[4,-3,6]$ to $\overline{1} \cdot B_{-87} = \{\overline{1}, \overline{4}, \overline{7}, \overline{13}, \overline{16}, \overline{22}, \overline{25}, \overline{28}, \overline{34}, \overline{49}, \overline{52}, \overline{64}, \overline{67}, \overline{82}\}$ and it sends $[2,1,11]$, $[2,-1,11]$, and $[3,3,8]$ to $\overline{2} \cdot B_{-87} = \{\overline{2}, \overline{8}, \overline{11}, \overline{14}, \overline{17}, \overline{26}, \overline{32}, \overline{41}, \overline{44}, \overline{47}, \overline{50}, \overline{56}, \overline{68}, \overline{77}\}$. By Theorem 4.1.27, the group K_{-87}/B_{-87} is of order 2, confirming that the Gauss map is onto.

Example 4.2.8. $\underline{d = 60}$. The Gauss map ω_{60} sends $[1,8,1]$ to $\overline{1} \cdot B_{60} = \{\overline{1}, \overline{49}\}$, sends $[3,12,7]$ to $\overline{7} \cdot B_{60} = \{\overline{7}, \overline{43}\}$, sends $[11,18,6]$ to $\overline{11} \cdot B_{60} = \{\overline{11}, \overline{59}\}$, and sends $[2,10,5]$ to $\overline{17} \cdot B_{60} = \{\overline{17}, \overline{53}\}$. By Theorem 4.1.27, the group K_{60}/B_{60} is of order 4, confirming that the Gauss map is onto.

Example 4.2.9. $\underline{d = -260}$. The Gauss map ω_{-260} sends $[1,0,65]$ and $[9,8,9]$ to $\overline{1} \cdot B_{-260} = \{\overline{1}, \overline{9}, \overline{29}, \overline{49}, \overline{61}, \overline{69}, \overline{81}, \overline{101}, \overline{121}, \overline{129}, \overline{181}, \overline{209}\}$, sends $[3,2,22]$ and $[3,-2,22]$ to $\overline{3} \cdot B_{-260} = \{\overline{3}, \overline{23}, \overline{27}, \overline{43}, \overline{87}, \overline{103}, \overline{107}, \overline{127}, \overline{147}, \overline{183}, \overline{207}, \overline{243}\}$, sends $[6,2,11]$ and $[6,-2,11]$ to $\overline{11} \cdot B_{-260} = \{\overline{11}, \overline{19}, \overline{31}, \overline{59}, \overline{71}, \overline{99}, \overline{111}, \overline{119}, \overline{151}, \overline{171}, \overline{219}, \overline{239}\}$, and sends

$[5, 0, 13]$ and $[2, 2, 33]$ to $\overline{33} \cdot B_{-260} = \{\overline{33}, \overline{37}, \overline{57}, \overline{73}, \overline{93}, \overline{97}, \overline{137}, \overline{177}, \overline{193}, \overline{197}, \overline{213}, \overline{253}\}$. By Theorem 4.1.27, the group K_{-260}/B_{-260} is of order 4, confirming that the Gauss map is onto.

The Gauss map sends the elements of one abelian group to another such group and it is natural to check if this map is a homomorphism, which indeed it is, as confirmed in the following important theorem.

Theorem 4.2.10. *If d is a fixed fundamental discriminant, the Gauss map $\omega_d : \mathcal{H}(d) \to K_d/B_d$ is a homomorphism.*

Proof: Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be any two given classes in $\mathcal{H}(d)$ and assume that $F_1 \in \mathcal{C}_1$ and $F_2 \in \mathcal{C}_2$ are concordant forms. Let m_1, m_2 be positive integers, both relatively prime to d, that are representable by F_1 and F_2, respectively. We then have, by definition, $\omega_d(\mathcal{C}_1) = \overline{m_1} \cdot B_d$ and $\omega_d(\mathcal{C}_2) = \overline{m_2} \cdot B_d$. By Theorem 3.1.6, the positive integer $m_1 m_2$ (which is relatively prime to d) is representable by the composite form $F_1 * F_2$, which lies in the class $\mathcal{C}_1 * \mathcal{C}_2$. This means that $\omega_d(\mathcal{C}_1 * \mathcal{C}_2) = \overline{m_1 m_2} \cdot B_d$. Observing that $\overline{m_1 m_2} \cdot B_d = (\overline{m_1} \cdot \overline{m_2}) \cdot B_d = (\overline{m_1} \cdot B_d)(\overline{m_2} \cdot B_d)$, the proof is complete. □

With the Gauss map defined, we are finally ready to introduce the classification of forms according to genus.

Definition 4.2.11. *If d is a fixed fundamental discriminant and F_1, F_2 are forms of discriminant d, we say that F_1 and F_2 (or, more formally, the classes $\mathcal{C}_1$ and $\mathcal{C}_2$ to which they belong) lie in the same "genus" if $\omega_d(\mathcal{C}_1) = \omega_d(\mathcal{C}_2)$. The "principal genus" consists of all forms (or, again, the classes to which they belong) which are sent to the identity element $\overline{1} \cdot B_d$ under the Gauss map. In other words, the principal genus* *consists of all classes in the set* $\ker(\omega_d)$ *and clearly the principal class* $\mathcal{C}_0$ *is contained in the principal genus.*

Comment 4.2.12. *Of course,* $\ker(\omega_d)$ *is a normal subgroup of* $\mathcal{H}(d)$ *and*

$$\mathcal{H}(d)/\ker(\omega_d) \cong \operatorname{im}(\omega_d), \tag{4.2.1}$$

by the First Isomorphism Theorem. Each coset of $\mathcal{H}(d)/\ker(\omega_d)$ *constitutes a genus of classes and each genus contains the same number of classes. Recalling the examples above, there is one class per genus when* $d = -84$ *and* $d = 60$*, two classes per genus when* $d = -39$ *and* $d = -260$*, and three classes per genus when* $d = -87$*. There is no upper limit to the number of classes that can lie in a given genus.*

Definition 4.2.13. *If* d *is a fixed fundamental discriminant, the quotient group* $\mathcal{H}(d)/\ker(\omega_d)$ *is called the "genus group" and is denoted by* $\mathcal{G}(d)$*.*

Comment 4.2.14. *Once we know that the Gauss map is onto, we may conclude immediately that* $\mathcal{G}(d) \cong K_d/B_d$*; recall from Theorem* 4.1.27 *that we already know the exact structure of* K_d/B_d*!*

Theorem 4.2.15. *Let* d *be a fixed fundamental discriminant and* F *a form of discriminant* d *belonging to the class* $\mathcal{C} \in \mathcal{H}(d)$ *which is concordant with a form* F_0' *lying in the principal class* $\mathcal{C}_0$*. If* $m \in \mathbb{Z}^+$ *is relatively prime to* d *and representable by* F*, then every element in the coset* $\overline{m} \cdot B_d$ *will be hit by positive integers representable by* F *upon reduction modulo* d*.*

Proof: Every element in the coset $\overline{m} \cdot B_d$ is of the form $\overline{m} \cdot \overline{a}$ for some element $\overline{a} \in B_d$. By assumption, $F(x_1, y_1) = m$ for some $x_1, y_1 \in \mathbb{Z}$. Given an arbitrary element $\overline{a} \in B_d$, we know by Proposition 4.2.2 that there is a positive integer b, with $\overline{b} = \overline{a}$, such that $F_0'(x_2, y_2) = b$ for some $x_2, y_2 \in \mathbb{Z}$. By Theorem 3.1.6, the positive integer mb is representable by the composite form $F * F_0'$, which lies in the class $\mathcal{C} * \mathcal{C}_0 = \mathcal{C}$. This implies that the element $\overline{m} \cdot \overline{a}$ is hit by $F \sim F * F_0'$, which completes the proof since $\overline{a} \in B_d$ was chosen arbitrarily. □

The following corollary will prove to be useful in Section 4.3.

Corollary 4.2.16. *If d is a fixed fundamental discriminant and F is a form of discriminant d that lies in the principal genus of $\mathcal{H}(d)$, then there exist integers x, y such that $F(x, y)$ is a positive integer congruent to* 1 *modulo d.*

Proof: Let $m \in \mathbb{Z}^+$ be such that $\gcd(m, d) = 1$ and m is representable by F. The fact that F lies in the principal genus just means that $\overline{m} \cdot B_d = \overline{1} \cdot B_d$. Since $\overline{1} \in \overline{m} \cdot B_d$, the result follows immediately from Theorem 4.2.15. □

An especially nice situation arises when there is exactly one class per genus. In this case, $\ker(\omega_d) = \{\mathcal{C}_0\}$, and we then have $\mathcal{G}(d) \cong \mathcal{H}(d)$, namely, the genus group and class group coincide. This is interesting for several reasons. First, once we know the Gauss map is onto, we may conclude that $\mathcal{H}(d) \cong \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$, with exactly $t-1$ copies of $\mathbb{Z}_2$, where as usual t is the number of distinct prime divisors of d. Indeed, we have $|\mathcal{H}(d)| = 2^{t-1}$ if and only if $\ker(\omega_d) = \{\mathcal{C}_0\}$. It is known that there are only finitely many negative d for which this occurs and the number of known such d is exactly 65. We display these discriminants below and group them with respect to the value of t.

$t = 1 : d = -3, -4, -7, -8, -11, -19, -43, -67, -163$ (these are precisely the 9 negative discriminants with $h(d) = 1$ mentioned in Section 2.5).

$t = 2 : d = -15, -20, -24, -35, -40, -51, -52, -88, -91, -115, -123, -148, -187,$

$-232, -235, -267, -403, -427$ (these are precisely the 18 negative discriminants with $h(d) = 2$).

$t = 3 : d = -84, -120, -132, -168, -195, -228, -280, -312, -340, -372, -408, -435,$
$-\, 483, -520, -532, -555, -595, -627, -708, -715, -760, -795, -1012, -1435.$

$t = 4 : d = -420, -660, -840, -1092, -1155, -1320, -1380, -1428, -1540, -1848,$
$-\, 1995, -3003, -3315.$

$t = 5 : d = -5460$ (which brings the final tally to 65).

It is an open problem whether this is the complete list of all negative discriminants for which there is one class per genus. It has been proved that there is at most one more such discriminant and it has also been proved that the above list would indeed be complete if a certain other famous conjecture could be shown to hold, the so-called "extended Riemann hypothesis," or ERH. Many well-known open problems in Number Theory would be instantly resolved if the ERH were proved, which makes it the most notable open conjecture in all of Number Theory.

Why is Genus Theory useful? For starters, it gives us the best known lower bound for the size of the class group, namely, $2^{t-1} \leq |\mathcal{H}(d)|$ since $2^{t-1} \mid |\mathcal{H}(d)|$ (again, this is contingent upon the Gauss map being onto). Another interesting avenue is opened up by the following result.

