AMS / MAA DOLCIANI MATHEMATICAL EXPOSITIONS VOL 52

# QUADRATIC NUMBER THEORY

$\langle 2 \rangle \langle 3 \rangle$
$= ([2:1][2:1])([3:1][3:-1])$
$= ([2:1][3:1])([2:1][3:-1])$
$= \langle 1+\sqrt{-5} \rangle \langle 1-\sqrt{-5} \rangle$

## An Invitation to Algebraic Methods in the Higher Arithmetic

J. L. Lehman

MAA PRESS
An Imprint of the American Mathematical Society

**AMS/MAA** | DOLCIANI MATHEMATICAL EXPOSITIONS

VOL **52**

# Quadratic Number Theory

## An Invitation to Algebraic Methods in the Higher Arithmetic

**J. L. Lehman**


Providence, Rhode Island

2010 *Mathematics Subject Classification*. Primary 11R11, 11R29, 11R27, 11E25, 11E16, 11A55, 11B50, 11Y40.

For additional information and updates on this book, visit
**www.ams.org/bookpages/dol-52**

**Library of Congress Cataloging-in-Publication Data**

Names: Lehman, J. L. (James Larry), 1957– author.
Title: Quadratic number theory: An invitation to algebraic methods in the higher arithmetic / J.L. Lehman.
Description: Providence, Rhode Island: MAA Press, an imprint of the American Mathematical Society, [2019] | Series: Dolciani mathematical expositions; volume 52 | Includes an index.
Identifiers: LCCN 2018040720 | ISBN 9781470447373 (alk. paper)
Subjects: LCSH: Algebraic number theory. | Number theory. | Quadratic fields. | Algebraic fields. | AMS: Number theory – Algebraic number theory: global fields – Quadratic extensions. msc | Number theory – Algebraic number theory: global fields – Class numbers, class groups, discriminants. msc | Number theory – Algebraic number theory: global fields – Units and factorization. msc | Number theory – Forms and linear algebraic groups – Sums of squares and representations by other particular quadratic forms. msc | Number theory – Forms and linear algebraic groups – General binary quadratic forms. msc | Number theory – Elementary number theory – Continued fractions. msc | Number theory – Sequences and sets – Sequences (mod $m$). msc | Number theory – Computational number theory – Algebraic number theory computations. msc
Classification: LCC QA247 .L41955 2019 | DDC 512.7/4–dc23
LC record available at https://lccn.loc.gov/2018040720



10 9 8 7 6 5 4 3 2 1 24 23 22 21 20 19

# Contents

# Preface

This book is intended as an introduction to algebraic methods in number theory, suitable for mathematics students and others with a moderate background in elementary number theory and the terminology of abstract algebra. Although often first encountered at the graduate level, algebraic number theory can be a valuable field of study for undergraduate mathematics students, providing context for and connections between different areas of the mathematics curriculum and serving as a motivation for the historical development of abstract algebraic concepts. We have aimed this text toward undergraduate students and nonspecialists by restricting our attention to questions arising from squares of integers, thus referring to our topic as *quadratic number theory*. This grounding in easily stated problems motivates the key concepts of algebraic number theory but allows for "hands-on" computational techniques, often as applications of topics from elementary number theory. Many of these methods are approached in an original way in this text, which we describe further in this preface.

**Background.** Number theory (sometimes called the higher arithmetic) is defined broadly as the study of the properties of integers. Many arithmetic problems can be approached by "elementary" methods, that is, in terms of the set of integers itself. But in some cases, properties of integers might be most easily obtained and understood by working within larger sets of numbers. An example, which we will take as our starting point in Chapter 1, is the classical problem of determining which integers can be written as a sum of two squares. While we can answer this question by elementary means, as we will see in §1.1, the results can be more naturally explained by appealing to the set of *Gaussian integers*, $\mathbb{Z}[i] = \{q + ri \mid q, r \in \mathbb{Z}\}$, where $i^2 = -1$. An integer $n$ that is a sum of two squares is also a product of two Gaussian integers:

$$n = q^2 + r^2 = (q + ri)(q - ri).$$

Writing the sum as a product allows us to rephrase the problem in terms of factorization of $n$ in the Gaussian integers, where a classification of *irreducible* elements of $\mathbb{Z}[i]$ leads to a complete description of sums of two squares of integers.

Similar examples, such as representations of integers as $x^2+2y^2$ or $x^2+3y^2$, might be approached using numbers of the form $q+r\sqrt{-2}$ or $q+r\sqrt{-3}$. Introducing these numbers raises new questions, however. Which numbers of this type are most analogous to integers in their properties? Which elements in these sets can be regarded as "prime" factors, and how can we distinguish between different primes? Does uniqueness of prime factorization—a familiar property of the integers—hold in these more general sets of numbers? For instance, in $\mathbb{Z}[\sqrt{-7}] = \{q+r\sqrt{-7} \mid q, r \in \mathbb{Z}\}$, the equation

$$2 \cdot 2 \cdot 2 = 8 = (1+\sqrt{-7})(1-\sqrt{-7})$$

appears to present two different factorizations of a number into terms that cannot be broken down further. In this example, for reasons we will clarify later, it turns out that a better setting for this factorization is the set

$$D_{-7} = \left\{ q + rz \mid q, r \in \mathbb{Z} \text{ and } z = \frac{1+\sqrt{-7}}{2} \right\}.$$

If $\overline{z} = \frac{1-\sqrt{-7}}{2} = 1 - z$, we find that

$$2 \cdot 2 \cdot 2 = (z \cdot \overline{z})(z \cdot \overline{z})(z \cdot \overline{z}) = (z^2 \cdot \overline{z})(z \cdot \overline{z}^2) = (1+\sqrt{-7})(1-\sqrt{-7}),$$

so that the apparently different factorizations are merely different groupings of the same terms. As another example, the following might appear to present different factorizations of 7 in $\mathbb{Z}[\sqrt{2}] = \{q+r\sqrt{2} \mid q, r \in \mathbb{Z}\}$:

$$(3+\sqrt{2})(3-\sqrt{2}) = 7 = (5+4\sqrt{2})(-5+4\sqrt{2}).$$

This time, however, we find that

$$(5+4\sqrt{2})(-5+4\sqrt{2}) = (3+\sqrt{2})(1+\sqrt{2})(-1+\sqrt{2})(3-\sqrt{2}) = (3+\sqrt{2})(3-\sqrt{2}),$$

and we say that the factors are *unit* multiples of each other, or *associates*, so are not regarded as distinct factorizations (in the same way that $3 \cdot 5$ and $(-3)(-5)$ are not viewed as different ways of factoring 15 in the integers). But we will later show that other examples of distinct factorizations, such as

$$2 \cdot 3 = 6 = (1+\sqrt{-5})(1-\sqrt{-5})$$

in the set $\mathbb{Z}[\sqrt{-5}] = \{q+r\sqrt{-5} \mid q, r \in \mathbb{Z}\}$, cannot be resolved in either of these ways.

Ernst Kummer (1810–1893) made a major advance in attacking this problem of distinct irreducible factorization, reasoning that in such cases, the apparent lack of uniqueness could be remedied by considering a larger set of "ideal numbers," in which terms factor further, similarly to the case of $\mathbb{Z}[\sqrt{-7}]$ and $D_{-7}$ noted above. As an often-used analogy to Kummer's concept, suppose that some alien beings know all about even integers, but have no concept of odd integers.

The set $E$ of even integers has many properties in common with our set $\mathbb{Z}$ (aside from an identity element for multiplication). In particular, we can generalize the concept of divisibility in $E$, where we could say that $a$ divides $b$ if there is an element $q$ in $E$ such that $b = aq$. For instance, we would say that 6 divides 12 because $12 = 6 \cdot 2$ with 2 in $E$, but that 6 does not divide 30 because there is no *even* integer that we can multiply by 6 to obtain 30. We might then define an element $p$ in $E$ to be *prime* if $p$ cannot be written as a product of two elements in $E$. The prime elements of $E$ are precisely the numbers that are (in our usual terminology) congruent to 2 modulo 4, that is, 2, 6, 10, 14, and so forth. We find that every element of $E$ can be written as a product of primes. But this factorization is not always unique, as illustrated for example by 60, which can be written either as $2 \cdot 30$ or as $6 \cdot 10$. Of course, knowing about odd integers, we recognize these two factorizations as different combinations of the "true" prime factorization of 60:

$$2 \cdot 30 = 2 \cdot (2 \cdot 3 \cdot 5) = (2 \cdot 3) \cdot (2 \cdot 5) = 6 \cdot 10.$$

However, the aliens familiar only with even integers might regard these odd integers as ideal numbers, introduced simply to obtain unique factorization.

Kummer did not define ideal numbers precisely, but rather described only their divisibility properties. Richard Dedekind (1831–1916) recognized that ideal numbers could be defined as certain types of subsets, which he called "ideals," of a set such as $\mathbb{Z}[\sqrt{-5}]$, and so be studied in a concrete way. In addition to clarifying Kummer's work, Dedekind's definition of ideals found applications to other algebraic problems and was a major factor in the development of modern abstract algebra in the nineteenth and twentieth centuries.

There is no doubt, however, that Dedekind regarded ideals as being "numbers," in some sense, as had Kummer. In his 1877 treatise *Theory of Algebraic Integers*, Dedekind compared the definition of ideals to his earlier development of irrational numbers as certain types of subsets of the rational numbers, now known as *Dedekind cuts*, which placed the set of real numbers on firm logical ground. Thus the concept of a number being defined as a set was not unnatural for him.

One goal of this book is to recapture this "numerical" interpretation of ideals. We can do so, as we describe in the next subsection, in the special case of domains of *quadratic integers* defined in terms of roots of degree two polynomials with integer coefficients. (The work of Kummer and Dedekind was in a broader setting of *algebraic integers*, using roots of polynomials of arbitrary degree having integer coefficients.) Thus we may regard quadratic number theory, and this text in particular, as a stepping stone toward the concepts and methods of algebraic number theory.

**Innovative Aspects of the Text.** This book is divided into five parts, each consisting of two or three chapters. Each part has a separate introduction, and

each chapter ends with a review of concepts and results, so a detailed outline of the text is unnecessary here. Instead, we briefly describe several innovations, particularly in methods of representing ideals and quadratic forms, which distinguish this work from previous treatments of algebraic number theory. We omit all specific details of definitions and calculations at this point, but refer to chapters in the text where these are found.

**Ideal Number Notation.** Our main innovation is a notation for ideals of a quadratic domain that facilitates computations with those objects. To motivate these expressions as a natural development, we first associate an "ideal form" with every Gaussian integer (Chapter 1), and then with all examples of quadratic integers (Chapter 2), and we demonstrate that calculations of divisibility and factorization can be simplified using these ideal forms. In an arbitrary quadratic domain, however, it appears that "ideal number" expressions are necessary to fill in some gaps and produce uniqueness of irreducible factorization. We make this precise with the traditional definition of ideals (Chapter 3), but maintain the ideal number notation for these sets. We demonstrate methods of writing an arbitrary ideal as an ideal number in practice. Using these representations, we classify prime ideals, we describe factorization of ideals into prime ideals, and we derive formulas for multiplication of ideals. Each of these calculations requires only basic techniques of solving linear or quadratic congruences, as in elementary number theory.

**Ideal Notation for Quadratic Forms.** We use the question of which integers can be represented by a given quadratic form as a motivation for many concepts of algebraic number theory. Here also we initiate a revised method of representing these objects, showing (Chapter 4) that every quadratic form of a given discriminant can be expressed with essentially the same notation that we use for ideals in a corresponding quadratic domain. We show that these expressions are useful in classifying quadratic forms, recognizing equivalences among forms, and describing representations of integers by a particular quadratic form. Furthermore, we demonstrate (Chapter 5) that we can apply the similarity of notation between ideals and quadratic forms in various ways. In particular, we show that the operation of composition on quadratic forms mirrors the multiplication of ideals when both are carried out in ideal number notation. Using ideal notation, we establish a method of listing all classes of ideals, or quadratic forms, of negative discriminant and determining the algebraic structure of the resulting class groups (Chapter 6), which we then apply to representations of integers by positive definite forms (Chapter 7). Ideal notation also gives us a systematic method of using class groups of quadratic forms of primitive discriminant to compute class groups of square multiples of that discriminant (Chapter 8).