Theorem 4.2.17. *If d is a fixed fundamental discriminant and p is a prime such that $\chi_d(p) = 1$, then p is representable by some form of discriminant d.*

Proof: If $p = 2$ and $\chi_d(p) = 1$, then $d \equiv 1 \pmod 8$ by Definition 4.1.4. The form $2x^2 + xy + \frac{(1-d)}{8}y^2$ has integer coefficients, discriminant equal to d, and clearly represents 2. Now assume p is an odd prime. By Definition 4.1.5, $\chi_d(p) = 1$ implies that the Legendre symbol $\left(\frac{d}{p}\right)$ is equal to one, which in turn means that d is a quadratic residue modulo p. A direct application of Theorem 2.2.5 completes the proof. $\square$

This last theorem is quite powerful, and allows us to quickly overcome the difficulties first encountered by Fermat and Euler. Recall that the real difficulty in Section 1.3 boiled down to the following problem: Given a prime p of the form $4k+1$, prove that p is representable by the quadratic form x^2+y^2. First note that for such a prime p, we have $\chi_{-4}(p) = 1$ by Proposition 4.1.16. Theorem 4.2.17 guarantees that some form of discriminant -4 represents p, but by Table 1 in Section 2.4, we know that every form of discriminant -4 is equivalent to the form $x^2 + y^2$, which completes the proof. We tackle Fermat's second theorem in Section 1.2 in a similar way. For any prime p that is congruent to 1 or 3 modulo 8, we have $\chi_{-8}(p) = 1$ by Proposition 4.1.18. Every form of discriminant -8 is equivalent to x^2+2y^2 (again, see Table 1), which completes the proof of this theorem. Euler's theorem, stated in equation (1.2.4), is handled in a similar way, but here Genus Theory <u>is</u> <u>needed</u>. For any prime p congruent to 1 or 9 modulo 20, we quickly confirm that $\chi_{-20}(p) = 1$. This means, by Theorem 4.2.17, that some form of discriminant -20 represents such a prime p. However, as Table 1 shows, there are two classes of forms of discriminant -20, so we are not quite finished as in the class number one examples above. Nevertheless, the form $(2, 2, 3)$ only represents integers relatively prime to 20 in the following congruence classes (mod 20): $\overline{3}, \overline{7}$. This rules out $(2, 2, 3)$ as far as representing the primes of interest and allows us to conclude that every prime p that is congruent to 1 or 9 modulo 20 is representable by the form $x^2 + 5y^2$. This particular example shows nicely, from a historical point of view, how Genus Theory was most likely discovered and why it was developed further from the beginning. If there is exactly one class per genus, as in the discriminant -20 example just discussed, we can pinpoint exactly which form of discriminant d (more precisely, which class of forms) represents p by knowing the values of $\chi_{d_j}(p)$ for $1 \leq j \leq t$. If there is more than one class per genus, then we know that a form (or class) from a specific genus represents p but we can not say which one (or ones, as the case may be) actually does so from Genus Theory alone. The following example, with $d = -260$, illustrates this point. We have $\chi_{-260}(37) = 1$, so we know by Theorem 4.2.17 that the prime 37 is representable by a form of discriminant -260. Looking at Example 4.2.9, we may use Genus Theory to rule out all forms except those in the classes $[5, 0, 13]$ and $[2, 2, 33]$. We find easily that $2(1)^2 + 2(1)(1) + 33(1)^2 = 37$, and a few simple computations convince us quickly that 37 is not representable by the form $5x^2 + 13y^2$. In a similar way, we may quickly check that the prime 97 is representable by $5x^2 + 13y^2$, but not by $(2, 2, 33)$. Genus Theory quickly limits the possibilities, but does not tell us which form or forms in a given genus represents a particular prime number. Note that the prime 3 is representable by forms in *both* classes $[3, 2, 22]$ and $[3, -2, 22]$ making up one of the genera in this example. This shows the main limitation of Genus Theory with regard to the representation problem of integers by forms and clarifies the statement we made in the first paragraph of Section 2.4 that "a full resolution to the problem" is not provided by the theory developed in this thesis. More advanced ideas, involving "ring class fields," do allow one to distinguish between forms in the same genus, concerning the representation of prime numbers in particular, but these ideas lie beyond the scope of this thesis (see the book by Cox [Co] for a nice introduction to these more advanced developments).

The last theorem we wish to prove in this section is that the Gauss map is surjective for all fundamental discriminants. In order to fully appreciate this theorem, we will provide a summary, in hindsight, of the main ingredients used in this proof and we will find indeed that almost every result proved in this thesis was called upon.

Before coming so far, however, there is still one major theorem that we wish to mention here since it plays a crucial rôle in proving that the Gauss map is onto. This is one of the most impressive results in the *Disquisitiones* [Ga] and its proof cost even the great Gauss some serious thought. The proof of this theorem, variously known as the "Duplication Theorem" or "Principal Genus Theorem," is a real tour de force and will be postponed until the next section. The Duplication Theorem states that

$$\ker(\omega_d) = \mathcal{S}(d), \tag{4.2.2}$$

in other words, the classes in the principal genus are precisely the square classes, with respect to composition, in the class group $\mathcal{H}(d)$. Illustrating this theorem in terms of our earlier examples, in the class group $\mathcal{H}(-39) \cong \mathbb{Z}_4$, both the identity class $\mathcal{C}_0$ and the class $[3, 3, 4]$ are squares, whereas in the class group $\mathcal{H}(-84) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, only the identity class itself is a square.

Theorem 4.2.18. *For any given fundamental discriminant d, the Gauss map $\omega_d : \mathcal{H}(d) \to K_d/B_d$ is surjective and*

$$\boxed{\mathcal{G}(d) \cong K_d/B_d \cong \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2\,,}$$

with exactly $t-1$ copies of $\mathbb{Z}_2$.

Proof: From the definition of $\mathcal{G}(d)$, the isomorphism (4.2.1), and the Duplication Theorem (4.2.2), we immediately have

$$\mathcal{G}(d) = \mathcal{H}(d)/\mathcal{S}(d) \cong \text{im}(\omega_d). \tag{4.2.3}$$

By Proposition 3.3.7 and Theorem 3.3.20 for the first isomorphism below and by Theorem 4.1.27 for the second, we have

$$\mathcal{H}(d)/\mathcal{S}(d) \cong \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2 \cong K_d/B_d, \tag{4.2.4}$$

with exactly $t-1$ copies of $\mathbb{Z}_2$. Since $\text{im}(\omega_d)$ is a subgroup of K_d/B_d and these two groups have the same finite cardinality, we conclude that ω_d is surjective, which completes the proof. □

Comment 4.2.19. *We now have the perspective to recapitulate the main ingredients going into the proof of Theorem* 4.2.18*. This proof – largely even the mere statement of the Theorem — really does depend directly or indirectly upon nearly every other result stated in this thesis. Besides the development of all the necessary background simply to define the equivalence and composition of binary quadratic forms, the class group* $\mathcal{H}(d)$*, and the genus group* $\mathcal{G}(d)$*, this proof uses the Duplication Theorem ingredient, whose proof (as seen in the next section) itself depends heavily on properties of* 3×3 *matrices and the study of certain ternary quadratic forms. The Gauss map* ω_d *and the squaring map* φ_d *are two homomorphisms obviously central to the current proof. Of course the Kronecker symbol* χ_d*, and its properties depending upon congruences, is instrumental in defining and understanding the quotient group* K_d/B_d*. In establishing the first isomorphism in statement* (4.2.4)*, it was also necessary to study ambiguous* *classes and count them by working with special ambiguous forms.*

We began this section with Theorem 4.2.1, which shows that the only elements in U_d hit by forms of discriminant d all lie within the subgroup K_d. We now conclude by showing that K_d is precisely the subset within U_d hit by forms of discriminant d.

Corollary 4.2.20. *Let d be a fixed fundamental discriminant. For every element $\overline{n} \in K_d$, there exists a positive integer m with $\overline{m} = \overline{n}$ such that m is representable by some form of discriminant d.*

Proof: By Theorem 4.2.15, we know that if $\overline{m} \cdot B_d$ is a coset within K_d/B_d that is in the image of the Gauss map ω_d, then every element in the coset $\overline{m} \cdot B_d$ will be hit by positive integers representable by some form of discriminant d upon reduction modulo d. By Theorem 4.2.18, we know that every coset within K_d/B_d is in the image of ω_d and since K_d is the set union of the cosets within K_d/B_d, the proof is complete. □

4.3 The Duplication Theorem of Gauss

To prove one of Gauss's most famous theorems regarding genera, it is expedient to discuss and prove some results about a special case of forms that are ternary instead of just binary forms. Just as in Section 2.2, there are specific nonabelian groups of matrices that play an important rôle in the transformation theory of ternary forms. Let $SL_3(\mathbb{Z})$ denote the set of all 3×3 matrices with integer entries having determinant $= 1$ (the natural generalization of the group $SL_2(\mathbb{Z})$ from Section 2.2). We also work with the "general linear" group $GL_3(\mathbb{Z})$ of all 3×3 matrices with integer entries having determinant $= \pm 1$ which clearly contains $SL_3(\mathbb{Z})$ as a subgroup.

Definition 4.3.1. *An integral ternary quadratic form is a homogeneous polynomial $F(x, y, z) = ax^2 + by^2 + cz^2 + uxy + vyz + wxz$ of degree 2 in three variables x, y, z with fixed integer coefficients a, b, c, u, v, w.*

Definition 4.3.2. *The matrix $\mathbf{M}(F)$ "belonging to" F, with F as above, is the symmetric 3×3 matrix*

$$\mathbf{M}(F) = \begin{pmatrix} a & u/2 & w/2 \\ u/2 & b & v/2 \\ w/2 & v/2 & c \end{pmatrix}. \tag{4.3.1}$$

Just as in Section 2.2, the 1×1 matrix (F) consisting of the ternary form $F(x, y, z)$ as a single entry, is given by the matrix equation $(F) = \begin{pmatrix} x \\ y \\ z \end{pmatrix}^T \cdot \mathbf{M}(F) \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix}$.

Definition 4.3.3. *The determinant $\delta(F)$ of a ternary quadratic form F is defined as the determinant of the matrix $\mathbf{M}(F)$ belonging to F.*

Definition 4.3.4. *Two integral ternary quadratic forms F and G are defined as being equivalent if and only if a matrix $\mathbf{D} \in GL_3(\mathbb{Z})$ exists such that*

$$\mathbf{D}^T \cdot \mathbf{M}(F) \cdot \mathbf{D} = \mathbf{M}(G). \tag{4.3.2}$$

As in Section 2.2, we often abbreviate the relationship between the two forms F and G as given in Definition 4.3.4 by $F\mathbf{D} = G$. There is one important difference between the notion of equivalence introduced in Section 2.2 among binary quadratic forms and that introduced in Definition 4.3.4, namely, the only tranformation matrices allowed in Section 2.2 were unimodular whereas Definition 4.3.4 allows matrices with determinant $= -1$ as well. This does not change the fact that equivalent forms must have the same determinant. Taking determinants in equation (4.3.2) gives

$$\det(\mathbf{D}^T) \cdot \det(\mathbf{M}(F)) \cdot \det(\mathbf{D}) = \det(\mathbf{M}(G)),$$

so $\det(\mathbf{D})^2 \cdot \delta(F) = \delta(G)$ since $\det(\mathbf{D}^T) = \det(\mathbf{D})$. Note that $\det(\mathbf{D})^2 = (\pm 1)^2 = 1$, establishing that equivalent ternary forms have the same determinant. It is also worth noting that if F is an integral ternary form and $\mathbf{D} = (d_{ij}) \in GL_3(\mathbb{Z})$, then the form $F\mathbf{D}$ is an integral ternary form as well. To see this, we note that the form $F\mathbf{D}$ is obtained by replacing x, y, and z in $F(x, y, z)$ by the expressions $d_{11}X + d_{12}Y + d_{13}Z$, $d_{21}X + d_{22}Y + d_{23}Z$, and $d_{31}X + d_{32}Y + d_{33}Z$, respectively, and then combining like terms in X^2, Y^2, Z^2, XY, YZ, and XZ, which will result in all integer coefficients by the closure properties of $\mathbb{Z}$. It is a straightforward exercise to verify that the definition of "equivalence" in Definition 4.3.4 leads to an equivalence relation among all integral ternary quadratic forms of a fixed determinant.

Certain useful facts about "cofactor matrices" will be needed in the sequel and we now develop the basic framework for proving these facts. We restrict ourselves throughout to working with 3×3 matrices with coefficients in $\mathbb{Q}$. The set of all such matrices will be denoted by $M_3(\mathbb{Q})$. Let $\mathbf{I}_3$ denote the 3×3 identity matrix and let $\mathbb{Q}^\times$ denote the set of all nonzero rational numbers. If $\alpha \in \mathbb{Q}$, we let $\alpha \mathbf{I}_3$ denote the 3×3 matrix with diagonal entries all equal to α and all off-diagonal entries equal to zero. It is easy to check that any matrix of the form $\alpha \mathbf{I}_3$ commutes with an arbitrary matrix $\mathbf{M} \in M_3(\mathbb{Q})$ under matrix multiplication, a fact used often in the sequel without further comment.