**Quadratic Continued Fraction Algorithm.** We extend the calculation of class groups to positive discriminants, and the topic of continued fractions of real numbers (Chapter 9) proves to be our main tool in this construction. Here our main innovation is a new algorithm (revised from standard methods) for computing the continued fraction of an arbitrary real quadratic number. We will see that this algorithm also produces a sequence of equivalent quadratic forms in ideal notation (Chapter 10). Thus we can systematically determine class groups of positive discriminant, which we then apply to representations of integers by indefinite quadratic forms (Chapter 11).

**Suborder Functions.** As a final topic, we consider patterns in sequences of integers defined by a second-order recurrence relation, particularly when those sequences are reduced modulo prime numbers, noting connections to powers of quadratic integers. An innovative technique that we introduce to describe these patterns is the *suborder function* on a field with $p$ elements, which we define in terms of a quadratic extension field (Chapter 12). We will see applications of these functions to properties of indefinite quadratic forms (Chapter 13), particularly in describing solutions of $x^2 - dy^2 = 1$ when $d$ is a positive integer with square divisors and in computing class groups of quadratic forms under the same circumstances.

**Prerequisites.** A preliminary version of this text was used in an undergraduate topics course in algebraic number theory at the University of Mary Washington, with a prerequisite of a course in number theory *or* a first-semester course in abstract algebra covering group theory. Students without a background in number theory soon picked up on required concepts after a brief introduction to techniques of solving linear and quadratic congruences. In this book, we similarly allow for a quick immersion into the main topics of quadratic number theory. We begin with a concise summary, without proofs, of necessary topics from elementary number theory in §§0.1–0.3. We introduce terminology and results from abstract algebra as needed, and the introduction to each part includes a description of required terminology and results for those chapters. These include definitions of divisibility (such as units, associates, irreducible and prime elements) in integral domains in Part One; group terminology (subgroups, cosets, conjugates) in connection with groups of matrices in Part Two; the structure of finite abelian groups in Part Three; some assumptions about convergence of sequences in Part Four; and basic properties of finite fields in Part Five.

**Appendices.** While the book's organization allows a quick introduction to the concepts of algebraic number theory, we have also attempted to make this text as self-contained as possible. Details of all arithmetic and algebraic prerequisites

are available in appendices—in the interest of space, these appear online[1] only. The following is a description of the material provided in these appendices.

**Appendix A: Number Systems.** Here we define and develop the basic sets of numbers in which we work throughout the text. We begin by establishing that a set $\mathbb{N}$ with all the properties of the natural numbers can be constructed from the null set using power sets and unions of sets. We define an order relation, and operations of addition and multiplication on $\mathbb{N}$, and prove the standard algebraic properties of these operations by inductive arguments. We then define the entire set of integers, $\mathbb{Z}$, using an equivalence relation on ordered pairs of natural numbers, and the set of rational numbers, $\mathbb{Q}$, with an equivalence relation on pairs of integers. The set of real numbers, $\mathbb{R}$, is constructed as a collection of subsets of rational numbers (*Dedekind cuts*, as mentioned previously in this preface), with the key concept of completeness established as a consequence of this definition. Finally, we define the complex numbers as a set of ordered pairs of real numbers. The results of Appendix A, if not the development itself, are familiar and are assumed in all parts of the main text.

**Appendix B: Elementary Number Theory.** In this appendix, we summarize the main concepts typically encountered in a first course in number theory—divisibility and prime factorization, congruence relations, and linear and quadratic congruences. Many of the results in Appendix B are used extensively in the main text and are summarized in §§0.1–0.3, as noted above. A formula for the number of solutions of an arbitrary quadratic congruence, stated without proof as Theorem 0.3.4, is proved in §B.4 using the concept of *seeding polynomials*. Proofs of the Quadratic Reciprocity Theorem and Legendre's Theorem on the existence of nontrivial solutions of $ax^2 + by^2 + cz^2 = 0$ appear in §B.5 and §B.6.

**Appendix C: Algebraic Systems.** This appendix includes a development of the algebraic terminology used at various points in this book. We define the main concepts of groups and prove the Fundamental Theorem of Finite Abelian Groups, required in describing the structure of class groups of ideals and of quadratic forms. We define rings, integral domains, and fields, and develop general properties of ideals, including operations on ideals, in an arbitrary integral domain. We also introduce general definitions of divisibility in an integral domain, with criteria to establish whether a given integral domain has unique irreducible factorization. We summarize the main facts on the existence and structure of finite fields, required in the chapters on quadratic recursive sequences.

**Note to the Reader.** As stated several times in this preface, this book places particular emphasis on a numerical interpretation of concepts from abstract algebra that arise from arithmetic questions, often using an innovative notational

[1] These appendices will be maintained at `www.ams.org/bookpages/dol-52`.

approach. For that reason, examples of numerical computations are an integral part of this text. Most examples that you will encounter are accessible via hand calculation or could lend themselves to short computer programs for further exploration. Perhaps the most important prerequisite for this text is a willingness to engage with these numerical techniques, to work through examples presented in the text and in exercises, and to explore how those examples can be generalized. My hope is that readers of all levels will be inspired to further discovery in quadratic number theory, or to research in other areas of algebraic number theory.

## Acknowledgments

The notational approaches that motivate this text developed gradually over the course of several directed studies that I led, and were tested and refined in a topics class I taught at the University of Mary Washington. I am grateful to my department for offering this course, to the university for supporting the writing of this text via a sabbatical leave, and particularly to the students who expressed interest in this topic and who convinced me (indirectly) that a book on algebraic number theory geared toward undergraduates was a feasible idea.

From MAA Press, I am very appreciative of the prompt attention that acquisitions editor Stephen Kennedy gave to my manuscript and the continued support that he has shown throughout the review process. I am particularly thankful to Steve for recommending that this book be considered for publication in the Dolciani Mathematical Expositions series.

Above all, I am grateful to Harriet Pollatsek and the anonymous reviewers of the Dolciani Board for their numerous suggestions for improvements to various versions of this text. The Dolciani standard of "mathematical elegance and ingenuity" has been a daunting challenge to aspire to at times. To the extent that this book meets that standard, I owe a great debt to Harriet and the board for their combination of critiques and encouragement.

J. L. Lehman

Fredericksburg, Virginia
August 2018

# Introduction: A Brief Review of Elementary Number Theory

Throughout this text, we will find that calculations with algebraic objects are obtained as applications of linear and quadratic congruences. In this introduction, we review methods of solving these congruences, and we compile other arithmetic preliminaries for later reference. We omit all proofs in the introduction—these and more details appear in Appendix B.

## 0.1 Linear Equations and Congruences

If $m$ and $n$ are integers, we say that *$m$ divides $n$* if there is an integer $q$ so that $n = mq$. We can test whether one integer divides another by the following theorem.

**Theorem 0.1.1** (Division Algorithm)**.** *If $n$ and $m$ are integers with $m > 0$, then there are unique integers $q$ and $r$ such that $n = mq + r$ and $0 \leq r < m$.*

In practice, we can find the *quotient* $q$ and *remainder* $r$ on division of $n$ by $m$ using the long division process, although some caution is required when $n$ is negative, as illustrated in the following example. We also write $r$ as $n \bmod m$. When $m$ is positive, then $m$ divides $n$ if and only if $n \bmod m = 0$. Note that $m$ divides $n$ if and only if $-m$ divides $n$, and that 0 divides $n$ if and only if $n = 0$.

**Example.** Let $n = -573$ and $m = 37$. By long division, we find that $573 = 37 \cdot 15 + 18$. So then $-573 = -(37 \cdot 15 + 18) = 37(-15) + (-18)$. Now to ensure that $r$ satisfies $0 \leq r < 37$, we adjust this equation as follows:

$$-573 = 37(-16 + 1) + (-18) = 37(-16) + (37 - 18) = 37(-16) + 19.$$

Thus $q = -16$ and $r = 19$ are the *unique* quotient and remainder on division of $-573$ by 37. In particular, $-573 \bmod 37 = 19$. ◊

**Exercise 0.1.1.** For the following values of $n$ and $m$, find the unique way of writing $n = mq + r$ with $0 \leq r < m$.

(a) $n = 679$ and $m = 23$.

(b) $n = -782$ and $m = 57$.

(c) $n = -3216$ and $m = 67$.

When $a$ and $b$ are integers, there is a unique integer $d \geq 0$ such that:

(1) $d$ divides $a$ and $d$ divides $b$, and

(2) if $c$ divides $a$ and $c$ divides $b$, then $c$ divides $d$.

We call $d$ the *greatest common divisor* of $a$ and $b$, and write $d = \gcd(a, b)$. We say that $a$ and $b$ are *relatively prime* if $\gcd(a, b) = 1$. The following fact leads to many important results about divisibility in the set of integers.

**Theorem 0.1.2.** *Let $a$ and $b$ be integers with $d = \gcd(a, b)$, and let $n$ be an integer. Then the equation $ax + by = n$ has an integer solution $(x, y)$ if and only if $d$ divides $n$.*

An expression of the form $ax + by$ is also called a *combination* of $a$ and $b$. Theorem 0.1.2 implies that when $a$ and $b$ are not both zero, then $d = \gcd(a, b)$ is the smallest positive combination of $a$ and $b$. The following are some important consequences of this fact.

**Corollary 0.1.3.** *Let $a$, $b$, and $c$ be integers. If $a$ divides $bc$ and $\gcd(a, b) = d$, then $a$ divides $cd$. In particular, if $a$ divides $bc$ and $a$ and $b$ are relatively prime, then $a$ divides $c$.*

**Definition.** An integer $n > 1$ is called *prime* if its only positive divisors are 1 and $n$, and is called *composite* otherwise.

**Corollary 0.1.4** (Euclid's Lemma)**.** *If $p$ is a prime number and $p$ divides a product $ab$ of integers, then $p$ divides $a$ or $p$ divides $b$ (or both).*

**Exercise 0.1.2.** Use Corollary 0.1.3 to show that Euclid's Lemma is true. If $n$ is composite, show that it is always possible to find integers $a$ and $b$ so that $n$ divides $ab$ but $n$ does not divide $a$ and $n$ does not divide $b$.

**Exercise 0.1.3.** Let $a$, $b$, and $n$ be integers, and suppose that $a$ divides $n$ and $b$ divides $n$. Show that if $\gcd(a, b) = d$, then $ab$ divides $nd$. (Hint: Use the second assumption to write $n = bq$ for some integer $q$. Then note that $a$ divides $bq$, and use Corollary 0.1.3.)

**Exercise 0.1.4.** If $a$ and $b$ are not both zero and $\gcd(a,b) = d$, use Exercise 0.1.3 to show that the positive integer $m = |ab|/d$ has the following properties: $m$ is a common multiple of $a$ and $b$ (that is, $a$ divides $m$ and $b$ divides $m$), and if $n$ is any common multiple of $a$ and $b$, then $m$ divides $n$. (We call $m$ the *least common multiple* of $a$ and $b$, and write $m = \operatorname{lcm}(a,b)$.)

The *Euclidean algorithm* is an efficient method for calculating the greatest common divisor $d$ of a pair of integers $a$ and $b$, and for constructing a solution of $ax + by = d$, from which we can solve $ax + by = n$ when $d$ divides $n$. It is based on repeated application of the division algorithm, as we illustrate with an example.

**Example.** Let $a = 567$ and $b = 98$. In the left-hand list of equations, we divide $a$ by $b$, then divide $b$ by the remainder of the first division, and so forth until we obtain the remainder zero.

$$\begin{aligned} 567 &= 98 \cdot 5 + 77 \\ 98 &= 77 \cdot 1 + 21 \\ 77 &= 21 \cdot 3 + 14 \\ 21 &= 14 \cdot 1 + 7 \\ 14 &= 7 \cdot 2 + 0 \end{aligned} \qquad \begin{aligned} 77 &= a - 5b \\ 21 &= -a + 6b \\ 14 &= 4a - 23b \\ 7 &= -5a + 29b \end{aligned}$$

It is a fact that $\gcd(a,b) = \gcd(b,r)$ when $a = bq + r$. Thus we find that

$$\gcd(567, 98) = \gcd(98, 77) = \gcd(77, 21) = \cdots,$$

eventually obtaining $\gcd(567, 98) = \gcd(7, 0) = 7$, the last nonzero remainder in the left-hand column of equations. Now in the right-hand list, we rewrite each equation on the left in terms of its remainder. By substitution, we find that each remainder has the form $ax+by$ for some $x$ and $y$. For instance, since $77 = a-5b$, then $21 = 98 - 77 = b - (a - 5b) = -a + 6b$. Thus $14 = 77 - 3(21) = (a - 5b) - 3(-a + 6b) = 4a - 23b$, and so forth. We find in particular that the last nonzero remainder, $\gcd(a,b)$, equals $as + bt$ for some integers $s$ and $t$. ◊

**Exercise 0.1.5.** Apply the Euclidean algorithm to each pair $a$ and $b$ to calculate $d = \gcd(a,b)$ and to find integers $s$ and $t$ so that $d = as + bt$.