Definition 4.3.5. *If* $\mathbf{M} = \left(\begin{smallmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} \\ \alpha_{21} & \alpha_{22} & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} \end{smallmatrix}\right) \in M_3(\mathbb{Q})$*, the* (r, s)*-minor submatrix of* $\mathbf{M}$*, denoted by* $\mathbf{M}_{rs}$*, is the* 2×2 *submatrix of* $\mathbf{M}$ *that remains when the entries from row*

r and column s are removed from $\mathbf{M}$. The (r,s)-minor of $\mathbf{M}$, denoted by M_{rs}, is the determinant of $\mathbf{M}_{rs}$. Finally, the (r,s)-cofactor of $\mathbf{M}$, denoted by C_{rs}, is defined as $(-1)^{r+s}M_{rs}$.

For example, consider the matrix $\mathbf{M} = \begin{pmatrix} -6 & \frac{5}{6} & \frac{2}{5} \\ -\frac{1}{2} & 3 & -\frac{2}{3} \\ -\frac{3}{2} & \frac{6}{5} & \frac{4}{5} \end{pmatrix}$. The $(1,1)$-minor submatrix $\mathbf{M}_{11}$ is $\begin{pmatrix} 3 & -\frac{2}{3} \\ \frac{6}{5} & \frac{4}{5} \end{pmatrix}$ and $M_{11} = \begin{vmatrix} 3 & -\frac{2}{3} \\ \frac{6}{5} & \frac{4}{5} \end{vmatrix} = 3 \cdot \frac{4}{5} - \frac{6}{5} \cdot (-\frac{2}{3}) = \frac{16}{5}$. We also have $M_{12} = \begin{vmatrix} -\frac{1}{2} & -\frac{2}{3} \\ -\frac{3}{2} & \frac{4}{5} \end{vmatrix} = (-\frac{1}{2}) \cdot \frac{4}{5} - (-\frac{3}{2}) \cdot (-\frac{2}{3}) = -\frac{7}{5}$, and $M_{13} = \begin{vmatrix} -\frac{1}{2} & 3 \\ -\frac{3}{2} & \frac{6}{5} \end{vmatrix} = (-\frac{1}{2}) \cdot \frac{6}{5} - (-\frac{3}{2}) \cdot 3 = \frac{39}{10}$. The corresponding cofactors are $C_{11} = \frac{16}{5}$, $C_{12} = \frac{7}{5}$, and $C_{13} = \frac{39}{10}$. A famous result due to Laplace shows that the determinant of a 3×3 matrix can be calculated in terms of the minors taken along any given row or down any given column.

Lemma 4.3.6 (Laplace expansion). *If $\mathbf{M} \in M_3(\mathbb{Q})$ is given as in Definition 4.3.5, then $\det(\mathbf{M})$ can be calculated by two equivalent methods.*
Expansion down column s: $\det(\mathbf{M}) = \sum_{r=1}^{3}(-1)^{(r+s)}\alpha_{rs}M_{rs} = \sum_{r=1}^{3} \alpha_{rs}C_{rs}$.
Expansion along row r: $\det(\mathbf{M}) = \sum_{s=1}^{3}(-1)^{(r+s)}\alpha_{rs}M_{rs} = \sum_{s=1}^{3} \alpha_{rs}C_{rs}$.
Further, if $r_1 \neq r_2$, then $\sum_{s=1}^{3}(-1)^{(r_2+s)}\alpha_{r_1 s}M_{r_2 s} = \sum_{s=1}^{3} \alpha_{r_1 s}C_{r_2 s} = 0$.

Expanding the matrix in our example along the first row gives
$\det(\mathbf{M}) = (-6)(\frac{16}{5}) + (\frac{5}{6})(\frac{7}{5}) + (\frac{2}{5})(\frac{39}{10}) = -\frac{2471}{150}$. Of course, expansion along either of the other two rows or down any of the three columns gives the same value for the determinant.

Definition 4.3.7. *The cofactor matrix of $\mathbf{M}$, denoted by $\overline{\mathbf{M}}$, is defined as the matrix which, for all $1 \leq r, s \leq 3$, has $(-1)^{r+s}M_{rs}$ as the row-r, column-s entry. We note that $\overline{\mathbf{M}} \in M_3(\mathbb{Q})$ when $\mathbf{M} \in M_3(\mathbb{Q})$.*

To complete the example above, using the cofactors already computed and calculating the other six, we find that $\overline{\mathbf{M}} = \begin{pmatrix} \frac{16}{5} & \frac{7}{5} & \frac{39}{10} \\ -\frac{14}{75} & -\frac{21}{5} & \frac{119}{20} \\ -\frac{79}{45} & -\frac{21}{5} & -\frac{211}{12} \end{pmatrix}$.

Definition 4.3.8. *The matrix* $\overline{\mathbf{M}}^T$*, which is the transpose of* $\overline{\mathbf{M}}$*, is known as the "adjoint matrix of* $\mathbf{M}$*," and will be denoted by* $\mathrm{Adj}(\mathbf{M})$*.*

Proposition 4.3.9. *If* $\mathbf{M} \in M_3(\mathbb{Q})$*, then* $\mathbf{M} \cdot \mathrm{Adj}(\mathbf{M}) = \delta \mathbf{I}_3$*, where* $\delta = \det(\mathbf{M})$*.*

Proof: Straightforward substitution and matrix multiplication gives

$$\begin{aligned}
\mathbf{M} \cdot \mathrm{Adj}(\mathbf{M}) &= \mathbf{M} \cdot \overline{\mathbf{M}}^T \\
&= \begin{pmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} \\ \alpha_{21} & \alpha_{22} & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} \end{pmatrix} \cdot \begin{pmatrix} M_{11} & -M_{21} & M_{31} \\ -M_{12} & M_{22} & -M_{32} \\ M_{13} & -M_{23} & M_{33} \end{pmatrix} \\
&= \begin{pmatrix} \beta & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \beta \end{pmatrix} \\
&= \beta \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},
\end{aligned}$$

where $\beta = \alpha_{11}M_{11} - \alpha_{12}M_{12} + \alpha_{13}M_{13} = -\alpha_{21}M_{21} + \alpha_{22}M_{22} - \alpha_{23}M_{23} = \alpha_{31}M_{31} - \alpha_{32}M_{32} + \alpha_{33}M_{33}$, the equivalent Laplace expansions of $\det(\mathbf{M})$ by minors by each row in turn, and so $\beta = \delta$. Each off-diagonal entry is easily seen to be zero because of the last statement in Lemma 4.3.6. □

Proposition 4.3.10. *If* $\mathbf{M} \in M_3(\mathbb{Q})$*, with* $\det(\mathbf{M}) = \delta \neq 0$*, then* $\det(\overline{\mathbf{M}}) = \delta^2$*.*

Proof: We have $\mathbf{M} \cdot \overline{\mathbf{M}}^T = \delta \mathbf{I}_3$ by Proposition 4.3.9. Taking determinants of both sides, $\det(\mathbf{M} \cdot \overline{\mathbf{M}}^T) = \det(\delta \mathbf{I}_3)$, so $\det(\mathbf{M}) \cdot \det(\overline{\mathbf{M}}^T) = \delta \cdot \left| \begin{smallmatrix} \delta & 0 \\ 0 & \delta \end{smallmatrix} \right| = \delta^3$. Since $\det(\overline{\mathbf{M}}^T) = \det(\overline{\mathbf{M}})$, then $\delta \cdot \det(\overline{\mathbf{M}}) = \delta^3$. Since $\delta \neq 0$, we conclude that $\det(\overline{\mathbf{M}}) = \delta^2$. □

Proposition 4.3.11. *If* $\mathbf{M} \in M_3(\mathbb{Q})$*, with* $\det(\mathbf{M}) = \delta \neq 0$*, then* $\overline{\mathbf{M}} \cdot \overline{\overline{\mathbf{M}}}^T = \delta^2 \mathbf{I}_3$*.*

Proof: Again, $\mathbf{M} \cdot \overline{\mathbf{M}}^T = \det(\mathbf{M}) \cdot \mathbf{I}_3$ by Proposition 4.3.9. Therefore, by replacing matrix $\mathbf{M}$ with matrix $\overline{\mathbf{M}}$, we have $\overline{\mathbf{M}} \cdot \overline{\overline{\mathbf{M}}}^T = \det(\overline{\mathbf{M}}) \cdot \mathbf{I}_3 = \delta^2 \mathbf{I}_3$, with the last equality holding by Proposition 4.3.10. □

Proposition 4.3.12. *If* $\mathbf{M} \in M_3(\mathbb{Q})$*, with* $\det(\mathbf{M}) = \delta \neq 0$*, then* $\overline{\overline{\mathbf{M}}} = (\delta \mathbf{I}_3) \cdot \mathbf{M}$*.*

Proof: First, the matrix $\overline{\mathbf{M}}^T$ is invertible, with its inverse given by Proposition 4.3.9 as $(\frac{1}{\delta}\mathbf{I}_3) \cdot \mathbf{M}$. Applying the transpose operation to both sides of the matrix relation in Proposition 4.3.11 yields the relation i): $\overline{\overline{\mathbf{M}}} \cdot \overline{\mathbf{M}}^T = \delta^2 \mathbf{I}_3$. Multiplying both sides of the matrix relation in Proposition 4.3.9 by $\delta \mathbf{I}_3$ gives ii): $((\delta \mathbf{I}_3) \cdot \mathbf{M}) \cdot \overline{\mathbf{M}}^T = \delta^2 \mathbf{I}_3$. Multiplying on the right by the inverse of $\overline{\mathbf{M}}^T$ in both equations i) and ii), and then comparing, completes the proof. □

Proposition 4.3.13. *The cofactor matrix of a product is the product of the cofactor matrices: If* $\mathbf{M}, \mathbf{N} \in M_3(\mathbb{Q})$*, with* $\det(\mathbf{M}) = \delta \neq 0$ *and* $\det(\mathbf{N}) = \gamma \neq 0$*, then* $\overline{\mathbf{M} \cdot \mathbf{N}} = \overline{\mathbf{M}} \cdot \overline{\mathbf{N}}$*.*

Proof: Applying the transpose operation to both sides of the matrix relation in Proposition 4.3.9 yields $\overline{\mathbf{M}} \cdot \mathbf{M}^T = \delta \mathbf{I}_3$, and so $\mathbf{M}^T = (\overline{\mathbf{M}})^{-1} \cdot (\delta \mathbf{I}_3)$. Similarly, $\mathbf{N}^T = (\overline{\mathbf{N}})^{-1} \cdot (\gamma \mathbf{I}_3)$. From Proposition 4.3.9, we have $(\mathbf{MN}) \cdot (\overline{\mathbf{MN}})^T = \det(\mathbf{MN}) \cdot \mathbf{I}_3 = (\delta \mathbf{I}_3) \cdot (\gamma \mathbf{I}_3)$. Applying the transpose operation to both sides gives $\overline{\mathbf{MN}} \cdot \mathbf{N}^T \cdot \mathbf{M}^T = (\delta \mathbf{I}_3) \cdot (\gamma \mathbf{I}_3)$. Using the expressions for $\mathbf{M}^T$ and $\mathbf{N}^T$ above, and recalling that the matrix $\gamma \mathbf{I}_3$ commutes with everything, we conclude that $\overline{\mathbf{MN}} \cdot (\overline{\mathbf{N}})^{-1} \cdot (\overline{\mathbf{M}})^{-1} = \mathbf{I}_3$, which completes the proof. □

Proposition 4.3.14. *If* $\mathbf{M} \in M_3(\mathbb{Q})$*, with* $\det(\mathbf{M}) = \delta \neq 0$*, then* $\overline{\mathbf{M}^T} = \overline{\mathbf{M}}^T$*.*

Proof: The matrix $\overline{\mathbf{M}}^T$ is invertible, with inverse equal to $(\frac{1}{\delta}\mathbf{I}_3) \cdot \mathbf{M}$. From Proposition 4.3.9, we have $\mathbf{M} \cdot \overline{\mathbf{M}}^T = \delta \mathbf{I}_3$, and replacing $\mathbf{M}$ by $\mathbf{M}^T$ gives $\mathbf{M}^T \cdot \overline{\mathbf{M}^T}^T = \det(\mathbf{M}^T)\mathbf{I}_3 = \delta \mathbf{I}_3$. Applying the transpose operation to both sides gives $\overline{\mathbf{M}^T} \cdot \mathbf{M} = \delta \mathbf{I}_3$, and we now see that the matrix $\overline{\mathbf{M}^T}$ is invertible with inverse equal to $(\frac{1}{\delta}\mathbf{I}_3) \cdot \mathbf{M}$. Since the two matrices $\overline{\mathbf{M}}^T$ and $\overline{\mathbf{M}^T}$ have the same inverse, they are equal. □

As a first step towards proving the Duplication Theorem, we develop a reduction process for integral ternary forms that closely resembles the reduction theory already developed for binary forms in Section 2.3. To summarize from that section: We start with an arbitrary form. After a finite number of steps, we produce an equivalent form whose coefficients satisfy certain inequalities. The steps alternate between two types: The first type decreases the size of a and leaves $|b|$ unchanged. The second type adjusts the size of $|b|$, but does not change the value of a. This same basic strategy will be applied to ternary forms!