(a) $a = 504$ and $b = 186$.

(b) $a = 1247$ and $b = 913$.

(c) $a = 1350$ and $b = 1401$.

If $d = \gcd(a,b)$, then the Euclidean algorithm produces a solution of $ax + by = d$. Using this expression, we can construct all integer solutions of an arbitrary linear equation by the following formula.

**Theorem 0.1.5.** *Let $a$ and $b$ be integers (not both zero), and let $s$ and $t$ be a pair of integers for which $\gcd(a,b) = d = as + bt$. Let $n$ be a multiple of $d$, say with $n = dr$ for some integer $r$. Then all integer solutions of $ax + by = n$ are given by*

$$(x, y) = \left(sr + \frac{b}{d} \cdot q\,,\; tr - \frac{a}{d} \cdot q\right), \tag{0.1.1}$$

*where $q$ is an arbitrary integer.*

**Exercise 0.1.6.** Find all solutions of the following linear equations, or explain why no such solutions exist. (Use the calculations in the preceding example and in Exercise 0.1.5.)

(a) $567x + 98y = 201$.

(b) $504x + 186y = 202$.

(c) $504x + 186y = 204$.

(d) $1247x + 913y = 25$.

(e) $1350x + 1401y = 3000$.

**Linear Congruences.** When $a$ and $b$ are integers, and $m$ is a positive integer, we say that $a$ is *congruent* to $b$ modulo $m$, and write $a \equiv b \pmod{m}$, if $m$ divides $a - b$. Congruence modulo $m$ is an equivalence relation on the set of integers, and each integer is congruent to its remainder on division by $m$, so that the set $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$ is a collection of equivalence class representatives under this relation. If $a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$, then

$$a + b \equiv c + d \pmod{m} \qquad \text{and} \qquad ab \equiv cd \pmod{m}. \tag{0.1.2}$$

For cancellation in a congruence, we have the following general statement.

**Proposition 0.1.6** (Congruence Cancellation Property)**.** *Let $a$, $b$, $c$, and $m$ be integers, and let $\gcd(a,m) = d$. Then $ab \equiv ac \pmod{m}$ if and only if $b \equiv c \pmod{m/d}$.*

**Exercise 0.1.7.** Let $a$ and $m$ be integers with $\gcd(a,m) = 1$ and $m$ positive. Show that there is a positive integer $t$ so that $a^t \equiv 1 \pmod{m}$. (Hint: Explain why there must be integers $0 \le r < s$ so that $a^s \equiv a^r \pmod{m}$. If $\gcd(a,m) = 1$, use Proposition 0.1.6 to show that $a^{s-r} \equiv 1 \pmod{m}$.)

**Definition.** If $m$ is a positive integer and $\gcd(a,m) = 1$, then we refer to the smallest positive integer $t$ for which $a^t \equiv 1 \pmod{m}$ as the *order* of $a$ modulo $m$, and write $\mathrm{ord}_m(a) = t$.

**Exercise 0.1.8.** Let $m$ be a positive integer, let $a$ be an integer with $\gcd(a,m) = 1$, and let $t$ be the order of $a$ modulo $m$.

(a) Show that $a^n \equiv 1 \pmod{m}$ if and only if $t$ divides $n$.

(b) Show that $a^s \equiv a^r \pmod{m}$ if and only if $s \equiv r \pmod{t}$.

A *linear congruence* has the general form $ax \equiv b \pmod{m}$, where $a$ and $b$ are integers and $m$ is a positive integer. Solving a linear congruence means finding all integers $x$ that make the congruence a true statement. It suffices to find all solutions in the set $\mathbb{Z}_m$, and we refer to the *number of solutions* of a linear congruence as the number of solutions in $\mathbb{Z}_m$. Here we have the following main result.

**Theorem 0.1.7.** *Let $ax \equiv b \pmod{m}$ be a linear congruence with $d = \gcd(a, m)$, and suppose that $d = as + mt$ for some integers $s$ and $t$. If $b = dq$ for some integer $q$, then $ax \equiv b \pmod{m}$ has $d$ solutions in $\mathbb{Z}_m$, each congruent to $qs$ modulo $m/d$. If $d$ does not divide $b$, then $ax \equiv b \pmod{m}$ has no solutions.*

**Example.** Consider the congruence $69x \equiv 111 \pmod{123}$. Applying the Euclidean algorithm to $a = 69$ and $m = 123$, we find that $\gcd(a, m) = 3 = a(-16) + m(9)$. Here $b = 111 = 3 \cdot 37$ and so solutions exist, each congruent to $-16 \cdot 37 = -592$ modulo $m/d = 41$. There are three distinct solutions in $\mathbb{Z}_{123}$: $x = 23$, $x = 64$, and $x = 105$. ◊

**Exercise 0.1.9.** Find all solutions (in the appropriate set $\mathbb{Z}_m$) of the given linear congruence, or explain why no solutions exist.

(a) $23x \equiv 18 \pmod{39}$.

(b) $186x \equiv 246 \pmod{504}$.

(c) $221x \equiv 19 \pmod{247}$.

(d) $221x \equiv 117 \pmod{247}$.

**Systems of Linear Congruences.** A general problem we often encounter is to find all values of $x$ that simultaneously satisfy two or more linear congruences. Below is a description of these solutions in a special case of most interest.