Let F be an integral ternary form as given in Definition 4.3.1 and $\mathbf{M}(F) \in M_3(\mathbb{Q})$ the matrix belonging to F as given in Definition 4.3.2. We make the standing assumption that $\delta(F) \neq 0$. We also consider the cofactor matrix $\overline{\mathbf{M}(F)}$, and we designate its entries in the form

$$\overline{\mathbf{M}(F)} = \begin{pmatrix} A & U/2 & W/2 \\ U/2 & B & V/2 \\ W/2 & V/2 & C \end{pmatrix},$$

namely, we use the same letters as in $\mathbf{M}(F)$, only capitalized (this is a workable convention since this matrix is symmetric). By definition, it is easy to verify that $A = bc - v^2/4$, $B = ac - w^2/4$, and $C = ab - u^2/4$. An observation we make now, which will be important later, is that the coefficient C here is equal to an integer divided by 4, given that the corresponding form F is *integral*. The reduction process starts with an arbitrary integral ternary form F with $\delta(F) \in \mathbb{Q}^{\times}$, and each new form produced will be equivalent to F (see Definition 4.3.4) and will thus have the same nonzero determinant. For each integral ternary form F' that arises in the reduction process, we will keep track of the entries in both $\mathbf{M}(F')$ and $\overline{\mathbf{M}(F')}$. Each step taken in the reduction process is of one of two types and we now consider these two types in detail, applied to a given form F with coefficients as in Definition 4.3.1.

Transformation of "type a": Assuming that $\sqrt{|u^2 - 4ab|/3} < |a|$, we do the following: Consider the *binary* quadratic form $ax^2 + uxy + by^2$ (this is the "piece" of F involving only x and y). According to Comment 2.4.2, there is an element $\mathbf{E} = \left(\begin{smallmatrix} j & k \\ l & m \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ which, when applied to this binary form, produces a new form (a_1, u_1, b_1) in the same class such that

$$|a_1| \leq \sqrt{\frac{|u_1^2 - 4a_1b_1|}{3}} = \sqrt{\frac{|u^2 - 4ab|}{3}} < |a|. \tag{4.3.3}$$

We now embed $\mathbf{E}$ into a 3×3 matrix $\mathbf{D}_1$ as follows:

$$\mathbf{D}_1 = \left(\begin{smallmatrix} j & k & 0 \\ l & m & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right),$$

and note that $\mathbf{D}_1 \in GL_3(\mathbb{Z})$ (in fact, $\det(\mathbf{D}_1) = 1$). When we now consider the new integral ternary form $F_1 = F\mathbf{D}_1$, we easily compute the corresponding matrix $\mathbf{M}(F_1)$ to be

$$\mathbf{M}(F_1) = \left(\begin{smallmatrix} a_1 & u_1/2 & (wj+vl)/2 \\ u_1/2 & b_1 & (wk+vm)/2 \\ (wj+vl)/2 & (wk+vm)/2 & c \end{smallmatrix}\right).$$

The convention introduced above is used to label the entries of $\overline{\mathbf{M}(F_1)}$, namely, we set

$$\overline{\mathbf{M}(F_1)} = \left(\begin{smallmatrix} A_1 & U_1/2 & W_1/2 \\ U_1/2 & B_1 & V_1/2 \\ W_1/2 & V_1/2 & C_1 \end{smallmatrix}\right).$$

By definition, $C_1 = a_1b_1 - \frac{u_1^2}{4}$, and from above $u_1^2 - 4a_1b_1 = u^2 - 4ab$, so that $C_1 = C$. To summarize: If $\sqrt{|u^2 - 4ab|/3} < |a|$, then a transformation of "type a" is applied to produce a new ternary form F_1 such that $|a_1| < |a|$, $C_1 = C$, and F_1 satisfies "condition a" (which we define immediately below).

Definition 4.3.15. *Given an integral ternary form F with $\delta(F) \neq 0$ and with corresponding matrices $\mathbf{M}(F)$ and $\overline{\mathbf{M}(F)}$, we say that F satisfies "condition a" if $|a| \leq \sqrt{\frac{|u^2-4ab|}{3}}$ and F satisfies "condition C" if $|C| \leq \sqrt{\frac{|V^2-4BC|}{3}}$.*

Transformation of "type C ": Starting with F as in Definition 4.3.1, and assuming that $\sqrt{|V^2-4BC|/3} < |C|$ (in other words, we assume that F does not satisfy condition C), we do the following: Consider the *binary* quadratic form $Bx^2 + Vxy + Cy^2$. By Comment 2.4.2, there is an element $\mathbf{E} = \left(\begin{smallmatrix} j & k \\ l & m \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ which, when applied to this binary form, produces a new form (B_1, V_1, C_1) in the same class such that

$$|C_1| \leq \sqrt{\frac{|V_1^2 - 4B_1C_1|}{3}} = \sqrt{\frac{|V^2-4BC|}{3}} < |C|. \tag{4.3.4}$$

We now embed $\mathbf{E}$ into a 3×3 matrix $\mathbf{D}_1$ as follows:

$$\mathbf{D}_1 = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & j & k \\ 0 & l & m \end{smallmatrix}\right) \in SL_3(\mathbb{Z}).$$

A simple computation gives

$$\overline{\mathbf{D}_1} = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & m & -l \\ 0 & -k & j \end{smallmatrix}\right),$$

which is also an element of $SL_3(\mathbb{Z})$. We now consider the new integral ternary form $F_1 = F\overline{\mathbf{D}_1}$ with corresponding matrix $\mathbf{M}(F_1) = \overline{\mathbf{D}_1}^T \cdot \mathbf{M}(F) \cdot \overline{\mathbf{D}_1}$. A simple computation now shows that $a_1 = a$. Using both Propositions 4.3.13 and 4.3.14, we find that $\overline{\mathbf{M}(F_1)} = \overline{\overline{\mathbf{D}_1}}^T \cdot \overline{\mathbf{M}(F)} \cdot \overline{\overline{\mathbf{D}_1}}$. By Proposition 4.3.12, we have $\overline{\overline{\mathbf{D}_1}} = \mathbf{D}_1$ since $\det(\mathbf{D}_1) = 1$, and we conclude that $\overline{\mathbf{M}(F_1)} = \mathbf{D}_1^T \cdot \overline{\mathbf{M}(F)} \cdot \mathbf{D}_1$. A direct computation now shows that

$$\overline{\mathbf{M}(F_1)} = \begin{pmatrix} A & (Uj+Wl)/2 & (Uk+Wm)/2 \\ (Uj+Wl)/2 & B_1 & V_1/2 \\ (Uk+Wm)/2 & V_1/2 & C_1 \end{pmatrix}.$$

To summarize: If $\sqrt{|V^2 - 4BC|/3} < |C|$, then a transformation of "type C" is applied to produce a new ternary form F_1 such that $a_1 = a$, $|C_1| < |C|$, and F_1 satisfies condition C.

Definition 4.3.16. *Given an integral ternary form F with $\delta(F) \neq 0$ and with corresponding matrices $\mathbf{M}(F)$ and $\overline{\mathbf{M}(F)}$, we say that F is "reduced" if it simultaneously satisfies both conditions* a *and* C.

Theorem 4.3.17. *Any given integral ternary form with $\delta(F) \neq 0$ is equivalent to a reduced such form.*

Proof: We present this proof in the form of an algorithm. Start with F, $\mathbf{M}(F)$, and $\overline{\mathbf{M}(F)}$ as above. If F satisfies condition a and condition C, then F is reduced, and we are done. Otherwise, if condition a does not hold for F, we apply a "type a" transformation. If F does satisfy condition a, but does not satisfy condition C, we apply a "type C" transformation. Either way, we now have a new integral ternary form F_1 ("new" here meaning that $F_1 \neq F$, since either $|a_1| < |a|$ or $|C_1| < |C|$). The crucial observation here is that this algorithm must produce a reduced form after a finite number of steps. Each step we are forced to take when the current form is not reduced brings either a strict decrease in $|a|$ or in $|C|$, with the other quantity staying the same. Each time the a-coefficient is changed, $|a|$ decreases by at least 1 and each time the C-coefficient is changed, $|C|$ decreases by at least $\frac{1}{4}$. If $|a| = 0$ for the current form and it is not reduced, one last transformation of "type C" guarantees a new form that is reduced. If $|C| = 0$ for the current form and it is not reduced, one last transformation of "type a" guarantees a new form that is reduced. □

Corollary 4.3.18. *Every integral ternary quadratic form of nonzero determinant δ is equivalent to a form $F = ax^2 + by^2 + cz^2 + uxy + vyz + wxz$ that is reduced, and the following inequalities hold for the coefficients of the reduced form F:*
(i) $|a| \leq \sqrt{|u^2 - 4ab|/3}$, (ii) $|u^2 - 4ab| \leq \sqrt{64|a\delta|/3}$, *and* (iii) $|a| \leq \frac{4}{3}\sqrt[3]{|\delta|}$.