**Theorem 0.1.8** (Chinese Remainder Theorem)**.** *Let $m$ and $n$ be positive integers with $\gcd(m, n) = 1$, and let $s$ and $t$ be integers so that $ms + nt = 1$. If $a$ and $b$ are integers, then there is a unique $x$ modulo $mn$ that satisfies the pair of congruences*

$$x \equiv a \pmod{m} \qquad \text{and} \qquad x \equiv b \pmod{n}.$$

*This value of $x$ is congruent to $ant + bms$ modulo $mn$.*

**Example.** To solve $x \equiv 5 \pmod{17}$ and $x \equiv 7 \pmod{47}$ simultaneously, we can begin with the Euclidean algorithm applied to $m = 17$ and $n = 47$.

$$\begin{array}{rcl@{\qquad}rcl} 47 &=& 17 \cdot 2 + 13 & 13 &=& -2m + n \\ 17 &=& 13 \cdot 1 + 4 & 4 &=& 3m - n \\ 13 &=& 4 \cdot 3 + 1 & 1 &=& -11m + 4n \end{array}$$

(We omit the final equation since 1 must be the last nonzero remainder.) We can verify that $1 = -11 \cdot 17 + 4 \cdot 47 = -187 + 188$. Here $188 \cdot 5 - 187 \cdot 7 = -369$ satisfies the pair of congruences, and an integer $x$ satisfies this system if and only if $x \equiv -369 \pmod{799}$, where $799 = 17 \cdot 47$. Selecting the unique representative in $\mathbb{Z}_{799}$, we might say that $x \equiv 430 \pmod{799}$ is *the* solution of $x \equiv 5 \pmod{17}$ and $x \equiv 7 \pmod{47}$. ◊

**Exercise 0.1.10.** Find all solutions of the given pair of linear congruences.

(a) $x \equiv 7 \pmod{13}$ and $x \equiv 29 \pmod{41}$.

(b) $x \equiv 17 \pmod{63}$ and $x \equiv 14 \pmod{82}$.

(c) $x \equiv 374 \pmod{1247}$ and $x \equiv 821 \pmod{913}$.

We will use the claim of the following exercise on several occasions.

**Exercise 0.1.11.** Let $m$ be a positive integer and let $a$, $b$, $c$, and $d$ be integers with $\gcd(a, b) = 1$. Show that there is an integer $x$ simultaneously satisfying $ax \equiv c \pmod{m}$ and $bx \equiv d \pmod{m}$ if and only if $m$ divides $ad - bc$. Show that the solution is unique modulo $m$. (Hint: If $as + bt = 1$ and $ad - bc = mu$ for some integers $s$, $t$, and $u$, show that $x = cs + dt$ satisfies both congruences. If $y$ also satisfies both congruences, show that $a(x-y) = mq$ and $b(x-y) = mr$ for some integers $q$ and $r$, and then that $x - y = m(qs + rt)$.)

## 0.2 Quadratic Congruences Modulo Primes

A *quadratic congruence* has the general form $f(x) \equiv 0 \pmod{m}$, where $f(x) = ax^2+bx+c$ and $m$ is a positive integer. We will describe a formula for the *number* of solutions of an arbitrary quadratic congruence in terms of the *discriminant* of $f(x)$, that is, $\Delta = b^2 - 4ac$. (As with linear congruences, the number of solutions of $f(x) \equiv 0 \pmod{m}$ means the number of different congruence classes of solutions.) Here it is convenient to begin in this section with the case in which $m = p$ is a prime number. We will assume that $p$ does not divide the coefficient of $x^2$ in $f(x)$, since otherwise $f(x) \equiv 0 \pmod{p}$ reduces to a linear congruence. The following proposition describes solutions of a quadratic congruence when $p = 2$.

**Proposition 0.2.1.** *Let $f(x) = ax^2 + bx + c$ with $a$ odd, and let $\Delta = b^2 - 4ac$.*

(1) *If $b$ is odd and $c$ is even, then $\Delta \equiv 1 \pmod 8$, and $f(x) \equiv 0 \pmod 2$ has two solutions, $x = 0$ and $x = 1$, in $\mathbb{Z}_2$.*

(2) *If $b$ and $c$ are odd, then $\Delta \equiv 5 \pmod 8$, and $f(x) \equiv 0 \pmod 2$ has no solutions in $\mathbb{Z}_2$.*

(3) *If $b$ is even, then $\Delta \equiv 0 \pmod 4$, and $f(x) \equiv 0 \pmod 2$ has one solution in $\mathbb{Z}_2$, namely $x = 0$ if $c$ is even, and $x = 1$ if $c$ is odd.*

If $p$ is an odd prime and $p$ does not divide $a$, then $ax^2 + bx + c \equiv 0 \pmod p$ has the same solutions as $(2ax + b)^2 \equiv \Delta \pmod p$, where $\Delta = b^2 - 4ac$. If we can find all $y$ such that $y^2 \equiv \Delta \pmod p$, then the solutions of the original congruence are obtained by solving $2ax + b \equiv y \pmod p$. Each such linear congruence has a unique solution since $\gcd(2a, p) = 1$.

Changing our notation, we can concentrate on quadratic congruences of the form $x^2 \equiv a \pmod p$, where $p$ is an odd prime and $a$ is an arbitrary integer. The *Legendre symbol* $\left(\frac{a}{p}\right)$ is defined as follows in terms of the number of solutions (in $\mathbb{Z}_p$) of this congruence:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } x^2 \equiv a \pmod p \text{ has two solutions,} \\ 0, & \text{if } x^2 \equiv a \pmod p \text{ has only one solution,} \\ -1, & \text{if } x^2 \equiv a \pmod p \text{ has no solutions.} \end{cases}$$

The following exercise shows that one of these three cases must occur, and that $\left(\frac{a}{p}\right) = 0$ if and only if $p$ divides $a$.

**Exercise 0.2.1.** Suppose that $b^2 \equiv a \pmod p$, where $p$ is an odd prime.

(a) Show that $-b \equiv p - b \pmod p$ also satisfies $x^2 \equiv a \pmod p$.

(b) Show that $-b \equiv b \pmod p$ if and only if $b \equiv 0 \pmod p$.

(c) Show that $x^2 \equiv a \pmod p$ has no more than two solutions. (Hint: If $b$ and $c$ are solutions, show that $p$ divides $c^2 - b^2 = (c - b)(c + b)$. Use Euclid's Lemma to explain why $c \equiv b \pmod p$ or $c \equiv -b \pmod p$.)