Proof: By Theorem 4.3.17, we already know that any given integral ternary form with nonzero determinant δ is equivalent to a reduced form F, and the inequality $|a| \leq \sqrt{|u^2 - 4ab|/3}$ holds by definition for a reduced ternary form. All we need to prove is that the other two inequalities in (ii) and (iii) above also hold for a reduced form F. The other inequality that holds, by definition, for a reduced ternary form F involves the coefficients from $\overline{\mathbf{M}(F)}$ rather than $\mathbf{M}(F)$, namely, $|C| \leq \sqrt{|V^2 - 4BC|/3}$. Recalling that $C = ab - \frac{u^2}{4}$, we see that $4|C| = |u^2 - 4ab|$. The $(1,1)$-entry of $\mathbf{M}(F)$ is a and the $(1,1)$-entry of $\overline{\overline{\mathbf{M}(F)}}$ is equal to $BC - \frac{V^2}{4}$. From Proposition 4.3.12, we have $\overline{\overline{\mathbf{M}(F)}} = (\delta\mathbf{I}_3) \cdot \mathbf{M}(F)$ since $\delta(F) = \delta$, and this implies that $BC - \frac{V^2}{4} = \delta a$. We may therefore translate the inequality involving $|C|$ above into $|u^2 - 4ab| \leq 4\sqrt{\frac{4|\delta a|}{3}}$, which establishes the inequality in (ii). The inequality in (iii) is obtained by combining the inequalities in (i) and (ii). Squaring both sides of

(i) and comparing with (ii) gives

$$|a|^2 \leq \frac{|u^2 - 4ab|}{3} \leq \frac{1}{3}\sqrt{\frac{64|a\delta|}{3}}.$$

Squaring again gives

$$|a|^4 \leq \frac{64|a\delta|}{27},$$

and dividing both sides by $|a|$ gives $|a|^3 \leq \frac{64}{27}|\delta|$. We obtain (iii) upon taking the cube root of both sides of this last inequality. □

Theorem 4.3.19. *Every integral ternary quadratic form of determinant $-\frac{1}{4}$ is equivalent to the form $y^2 - xz$.*

Proof: Any integral ternary quadratic form of determinant $-\frac{1}{4}$ that we start with is equivalent to a reduced ternary form F whose a-coefficient satisfies inequality (iii) in Corollary 4.3.18: $|a| \leq \frac{4}{3}\sqrt[3]{\frac{1}{4}} \approx .84$. Since a is an integer, we deduce that $a = 0$. Inequality (ii) in Corollary 4.3.18 now states that $|u^2| \leq 0$, which implies that the u-coefficient of F is equal to 0 as well. The corresponding matrix $\mathbf{M}(F)$ looks like

$$\mathbf{M}(F) = \begin{pmatrix} 0 & 0 & w/2 \\ 0 & b & v/2 \\ w/2 & v/2 & c \end{pmatrix}.$$

We have $\delta(F) = -\frac{1}{4}$, and when we solve for $\det(\mathbf{M}(F)) = -\frac{1}{4}$ we obtain $\frac{w}{2}(-\frac{bw}{2}) = -\frac{1}{4}$, which implies that $bw^2 = 1$, and so $b = 1$ and $w = \pm 1$, since b and w are both integers. So far we know that F may be written in the form $F = y^2 + cz^2 + vyz \pm xz$, and we only need a slight adjustment to complete the proof of this theorem. Assume first that $w = -1$. Let

$$\mathbf{D} = \left(\begin{smallmatrix} 1 & m & n \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right),$$

where m and n are arbitrarily chosen integers for the time being. No matter how m and n are chosen, we still have $\mathbf{D} \in GL_3(\mathbb{Z})$ since $\det(\mathbf{D}) = 1$. The ternary form F is equivalent to the ternary form $G = F\mathbf{D}$, whose corresponding matrix has the form

$$\mathbf{M}(G) = \mathbf{D}^T \cdot \mathbf{M}(F) \cdot \mathbf{D} = \left(\begin{smallmatrix} 0 & 0 & -1/2 \\ 0 & 1 & (v-m)/2 \\ -1/2 & (v-m)/2 & c-n \end{smallmatrix}\right).$$

Choosing $m = v$ and $n = c$ gives the form $G = y^2 - xz$, and since the ternary form we started with is equivalent to F, it is also equivalent to G by transitivity. If we now consider the case where $w = 1$ instead, the same argument goes through using rather the matrix

$$\mathbf{D} = \left(\begin{smallmatrix} 1 & m & n \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{smallmatrix}\right),$$

whose determinant is equal to -1 no matter which values are chosen for m and n. □

Proposition 4.3.20. *If d is a fixed fundamental discriminant and F is a binary quadratic form of discriminant d that lies in the principal genus of $\mathcal{H}(d)$, then there exists a matrix*

$$\mathbf{D} = \left(\begin{smallmatrix} r_1 & s_1 & t_1 \\ r_2 & s_2 & t_2 \\ r_3 & s_3 & t_3 \end{smallmatrix}\right) \in GL_3(\mathbb{Z})$$

such that

$$F(x,y) = (r_2x + s_2y)^2 - (r_1x + s_1y)(r_3x + s_3y)$$

and

$$\gcd(r_1s_2 - r_2s_1, d) = 1.$$

Proof: If $F = (a,b,c)$, we claim that there exist integers l, m, n such that $\det(\mathbf{A}) = -\frac{1}{4}$, where

$$\mathbf{A} = \begin{pmatrix} a & b/2 & l/2 \\ b/2 & c & m/2 \\ l/2 & m/2 & n \end{pmatrix}.$$

To see this, we calculate the determinant of $\mathbf{A}$ by expanding along the first row: $\det(\mathbf{A}) = a \cdot \det\begin{pmatrix} c & m/2 \\ m/2 & n \end{pmatrix} - \frac{b}{2} \cdot \det\begin{pmatrix} b/2 & m/2 \\ l/2 & n \end{pmatrix} + \frac{l}{2} \cdot \det\begin{pmatrix} b/2 & c \\ l/2 & m/2 \end{pmatrix} = a(cn - \frac{m^2}{4}) - \frac{b}{2}(\frac{bn}{2} - \frac{lm}{4}) + \frac{l}{2}(\frac{bm}{4} - \frac{cl}{2}) = acn - \frac{am^2}{4} - \frac{b^2n}{4} + \frac{blm}{4} - \frac{cl^2}{4} = -\frac{1}{4}(am^2 - blm + cl^2 + n(b^2 - 4ac)) = -\frac{1}{4}(F(m,-l) + nd)$. By Corollary 4.2.16, there exist integers m and $-l$ such that $F(m,-l)$ is a positive integer congruent to 1 modulo d, which means in particular that with m and $-l$ so chosen, $F(m,-l) - 1 = -nd$ for some integer n. Therefore, for these integer values of l, m, and n, we have $\det(\mathbf{A}) = -\frac{1}{4}$, which proves the claim made above.

If $\mathbf{M}$ is the matrix belonging to $y^2 - xz$, we have (recall Definition 4.3.2):

$$\mathbf{M} = \begin{pmatrix} 0 & 0 & -1/2 \\ 0 & 1 & 0 \\ -1/2 & 0 & 0 \end{pmatrix}.$$

By Theorem 4.3.19, there exists a matrix $\mathbf{D} \in GL_3(\mathbb{Z})$ such that $\mathbf{D}^T \cdot \mathbf{M} \cdot \mathbf{D} = \mathbf{A}$, and we set

$$\mathbf{D} = \left(\begin{smallmatrix} r_1 & s_1 & t_1 \\ r_2 & s_2 & t_2 \\ r_3 & s_3 & t_3 \end{smallmatrix}\right).$$

A direct computation, substituting the above expression for $\mathbf{A}$, gives us

$$\begin{aligned}(F(x,y)) &= \left(\begin{smallmatrix} x \\ y \\ 0 \end{smallmatrix}\right)^T \cdot \mathbf{A} \cdot \left(\begin{smallmatrix} x \\ y \\ 0 \end{smallmatrix}\right) \\ &= \left(\begin{smallmatrix} x \\ y \\ 0 \end{smallmatrix}\right)^T \cdot \mathbf{D}^T \cdot \mathbf{M} \cdot \mathbf{D} \cdot \left(\begin{smallmatrix} x \\ y \\ 0 \end{smallmatrix}\right) \qquad (4.3.5) \\ &= ((r_2x + s_2y)^2 - (r_1x + s_1y)(r_3x + s_3y)).\end{aligned}$$

The proof is now complete, assuming that $\gcd(r_1s_2 - r_2s_1, d) = 1$. However, if the minor $\left|\begin{smallmatrix} r_1 & s_1 \\ r_2 & s_2 \end{smallmatrix}\right|$ is not relatively prime to d, we need to modify $\mathbf{D}$. In this case, we will instead use $\mathbf{D}' = \mathbf{ED}$, where $\mathbf{E} \in SL_3(\mathbb{Z})$ satisfies the matrix equation $\mathbf{E}^T \cdot \mathbf{M} \cdot \mathbf{E} = \mathbf{M}$.

Let $\mathbf{J} = \left(\begin{smallmatrix} e & f \\ g & h \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$. Define $\mathbf{E_J}$ with integer entries dependent upon $\mathbf{J}$'s entries:

$$\mathbf{E_J} = \left(\begin{smallmatrix} e^2 & 2eg & g^2 \\ ef & eh+fg & gh \\ f^2 & 2fh & h^2 \end{smallmatrix}\right). \qquad (4.3.6)$$

Computation shows that

$$\mathbf{E_J}^T \cdot \mathbf{M} \cdot \mathbf{E_J} = \left(\begin{smallmatrix} 0 & 0 & -\frac{1}{2}(e^2h^2-2efgh+f^2g^2) \\ 0 & e^2h^2-2efgh+f^2g^2 & 0 \\ -\frac{1}{2}(e^2h^2-2efgh+f^2g^2) & 0 & 0 \end{smallmatrix}\right),$$

where, using the fact that $eh - fg = 1$, we have $e^2h^2 - 2efgh + f^2g^2 = (eh)^2 - 2(eh)fg + f^2g^2 = (1 + fg)^2 - 2(1 + fg)fg + f^2g^2 = f^2g^2 + 2fg + 1 - 2f^2g^2 - 2fg + f^2g^2 = 1$.

Therefore the other two nonzero entries are $-\frac{1}{2}$ and the matrix on the right-hand side above is $\mathbf{M}$ as desired. A further computation confirms that $\det(\mathbf{E_J}) = 1$: Expanding by minors using the first row, $\det(\mathbf{E_J}) = e^2((eh+fg)h^2 - 2fhgh) - 2eg(efh^2 - f^2gh) + g^2(2fhef - f^2(eh+fg)) = e^3h^3 - 3e^2fgh^2 + 3ef^2g^2h - f^3g^3 = (eh)^3 - 3(eh)^2fg + 3(eh)f^2g^2 - f^3g^3 = (1+fg)^3 - 3(1+fg)^2fg + 3(1+fg)f^2g^2 - f^3g^3 = f^3g^3 + 3f^2g^2 + 3fg + 1 - 3f^3g^3 - 6f^2g^2 - 3fg + 3f^3g^3 + 3f^2g^2 - f^3g^3 = 1$. This computation thus also verifies that $\mathbf{E_J} \in SL_3(\mathbb{Z})$.

Let $\mathbf{D'} = \mathbf{E_J}\mathbf{D}$, where $\mathbf{J}$ is still to be chosen, and denote the entries of $\mathbf{D'}$ by r'_i, s'_i, t'_i to correspond to the notation for $\mathbf{D}$'s entries. The minor

$$\begin{vmatrix} r'_1 & s'_1 \\ r'_2 & s'_2 \end{vmatrix}$$

is the final entry in the cofactor matrix

$$\overline{\mathbf{D'}} = \overline{\mathbf{E_J}}\,\overline{\mathbf{D}} = \begin{pmatrix} \vdots & \vdots & \vdots \\ 2eg^2h - g^2(eh+fg) & -(e^2gh - efg^2) & e^2(eh+fg) - 2e^2fg \end{pmatrix} \overline{\mathbf{D}} = \begin{pmatrix} \vdots & \vdots & \vdots \\ g^2 & -eg & e^2 \end{pmatrix} \overline{\mathbf{D}},$$

where the entries in the last row of $\overline{\mathbf{E_J}}$ simplify as shown because $eh - fg = 1$. We have $2eg^2h - g^2(eh+fg) = (eh)g^2 - fg^3 = (1+fg)g^2 - fg^3 = g^2$. Also $-(e^2gh - efg^2) = -eg(eh - fg) = -eg$. Finally $e^2(eh+fg) - 2e^2fg = e^2(eh+fg-2fg) = e^2(eh-fg) = e^2$. This matrix equation means $r'_1s'_2 - r'_2s'_1 = T_1g^2 - T_2eg + T_3e^2$, where the T_i are the entries in the last column of $\overline{\mathbf{D}}$. Calculating $\det(\mathbf{D})$ by expansion using the third column of $\mathbf{D}$, we find that

$$\det(\mathbf{D}) = t_1T_1 - t_2T_2 + t_3T_3 = \pm 1$$

(recall that $\mathbf{D} \in GL_3(\mathbb{Z})$), so $\gcd(T_1, T_2, T_3) = 1$ by Theorem 1.1.3. Since (T_1, T_2, T_3) is thus a primitive binary quadratic form (in the variables e and g), by Lemma 3.1.7 we can select e, g, and $\mathbf{J}$ such that $\gcd(r'_1 s'_2 - r'_2 s'_1, d) = 1$. Because $(\mathbf{D}')^T \cdot \mathbf{M} \cdot \mathbf{D}' = \mathbf{A}$, equations (4.3.5) are as valid for $\mathbf{D}'$ as they are for $\mathbf{D}$, so this completes the proof. □

Theorem 4.3.21. *If d is a fixed fundamental discriminant and F is a binary quadratic form of discriminant d that lies in the principal genus of $\mathcal{H}(d)$, then the form F is equivalent to a form (m^2, b, c), with $m \in \mathbb{Z}^+$ and $\gcd(m, d) = 1$.*

Proof: By Proposition 4.3.20, we know that there exist $r_1, r_2, r_3, s_1, s_2, s_3 \in \mathbb{Z}$ with $\gcd(r_1 s_2 - r_2 s_1, d) = 1$ such that $F(x, y) = (r_2 x + s_2 y)^2 - (r_1 x + s_1 y)(r_3 x + s_3 y)$. If $(x, y) = (-s_1, r_1)$, then $F(-s_1, r_1) = (r_2(-s_1) + s_2 r_1)^2 - (r_1(-s_1) + s_1 r_1)(r_3(-s_1) + s_3 r_1) = (r_1 s_2 - r_2 s_1)^2$. We know that $r_1 s_2 - r_2 s_1 \neq 0$ since $\gcd(r_1 s_2 - r_2 s_1, d) = 1$ and $|d| \geq 3$. If $n = |r_1 s_2 - r_2 s_1|$, we may summarize as follows: There exist integers $r, t \in \mathbb{Z}$ such that $F(r, t) = n^2$, with $n \in \mathbb{Z}^+$ and $\gcd(n, d) = 1$. If $e = \gcd(r, t)$, we know there exist $s, u \in \mathbb{Z}$ with $es = r$, $eu = t$, and $\gcd(s, u) = 1$. We then have $F(s, u) \cdot e^2 = n^2$, and so $e^2 \mid n^2$, which implies that $e \mid n$. Setting $em = n$, we conclude that $F(s, u) = m^2$, $m \in \mathbb{Z}^+$, $\gcd(m, d) = 1$, and this representation of m^2 by F is *proper* since $\gcd(s, u) = 1$. We now apply Theorem 2.2.4 to conclude that F is equivalent to the form (m^2, b, c) for some $b, c \in \mathbb{Z}$, with $m \in \mathbb{Z}^+$ and $\gcd(m, d) = 1$.
□

The Duplication Theorem (Gauss): *If d is a fundamental discriminant, then we have $\ker(\omega_d) = \mathcal{S}(d)$.*

Proof: The inclusion $\mathcal{S}(d) \subseteq \ker(\omega_d)$ is immediate because every element of K_d/B_d has order 1 or 2 and every element in $\mathcal{S}(d)$ is a square by definition. To show the opposite inclusion, let $\mathcal{C} \in \mathcal{H}(d)$ be chosen such that $\omega_d(\mathcal{C})= \overline{1} \cdot B_d$, that is, let $\mathcal{C}$ be a class in the principal genus. By Theorem 4.3.21, the class $\mathcal{C}$ contains a form (m^2, b, c), where m is a positive integer such that $\gcd(m, d) = 1$. Since the form (m^2, b, c) has discriminant d, so does the form (m, b, mc). Let $\mathcal{D} \in \mathcal{H}(d)$ be the class to which the form (m, b, mc) belongs. By Definition 3.1.1, the form (m, b, mc) is concordant with itself, and by Definition 3.1.4, we have $(m, b, mc) * (m, b, mc) = (m^2, b, c)$. This implies that $\mathcal{D}^2 = \mathcal{C}$, which shows that $\mathcal{C} \in \mathcal{S}(d)$, completing the proof of Gauss's Duplication Theorem. □

REFERENCES

[Co] D. Cox, Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication, John Wiley & Sons, Inc., New York, 1989.

[Da] H. Davenport, The Higher Arithmetic, An Introduction to the Theory of Numbers, Cambridge University Press, New York, 7th ed., 1999.

[DF] D. Dummit and R. Foote, Abstract Algebra, John Wiley & Sons, Inc., New York, 3rd ed., 2004.

[Eis] The On-Line Encyclopedia of Integer Sequences, http://oeis.org, OEIS Foundation, Inc., 2013.

[Fl] D. Flath, Introduction to Number Theory, John Wiley & Sons, Inc., New York, 1989.

[Ga] C. F. Gauss, Disquisitiones Arithmeticae, Yale University Press, New Haven, 1966.

[La] E. Landau, Elementary Number Theory, Chelsea Publishing Company, New York, 1958.

[Or] H. Orde, On Dirichlet's class number formula, J. London Math. Society (2), 18 (1978), 409–420.

[Ta1] B. Tangedal, Reduktionstheorie, Unpublished Notes, UNCG, 2011.

[Ta2] B. Tangedal, Dirichlet Characters and the Kronecker Symbol, Unpublished Notes, UNCG, 2011.

[Ta3] B. Tangedal, Understanding Genus Theory, Unpublished Notes, UNCG, 2011.

[Za] D. Zagier, Zetafunktionen und quadratische Körper, Springer-Verlag, Berlin, 1981.

APPENDIX A
PARI CODE

The PARI code below was developed and tested under GP/PARI Version 2.3.4 (released) running on the Windows 7 operating system. As almost all the commands and features used are basic and stable, the code should run equally well under newer (and even older) versions of PARI and/or on other operating systems. At most, only minor changes should be required.

A.1 Code to Reduce a Form Having a Negative Discriminant

```
reduce_neg(a,b,c,verbose)=
{aa = a; bb = b; cc = c; d = bb^2 - 4*aa*cc; trans = 0; not_yet = 1;
 if(verbose, print("The discriminant is ", d, "."));
 if(d>=0,
   if(verbose,
     print("This form does not have a negative discriminant."));
   return([]),
   if(aa<0,
     if(verbose,
       print("Multiplying coefficients by -1, ",
         "to get a positive definite form."));
     aa = -aa; bb = -bb; cc = -cc);
   while(cc<aa || abs(bb)>aa || (aa==cc && bb<0) ||
    (bb==-aa && aa<cc),
     if(verbose && not_yet,
       print("Reducing (", aa, ",", bb, ",", cc, ")...");
       not_yet = 0;);
     if(cc<aa || (aa==cc && bb<0),
       if(verbose, print("Applying transformation 1:"));
       trans++;
       tmp = aa; aa = cc; bb = -bb; cc = tmp;
       if(verbose, print("(", aa, ",", bb, ",", cc,")")));
     if(abs(bb)>aa || (bb==-aa && aa<cc),
       if(verbose, print("Applying transformation 2:"));
       trans++;
       u = bb\(2*aa);
       tmp = bb - 2*u*aa;
       if(abs(tmp)<=aa,
         bb = tmp,
         u++; bb = bb - 2*u*aa);
       cc = (bb^2 - d)/(4*aa);
       if(verbose, print("(", aa, ",", bb, ",", cc,")")));
   ) /* end of loop */
 );
   if(verbose,
     if(trans, print("Transformations used: ", trans),
               print("The given form is already reduced.")));
   return([aa,bb,cc])
}
```

A.2 Code to Calculate All Reduced Forms for a Given Negative Discriminant

```
/* PARI (Version 2.3.4) Program prpdf:                              */
/*           Print Reduced Positive Definite Forms                  */
/*                                                                  */
/* If the program is stored in the file prpdf.gp in the current     */
/* directory, begin a PARI session and load the program with command*/
/* read("prpdf.gp").                                                */
/* Then run the program like this:  prpdf  or  prpdf()              */
/* After prompt, input a negative discriminant d,                   */
/* congruent to 0 or 1 (mod 4)                                      */
/* Simply press the <Enter> key to exit.                            */
/* Program also exits if non-integer input is encountered.          */
/* The program outputs reduced positive definite forms (a,b,c) as   */
/* described in Harold Davenport's THE HIGHER ARITHMETIC.           */
/* (See Table II, p. 144.)                                          */
/* This program prints both primitive and imprimitive reduced forms.*/
/* Each imprimitive form is followed by an asterisk ("*").          */
/* The class number (count of primitive forms) is also printed.     */
/* (The function h(d) is called to verify the class number by using */
/* the formula for when -d is a prime congruent to 3 (mod 4).)      */
/* The order of the output is by increasing absolute value of b,    */
/* unlike in Davenport's Table II, where the forms are sorted by    */
/* increasing a values.                                             */
/* Returns all forms from last discriminant                         */
/* processed in a vector, "forms", of vectors.                      */
/*                                                                  */
prpdf(verbose)=
{local(a, b, c, d, D, ac, b_max, b_start, class_no,
   class_no_by_formula, prim, imprim_forms, r, g, cpg, cstr, forms);
 forms=[];
 while(1, print;
   print1("Input a negative discriminant ",
     "(Just press <Enter> to exit): ");
   d = input();
   if(type(d)<>"t_INT" || d==0, print("Exiting program...");
     return(forms),
     if(d>0,
       print("** The positive integer input will be treated as ",
         "negative.");
       d = -d));
   if(d%4>1,
     print("** Discriminant must be congruent to 0 or 1 (mod 4)",
       "--Try again."),
     print();
     print("The reduced positive definite form(s) for discriminant ",
  "d = ",d,":");
forms = [];
class_no = 0;
imprim_forms = 0;
D = -d;
b_max = floor(sqrt(D/3));
if(D%4==0, b_start = 0, b_start = 1);
 forstep(b = b_start, b_max, 2,
  ac = (D+b^2)/4;
  fordiv(ac, a,
    c = ac/a;
    if(c<a, break);
    if((c>a && b<=a) || c==a,
      print1("(", a, ", ", b, ", ", c, ")");
      forms = concat(forms, [[a, b, c]]);
      if(gcd([a,b,c])>1,
        prim = 0; print("*"); imprim_forms++,
        prim = 1; print(); class_no++);
      if(b>0 && b<a && a<c,
        print1("(", a, ", ", -b, ", ", c, ")");
        forms = concat(forms, [[a, -b, c]]);
        if(prim, print(); class_no++,
          print("*"); imprim_forms++)
      )
    )
   )
);
print("The class number h(d) for discriminant d = ",d," is ",
  class_no,".");
class_no_by_formula = h(d);
if(class_no_by_formula<>-1,
  print1("(Checking with special case of the class number ",
   "formula ");
   if(class_no_by_formula==class_no, print("agrees.)"),
    print("disagrees: ", class_no_by_formula, ".)"))
);
if(imprim_forms>0,
  if(imprim_forms==1, print("There is ",imprim_forms,
    " imprimitive form."),
    print("There are ", imprim_forms, " imprimitive forms."));
  print("This is not a fundamental discriminant."),
  print("This is a fundamental discriminant.");
  r = omega(d);
  if(r==1, print("This is also a prime discriminant."));
  g = 2^(r-1);
  if (g > 1,
    cpg = class_no / g;
    if(cpg==1, cstr = "class", cstr = "classes");
  print("There are ", g, " total genera with ", cpg, " ",
    cstr, " per genus."),
  print("There is one genus.")
);
if(verbose == 2,
  print("The following are the values of m (mod ", D,
    ") for which Chi_", d, "(m) = 1:");
  vm = [];
  for(m=1, D-1, if((gcd(m, D) == 1) && (kronecker(d, m) == 1),
    print1(m, "  "); vm = concat(vm, m)));
  print(" ");
);
if(r > 1,
  factors = factor_d(d);
  print("The discriminant is the product of the prime ",
    "discriminants ",
  factor_d(d), ".");
  if(verbose == 2,
    print1("m        ",);
    for(j = 1, r, print1("Chi_", factors[j], "(m)       "));
    print(" ");
    for(k = 1, matsize(vm)[2], print1(vm[k], "           ");
      for(j = 1, r,
        kk = kronecker(factors[j], vm[k]);
```

```
               if(kk == 1, print1(" "));
               print1(kk, "             ")); print(" "));
         );
         print(" ")
        )
     )
   )
 )
}


/* The function h below implements the special case of the class    */
/* number formula, returning the class                              */
/* number for the appropriate cases when d < 0 & returning the      */
/* value -1 when inapplicable. The Kronecker symbol is equivalent to*/
/* the Legendre symbol by definition for the case (r|p) where r is  */
/* an integer and p is an odd prime as below. (Further, r < p below */
/* so that p never divides r here.)                                 */
/* PARI does not currently have a Legendre symbol function.         */
/*                                                                  */
h(d) =
{local(p, r, s);
 p = -d;
 if(p>3 && isprime(p) && p%4 == 3,
   s = sum(r = 1, (p-1)/2, kronecker(r, p));
   if(p%8==7, return(s), return(s/3)),
   return(-1))
}

/* The function factor_d below factors the fundamental discriminant */
/* d into its unique product of prime discriminants.                  */
/* Currently it is assumed that d is already known to be a negative */
/* fund. disc. The return value is the resulting array p of prime   */
/* discriminants. A vector beginning with one or more zeros is        */
/* returned in any error situation where d cannot be thus factored. */

/* Recall that -4, -8, and 8 are prime discriminants.                */
/*                                                                    */
factor_d(d) =
{local(p, dpf, df, ptmp);
 if(d >= -1, return([0]));
 dpf = omega(d);
 p = vector(dpf);
 if((dpf == 1) && (bigomega(d) == 1) && ((-d)%4 == 3), p = [d],
   df = factor(-d);
   for(j = 1, dpf,
     if((j == 1) && (df[1, 1] == 2) && (df[1, 2] == 2), p[j] = -4);
     ptmp = df[j, 1];
     if(ptmp%4 == 1, p[j] = ptmp);
     if(ptmp%4 == 3, p[j] = -ptmp)
   );
   if((df[1, 1] == 2) && (df[1, 2] == 3), ptmp = 8;
     if(prod(k = 2, dpf, p[k]) > 0, p[1] = -ptmp, p[1] = ptmp))
 );
 if(prod(k = 1, dpf, p[k]) <> d, p[1] = 0);
 return(p)
}
```