**Exercise 0.2.2.** Show that $\left(\frac{1}{p}\right) = 1$ for every odd prime $p$.

**Exercise 0.2.3.** Show that if $a \equiv b \pmod p$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

The following theorems and exercises allow us to calculate an arbitrary Legendre symbol through a systematic reduction process, as we will demonstrate.

**Theorem 0.2.2** (Euler's Criterion)**.** *If $p$ is an odd prime and $a$ is an integer, then*

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

**Exercise 0.2.4.** Use Euler's Criterion to show that if $p$ is an odd prime, then

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

**Exercise 0.2.5.** Use Euler's Criterion to show that if $p$ is an odd prime and $a$ and $b$ are integers, then

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

By Exercise 0.2.5, it suffices to calculate symbols of the form $\left(\frac{q}{p}\right)$, where $q$ is prime. Our final two claims allow us to do so in every case.

**Theorem 0.2.3.** *If $p$ is an odd prime, then*

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 8 \quad \text{or} \quad p \equiv 7 \pmod 8, \\ -1, & \text{if } p \equiv 3 \pmod 8 \quad \text{or} \quad p \equiv 5 \pmod 8. \end{cases}$$

**Theorem 0.2.4** (Quadratic Reciprocity Theorem)**.** *If $p$ and $q$ are distinct odd primes, then*

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right), & \text{if } p \equiv 1 \pmod 4 \quad \text{or} \quad q \equiv 1 \pmod 4, \\ -\left(\frac{p}{q}\right), & \text{if } p \equiv 3 \pmod 4 \quad \text{and} \quad q \equiv 3 \pmod 4. \end{cases}$$

**Example.** The number of solutions of $x^2 \equiv 70 \pmod{79}$ is determined by the Legendre symbol $\left(\frac{70}{79}\right)$. We have that

$$\left(\frac{70}{79}\right) = \left(\frac{2}{79}\right)\left(\frac{5}{79}\right)\left(\frac{7}{79}\right) = 1 \cdot \left(\frac{79}{5}\right) \cdot -\left(\frac{79}{7}\right),$$

using Theorem 0.2.3 with the observation that $79 \equiv 7 \pmod 8$, and Theorem 0.2.4 with $5 \equiv 1 \pmod 4$, $7 \equiv 3 \pmod 4$, and $79 \equiv 3 \pmod 4$. But now we can simplify these symbols, since $79 \equiv 4 \pmod 5$ and $79 \equiv 2 \pmod 7$, as in Exercise 0.2.3:

$$\left(\frac{70}{79}\right) = -\left(\frac{79}{5}\right) \cdot \left(\frac{79}{7}\right) = -\left(\frac{4}{5}\right)\left(\frac{2}{7}\right) = -\left(\frac{2}{5}\right)^2\left(\frac{2}{7}\right) = -(-1)^2 \cdot 1 = -1,$$

again using Theorem 0.2.3. By definition, this means that $x^2 \equiv 70 \pmod{79}$ has no solutions. (We could also have applied Exercise 0.2.3 at the start to write

$\left(\frac{70}{79}\right) = \left(\frac{-9}{79}\right) = \left(\frac{-1}{79}\right)\left(\frac{3}{79}\right)^2 = -1$, using Exercise 0.2.4. Here note that $\left(\frac{3}{79}\right)^2$ equals $1^2$ or $(-1)^2$ in any case, so must be 1.) ◊

**Exercise 0.2.6.** Calculate the following Legendre symbols.

(a) $\left(\frac{-19}{43}\right)$.

(b) $\left(\frac{35}{67}\right)$.

(c) $\left(\frac{46}{97}\right)$.

**Exercise 0.2.7.** Show that if $p$ and $q$ are odd primes and $q \equiv 3 \pmod 4$, then $\left(\frac{-q}{p}\right) = \left(\frac{p}{q}\right)$.

**Example.** Consider $x^2 + 11x + 7 \equiv 0 \pmod{719}$, where $p = 719$ is prime. This congruence has the same solutions as $(2x + 11)^2 \equiv 93 \pmod{719}$, here calculating $\Delta = 11^2 - 4 \cdot 1 \cdot 7 = 93$ as the discriminant of the quadratic polynomial. Now

$$\left(\frac{93}{719}\right) = \left(\frac{3}{719}\right)\left(\frac{31}{719}\right) = -\left(\frac{719}{3}\right) \cdot -\left(\frac{719}{31}\right),$$

since 3, 31, and 719 are all congruent to 3 modulo 4. With $719 \equiv 2 \pmod 3$ and $719 \equiv 6 \pmod{31}$, we then find that

$$\left(\frac{93}{719}\right) = \left(\frac{719}{3}\right)\left(\frac{719}{31}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{31}\right)\left(\frac{3}{31}\right) = -1 \cdot 1 \cdot -\left(\frac{31}{3}\right) = \left(\frac{1}{3}\right) = 1.$$

Our conclusion is that $y^2 \equiv 93 \pmod{719}$ has two solutions, and thus our original congruence also has two solutions. But the Legendre symbol tells us nothing about what these solutions are, only that they must exist. Extensive trial-and-error calculations verify that $314^2 \equiv 93 \pmod{719}$. So our original congruence has two solutions, obtained by solving $2x + 11 \equiv 314 \pmod{719}$ and $2x + 11 \equiv -314 \pmod{719}$ for $x = 511$ and $x = 197$, respectively. ◊

**Exercise 0.2.8.** Solve the following quadratic congruences, or explain why no solutions exist.

(a) $x^2 + x - 3 \equiv 0 \pmod{17}$.

(b) $3x^2 + 5x + 8 \equiv 0 \pmod{19}$.

(c) $5x^2 - x + 1 \equiv 0 \pmod{23}$.

In this book, we will assume that all quadratic congruences modulo prime numbers that we encounter can be solved by trial-and-error, as in the preceding example, with the Legendre symbol determining whether solutions exist. Systematic approaches, which can be far more efficient for large prime moduli, do exist, and are introduced in Appendix B.

## 0.3 Quadratic Congruences Modulo Composite Integers

In this section, we demonstrate that we can solve $f(x) \equiv 0 \pmod{m}$, where $f(x)$ is a quadratic polynomial and $m$ is a positive integer, if we know solutions of $f(x) \equiv 0 \pmod{p}$ for every prime $p$ that divides $m$. Our first result, which holds for polynomials of arbitrary degree, shows that we can use solutions of $f(x) \equiv 0 \pmod{p}$ to solve the same congruence modulo $p^2$, and then modulo $p^3$, and so forth up to an arbitrary positive integer power of $p$.