A.3 Code to Compose Two Forms of the Same Discriminant

```
/* This code requires the discriminant to be fundamental.          */
/* For negative discriminants, the forms must both be positive     */
/* definite (a>0 and aa>0 so also c>0 and cc>0).                   */
/* Recursion is used to employ short-cuts; compose calls itself at  */
/* most twice.                                                     */
/* Setting zverbose = 3 before calling compose overrides specified */
/* verbose value when zagierreduce is called                       */

compose(a, b, c, aa, bb, cc, verbose) =
{d = b^2 - 4*a*c;
dd = bb^2 - 4*aa*cc;
if(zverbose<>3,zverbose=verbose);
/* zverbose=3 causes use of lexicographically first form in cycle  */
```

```
if(d==dd && isfundamental(d)==1 && ((dd<0 && a>0 && aa>0) || (dd>0)),
  if(verbose,
    if(dd<0,
      print("Positive definite with matching negative fundamental ",
       "discriminants"),
      print("Indefinite with matching positive fundamental ",
       "discriminants")));
  if(areconcordant(a, b, c, aa, bb, cc, verbose)==1,
    if(d<0,
      rf = reduce_neg(a*aa, b, (b^2-d)/(4*a*aa), verbose),
      rf = zagierreduce(a*aa, b, (b^2-d)/(4*a*aa), zverbose)
    );
    return(rf),
    if(gcd(a, aa)==1,
      n = bezout(a, aa)*(bb-b)/2;
      if(verbose, print(n));
      f1 = applytranstoform(1, n[1], 0, 1, a, b, c);
      if(verbose, print(f1));
      f2 = applytranstoform(1, -n[2], 0, 1, aa, bb, cc);
      if(verbose, print(f2));
      f3 = compose(f1[1], f1[2], f1[3], f2[1], f2[2], f2[3], verbose);
      if(verbose, print(f3));
      return(f3),
/* case where a and aa are not relatively prime but a and cc are */
```

```
      if(gcd(a, cc)==1,
        tmp = aa; aa = cc; cc = tmp; bb = -bb;
        if(verbose, print("Inverted the second form."));
        compose(a, b, c, aa, bb, cc, verbose),
/* case where gcd(a,aa)>1 and gcd(a,cc)>1 but gcd(c,aa)=1 */
        if(gcd(c, aa)==1 || (denominator(a/aa)==1 &&
         denominator(cc/c)==1 && b==-bb),
          tmp = a; a = c; c = tmp; b = -b;
          if(verbose, print("Inverted the first form."));
          compose(a, b, c, aa, bb, cc, verbose),
/* case where both must be inverted so new a, aa are rel. prime     */
          if(gcd(c, cc)==1,
            tmp = a; a = c; c = tmp; b = -b;
            tmp = aa; aa = cc; cc = tmp; bb = -bb;
            if(verbose, print("Inverted both the first and second ",
             "forms."));
            compose(a, b, c, aa, bb, cc, verbose),
/* case where second can be inverted to get concordant forms */
            if(denominator(aa/a)==1 && denominator(c/cc)==1 && b==-bb,
              tmp = aa; aa = cc; cc = tmp; bb = -bb;
              if(verbose, print("Inverted the second form; b’s were ",
               "opposites."));
              compose(a, b, c, aa, bb, cc, verbose),
/* case where inversions don’t find relatively prime a, aa */
```

```
              ff = factor(aa);
              r = 1; s = 1;
              for(kk = 1, matsize(ff)[1],
                if(a%ff[kk,1]==0 && c%ff[kk,1]<>0,
                  r = r*ff[kk,1]^ff[kk,2]);
                if(a%ff[kk,1]<>0, s = s*ff[kk,1]^ff[kk,2])
              );
              n = bezout(r,s);
              tmp = applytranstoform(r,-n[2],s,n[1],a,b,c);
              a = tmp[1]; b = tmp[2]; c = tmp[3];
              if(verbose,
                print("Transformed the first form to ",tmp));
              compose(a, b, c, aa, bb, cc, verbose)
            )
          )
        )
      )
    )
  ),
if(verbose,
  if(d==dd && dd<0 && isfundamental(d)==1,
    print("Forms are not both positive definite."),
    print("Discriminants do not match or are not fundamental.");
  )
```

```
);
return([0])
)
}


/* The following procedure assumes that both forms have the         */
/* same discriminant.                                               */
areconcordant(a, b, c, aa, bb, cc, verbose) =
{if(a*aa<>0 && denominator(c/aa)==1 && denominator(cc/a)==1 && b==bb,
   if(verbose, print("Forms are concordant."));
   return(1), return(0))
}


applytranstoform(r,s,t,u,a,b,c) =
{if(r*u-s*t==1,
   a1 = a*r^2 + b*r*t + c*t^2;
   b1 = 2*a*r*s + b*(r*u+s*t) + 2*c*t*u;
   c1 = a*s^2 + b*s*u + c*u^2;
   return([a1, b1, c1]),
   print("This is not a unimodular transformation.");
   return([0]))
}
```

A.4 Code to Generate a Class Group Table (Optionally by Outputting LaTeX Commands)

```
/* Use format=1 for LaTeX commands to create table.        */
/* Default format only outputs compositions, not operands. */
/* Note that with indefinite forms the representatives */
/* that display for a cycle may not always be the same */
/* and they are also not necessarily the same as in the */
/* row and column headings.  These may be manually replaced */
/* with a preferred representative of the cycle if desired. */
/* Call zagierreduce with the form and verbose = 2 to see */
/* the entire cycle. To force the lexicographically first */
/* member of a cycle to be displayed, leave zverbose = 3 below. */

create_group_table(v, format) =
{if(format==1, print_latex_first);
zverbose = 3;
for(l=1, matsize(v)[2],
  for(m=1, matsize(v)[2],
    fff = compose(v[l][1], v[l][2], v[l][3], v[m][1], v[m][2], v[m][3]);
    if(format==1,
      print_latex_line,
      if(m==matsize(v)[2], print1(fff), print1(fff, ", "))
    )
  );
  print();
);
if(format==1, print_latex_last)
}

print_latex_first()=
{print("\\begin{table}[h]");
d = v[1][2]^2 - 4*v[1][1]*v[1][3];
print("\\caption{Class Group Table for Discriminant $", d,
  "$ \\label{tab", if(d<0, "n", ""), abs(d),"}}");
print("\\centering");
print1("\\begin{tabular}{|");
for(n=1, matsize(v)[2] + 1, print1("c|"));
print("}");
print("\\hline");
print1("$*$");
for(k=1, matsize(v)[2], print1(" & $", v[k], "$"));
print("\\\\ \\hline")
}

print_latex_line()=
{
if(m==1, print1("$",v[l],"$"));
print1(" & ");
```

```
print1("$", fff, "$");
if(m==matsize(v)[2], print1("\\\\ \\hline"))
}


print_latex_last()=
{
print("\\end{tabular}");
print("\\end{table}");
kill(zverbose)
}
```

A.5 Code to Calculate the Order of an Element of a Class Group

```
findclassorder(v) =
{d=v[2]^2-4*v[1]*v[3];
if(isfundamental(d) && d<0,
if(d%2==0, pf = [1,0,-d/4], pf = [1,1,-(d-1)/4]);
print(pf);
order=1;
vv=v;
while(vv<>pf,
vv=compose(vv[1],vv[2],vv[3],v[1],v[2],v[3]);
order++;
);
return(order)
)
}
```

A.6 Code to Calculate Whether a Class Group is Cyclic

```
/* Below, w is a vector of vectors, one for each class for which    */
/* the class order is desired.                                       */
/* The returned vector, z, contains the respective orders.           */
/* The code assumes that w contains exactly all the vectors of a    */
/* class group.
/* There are simple ways to make this procedure more efficient in   */
/* handling large class groups if necessary.                         */
/*                                                                   */
findclassorders(w, verbose) =
{z = []; max_order = 0; gen = 0;
for(k=1, matsize(w)[2],
  tmp = findclassorder(w[k], verbose);
  max_order = max(max_order, tmp);
  z = concat(z, tmp);
  if(gen==0 && tmp==matsize(w)[2], gen = k)
);
if(max_order==matsize(w)[2],
  print("Class group is cyclic of order ", max_order, ".");
  print("The class ", w[gen], " is a generator."),
  print("Class group is *noncyclic* of order ", matsize(w)[2], "."));
return(z)
}
```

A.7 Code to Reduce a Form With a Positive Discriminant into its Cycle of Forms by Zagier’s Method

```
\\ zagierreduce(a,b,c,verbose)
\\
\\ This function reduces indefinite binary quadratic forms using
\\ Zagier’s method. The specified form (a,b,c) must have a positive
\\ fundamental discriminant. The product of the transformation
\\ matrices is displayed after reduction. If the optional fourth
\\ argument, verbose, is given as a nonzero value, then the cycle
\\ length is also calculated with each form in the cycle displayed.
\\
\\ 4th argument (verbose) supports different levels and modes
\\      (no output for verbose = 0; normal output for verbose = 1)
\\      (verbose = 2 causes cycle to be calculated and displayed also)
\\      (verbose = 3 has same display as verbose = 0 but returns
\\          the form in the cycle that is lexicographically first)
\\
{zagierreduce(a,b,c,verbose) = d=b^2-4*a*c;
if(d>0 && isfundamental(d)==1,
if(a>0 && c>0 && b>a+c,
  r = [a,b,c];
  if(verbose==1 || verbose==2,
    print("Form (", a, ",", b, ",", c, ") of discriminant ", d,
      " is already reduced!")
  ),
  if(verbose==1 || verbose==2,
    print("Reducing form (", a, ",", b, ",", c, ") of discriminant ",
     d, " ...")
  );
  cnt = 0;
  T = [1, 0; 0, 1];
  until(a>0 && c>0 && b>a+c,
    n = ceil((b+sqrt(d))/(2*c));
    T = T*[0, -1; 1, n];
    aa = c;
    bb = -b + 2*c*n;
    cc = a - b*n + c*n^2;
    cnt++;
    a = aa;
    b = bb;
    c = cc;
    if(verbose==1 || verbose==2,
      print();
```

```
        print1(cnt,": (", a, ",", b, ",", c, ") [n=", n, "]")
      )
    );
    r = [a,b,c];
    if(verbose==1 || verbose==2,
      print(" is the Zagier-reduced form.");
      printp(T, " is the product of the transformation matrices.")
    )
  );
    if(verbose==2 || verbose==3,
      sa = a; sb = b; sc = c;
      aa = 0; bb = 0; cc = 0;
      cnt = 0;
      if(verbose==2,print("Finding the cycle length ..."));
      vv = [];
      while(sa<>aa || sb<>bb || sc<>cc,
        n = ceil((b+sqrt(d))/(2*c));
        aa = c;
        bb = -b + 2*c*n;
        cc = a - b*n + c*n^2;
        cnt++;
        a = aa;
        b = bb;
        c = cc;
      if(verbose==2,
        print(cnt,": (", a, ",", b, ",", c, ") [n=", n, "]"),
        vv = concat(vv,[[a,b,c]]);
      )
    );
    if(verbose==2,print("The cycle length is ", cnt, "."),
    S=Set(vv); r=eval(S[1]); \\ Take first entry lexicographically
    )
  );
  return(r),
  if(verbose==1 || verbose==2,
    print("These are not the coefficients of a form with ",
      "positive fundamental discriminant.")
  );
  return([0])
)
}
```

APPENDIX B
CALCULATED SEQUENCES AND DATA

B.1 Integer Sequences

These existing entries in the On-Line Encyclopedia of Integer Sequences (OEIS) [Eis] are some of those most directly related to the topic of this thesis:

- A000926 Euler's "numerus idoneus" (idoneal, or suitable, or convenient numbers).
- A003171 Discriminants of orders of imaginary quadratic fields with 1 class per genus (a finite sequence).
- A003173 Heegner numbers: imaginary quadratic fields with unique factorization (or class number 1).
- A003636 Number of classes per genus in quadratic field with discriminant -n.
- A003640 Number of genera of quadratic field with discriminant -n.
- A003644 Discriminants of imaginary quadratic fields with 1 class per genus (a finite sequence).
- A003657 Discriminants of imaginary quadratic fields, negated.
- A003658 Fundamental discriminants of real quadratic fields; indices of primitive positive Dirichlet L-series.
- A006371 Number of reduced binary quadratic forms of discriminant -n.

- A006641 Class number of forms with discriminant -A003657(n), or equivalently class number of imaginary quadratic field with discriminant -A003657(n).
- A013658 Discriminants of imaginary quadratic fields with class number 4 (negated).
- A014600 Class numbers h(D) of imaginary quadratic fields with discriminant D=0,1 mod 4, D<0.
- A014601 Congruent to 0 or 3 mod 4.
- A014602 Discriminants of imaginary quadratic fields with class number 1 (negated).
- A014603 Discriminants of imaginary quadratic fields with class number 2 (negated).
- A0192322 Negated discriminants of imaginary quadratic number fields whose class group is isomorphic to the Klein 4-group, C2 x C2.

For immediate access to any sequence for which the "A-number" is known — such as A003173 above — simply use that A-number's corresponding link http://oeis.org/A003173.

These new entries in the OEIS are based on calculations using PARI code:

- A225365 Negative fundamental discriminants with nonisomorphic class groups (negated).
- A227734 Negative fundamental discriminants with noncyclic class groups (negated).
- A227735 Negative fundamental discriminants with cyclic class groups of composite order (negated).

B.2 Sample Output From the Above PARI Code

Below is sample output of the procedure prpdf. Note that it is necessary to begin the procedure with the command prpdf(2) to get the fullest output, including the list of $\chi_{d_i}(m)$ values, which can be lengthy for large discriminants.

```
prpdf(2)


Input a negative discriminant (Just press <Enter> to exit): -84


The reduced positive definite form(s) for discriminant d = -84:
(1, 0, 21)
(3, 0, 7)
(2, 2, 11)
(5, 4, 5)
The class number h(d) for discriminant d = -84 is 4.
This is a fundamental discriminant.
There are 4 total genera with 1 class per genus.
The following are the values of m (mod 84) for which Chi_-84(m) = 1:
1  5  11  17  19  23  25  31  37  41  55  71
The discriminant is the product of the prime discriminants [-4, -3, -7].
m        Chi_-4(m)       Chi_-3(m)       Chi_-7(m)
1            1              1              1
5            1             -1             -1
11           -1             -1              1
17            1             -1             -1
```

```
19           -1              1             -1
23           -1             -1              1
25            1              1              1
31           -1              1             -1
37            1              1              1
41            1             -1             -1
55           -1              1             -1
71           -1             -1              1


Input a negative discriminant (Just press <Enter> to exit):
Exiting program...
%9 = [[1, 0, 21], [3, 0, 7], [2, 2, 11], [5, 4, 5]]

prpdf(2)

Input a negative discriminant (Just press <Enter> to exit): -260

The reduced positive definite form(s) for discriminant d = -260:
(1, 0, 65)
(5, 0, 13)
(2, 2, 33)
(3, 2, 22)
(3, -2, 22)
```

```
(6, 2, 11)

(6, -2, 11)

(9, 8, 9)

The class number h(d) for discriminant d = -260 is 8.

This is a fundamental discriminant.

There are 4 total genera with 2 classes per genus.

The following are the values of m (mod 260) for which Chi_-260(m) = 1:

1  3  9  11  19  23  27  29  31  33  37  43  49  57  59  61  69  71  73

81  87  93  97  99  101  103  107  111  119  121  127  129  137  147

151  171  177  181  183  193  197  207  209  213  219  239  243  253

The discriminant is the product of the prime discriminants [-4, 5, 13].

m        Chi_-4(m)       Chi_5(m)       Chi_13(m)

1            1              1              1

3           -1             -1              1

9            1              1              1

11           -1              1             -1

19           -1              1             -1

23           -1             -1              1

27           -1             -1              1

29            1              1              1

31           -1              1             -1

33            1             -1             -1

37            1             -1             -1

43           -1             -1              1
```

49	1	1	1
57	1	-1	-1
59	-1	1	-1
61	1	1	1
69	1	1	1
71	-1	1	-1
73	1	-1	-1
81	1	1	1
87	-1	-1	1
93	1	-1	-1
97	1	-1	-1
99	-1	1	-1
101	1	1	1
103	-1	-1	1
107	-1	-1	1
111	-1	1	-1
119	-1	1	-1
121	1	1	1
127	-1	-1	1
129	1	1	1
137	1	-1	-1
147	-1	-1	1
151	-1	1	-1
171	-1	1	-1

```
177            1             -1             -1
181            1              1              1
183           -1             -1              1
193            1             -1             -1
197            1             -1             -1
207           -1             -1              1
209            1              1              1
213            1             -1             -1
219           -1              1             -1
239           -1              1             -1
243           -1             -1              1
253            1             -1             -1
```

```
Input a negative discriminant (Just press <Enter> to exit):
Exiting program...
%35 = [[1, 0, 65], [5, 0, 13], [2, 2, 33], [3, 2, 22], [3, -2, 22],
[6, 2, 11], [6, -2, 11], [9, 8, 9]]
```

Below is sample output of the procedure reduce_neg with verbose=1 specified. The command reduce_neg(41,100,61) only returns the result.

```
reduce_neg(41,100,61,1)
The discriminant is -4.
Reducing (41,100,61)...
```

```
Applying transformation 2:
(41,18,2)
Applying transformation 1:
(2,-18,41)
Applying transformation 2:
(2,2,1)
Applying transformation 1:
(1,-2,2)
Applying transformation 2:
(1,0,1)
Transformations used: 5
%2 = [1, 0, 1]
```

Below is sample output of the procedure zagierreduce with different levels specified for the verbosity. A command such as zagierreduce(1,10,10) only returns the result. Note that commands such as zagierreduce(11,26,14,3) below, with verbosity 3, return the lexicographically first representative of the cycle. The [n=k] output in brackets corresponds to the transformation $\mathbf{T}_k$ of Section 2.5.

```
zagierreduce(1,10,10,1)
Reducing form (1,10,10) of discriminant 60 ...


1: (10,10,1) [n=1]
2: (1,8,1) [n=9] is the Zagier-reduced form.


[-1 -9]
```

```
[1 8]
 is the product of the transformation matrices.
%2 = [1, 8, 1]

zagierreduce(1,10,10,2)
Reducing form (1,10,10) of discriminant 60 ...

1: (10,10,1) [n=1]
2: (1,8,1) [n=9] is the Zagier-reduced form.

[-1 -9]

[1 8]
 is the product of the transformation matrices.
Finding the cycle length ...
1: (1,8,1) [n=8]
The cycle length is 1.
%3 = [1, 8, 1]

zagierreduce(11,26,14,2)
Form (11,26,14) of discriminant 60 is already reduced!
Finding the cycle length ...
1: (14,30,15) [n=2]
```

```
2: (15,30,14) [n=2]
3: (14,26,11) [n=2]
4: (11,18,6) [n=2]
5: (6,18,11) [n=3]
6: (11,26,14) [n=2]
The cycle length is 6.
%4 = [11, 26, 14]
```

```
zagierreduce(11,26,14,3)
%5 = [11, 18, 6]
```

Below is sample output of the procedure compose, which returns the composition of two forms with the same discriminant consistent with the algorithm described in Section 3.1. Different levels specified for the optional verbosity control the amount of output. A command such as compose(a,b,c,d,e,f,3) guarantees that the result returned is the lexicographically first element in a cycle in the case of $d > 0$. This procedure calls reduce_neg or zagierreduce as necessary.

```
compose(3,12,7,11,18,6)
%1 = [2, 10, 5]
```

```
compose(3,12,7,11,18,6,1)
Indefinite with matching positive fundamental discriminants
[12, -3, 3]
[3, 84, 583]
```

```
[11, 84, 159]

Indefinite with matching positive fundamental discriminants

Forms are concordant.

Reducing form (33,84,53) of discriminant 60 ...


1: (53,22,2) [n=1]

2: (2,10,5) [n=8] is the Zagier-reduced form.


[-1 -8]


[1 7]

 is the product of the transformation matrices.

[2, 10, 5]

%2 = [2, 10, 5]


compose(3,12,7,11,18,6,2)

Indefinite with matching positive fundamental discriminants

[12, -3, 3]

[3, 84, 583]

[11, 84, 159]

Indefinite with matching positive fundamental discriminants

Forms are concordant.

Reducing form (33,84,53) of discriminant 60 ...
```

```
1: (53,22,2) [n=1]
2: (2,10,5) [n=8] is the Zagier-reduced form.

[-1 -8]

[1 7]
 is the product of the transformation matrices.
Finding the cycle length ...
1: (5,10,2) [n=2]
2: (2,10,5) [n=5]
The cycle length is 2.
[2, 10, 5]
%3 = [2, 10, 5]

compose(3,12,7,11,18,6,3)
Indefinite with matching positive fundamental discriminants
[12, -3, 3]
[3, 84, 583]
[11, 84, 159]
Indefinite with matching positive fundamental discriminants
Forms are concordant.
[2, 10, 5]
%4 = [2, 10, 5]
```