**Theorem 0.3.1.** *Let $f(x)$ be a polynomial with integer coefficients, let $f'(x)$ be its derivative, let $p$ be a prime number, and let $e$ be a positive integer. Then an integer $s$ is a solution of the congruence $f(x) \equiv 0 \pmod{p^{e+1}}$ if and only if $s = r + p^e t$, where $r$ satisfies $f(x) \equiv 0 \pmod{p^e}$ and $t$ satisfies the linear congruence*

$$f'(r) \cdot t \equiv -\frac{f(r)}{p^e} \pmod{p}. \tag{0.3.1}$$

**Example.** Let $f(x) = x^2 + 11x + 7$ and let $p = 17$. The congruence $f(x) \equiv 0 \pmod{17}$ has the same solutions as $(2x + 11)^2 \equiv 93 \pmod{17}$. With $\left(\frac{93}{17}\right) = \left(\frac{8}{17}\right) = \left(\frac{2}{17}\right)^3 = 1^3 = 1$, two solutions of $y^2 \equiv 93 \pmod{17}$ exist, specifically $y \equiv \pm 5 \pmod{17}$ since $93 \equiv 5^2 \pmod{17}$. Solving

$$2x + 11 \equiv 5 \pmod{17} \quad \text{and} \quad 2x + 11 \equiv -5 \pmod{17},$$

we find that $x \equiv -3 \equiv 14 \pmod{17}$ and $x \equiv -8 \equiv 9 \pmod{17}$ are the solutions of $f(x) \equiv 0 \pmod{17}$.

Any solution of $f(x) \equiv 0 \pmod{17^2}$ also satisfies $f(x) \equiv 0 \pmod{17}$, so must have the form $s = r + 17t$, where $r = 9$ or $r = 14$, and $t$ is an integer. (We can assume that $t$ is an element of $\mathbb{Z}_{17}$, since we are looking for values of $s$ in $\mathbb{Z}_{289}$.) The following table helps us keep track of the necessary calculations in applying the theorem with $e = 1$. Note that $f'(x) = 2x + 11$.

| $r$ | $f(r)$ | $-f(r)/17$ | $f'(r)$ | $t$ | $s$ |
|---|---|---|---|---|---|
| 9 | 187 | −11 | 29 | 9 | 162 |
| 14 | 357 | −21 | 39 | 6 | 116 |

For instance, when $r = 9$, we solve $29t \equiv -11 \pmod{17}$, which simplifies to $12t \equiv 6 \pmod{17}$ with solution $t = 9$, so that $s = r + 17t = 9 + 17(9) = 162$.

When $r = 14$, we solve $39t \equiv -21 \pmod{17}$, that is, $5t \equiv 13 \pmod{17}$ with solution $t = 6$, so that $s = r + 17t = 14 + 17(6) = 116$.

Now if we want to solve $f(x) \equiv 0 \pmod{17^3}$, we can apply the theorem again with $e = 2$. Any solution of $f(x) \equiv 0 \pmod{17^3}$ has the form $s = r + 17^2 t$ with $r = 162$ or $r = 116$.

| $r$ | $f(r)$ | $-f(r)/289$ | $f'(r)$ | $t$ | $s$ |
|---|---|---|---|---|---|
| 162 | 28033 | $-97$ | 335 | 16 | 4786 |
| 116 | 14739 | $-51$ | 243 | 0 | 116 |

When $r = 162$, we solve $335t \equiv -97 \pmod{17}$, which simplifies to $12t \equiv 5 \pmod{17}$ with solution $t = 16$. When $r = 116$, we solve $243t \equiv -51 \pmod{17}$, which simplifies to $5t \equiv 0 \pmod{17}$ with solution $t = 0$. Here $f(x) \equiv 0 \pmod{17^3}$ has two solutions: $x = 4786$ and $x = 116$. ◊

Congruence (0.3.1) is a linear congruence modulo $p$. According to Theorem 0.1.7, this congruence has a unique solution if $p$ does not divide $f'(r)$, and has either $p$ solutions or no solutions when $p$ divides $f'(r)$. For a quadratic polynomial $f(x)$, the latter case occurs if and only if $p$ divides $\Delta$, the discriminant of $f(x)$. The next example illustrates this possibility.

**Example.** Let $f(x) = x^2 + 11x + 7$ and let $p = 3$. Here $f(x) \equiv 0 \pmod{3}$ has the same solutions as $(2x + 11)^2 \equiv 93 \pmod{3}$, that is, just one solution since 3 divides 93. Solving $2x + 11 \equiv 0 \pmod{3}$, we find that $x = 2$ is this solution. Now any solution of $f(x) \equiv 0 \pmod{9}$ has the form $s = 2 + 3t$, where $t$ satisfies $f'(2) \cdot t \equiv -\frac{f(2)}{3} \pmod{3}$. With $f'(2) = 15$ and $f(2) = 33$, this congruence becomes $15t \equiv -11 \pmod{3}$, which has no solutions since $\gcd(15, 3) = 3$ does not divide $-11$. Thus $f(x) \equiv 0 \pmod{3^2}$ has no solutions, and neither can $f(x) \equiv 0 \pmod{3^e}$ for any $e \geq 2$. ◊

**Exercise 0.3.1.** Find all solutions of $x^2 + x - 1 \equiv 0 \pmod{m}$ for each of the following values of $m$.

(a) $m = 5$, $m = 25 = 5^2$, and $m = 125 = 5^3$.

(b) $m = 11$, $m = 121 = 11^2$, and $m = 1331 = 11^3$.

(c) $m = 19$, $m = 361 = 19^2$, and $m = 6859 = 19^3$.

Theorem 0.3.1 shows that we can use solutions of $f(x) \equiv 0 \pmod{p}$ to solve $f(x) \equiv 0 \pmod{p^e}$ for every $e > 1$. Our next result implies that we can then solve $f(x) \equiv 0 \pmod{m}$ for an arbitrary positive integer $m$ as an application of the Chinese Remainder Theorem.

**Theorem 0.3.2.** *Let $f(x)$ be a polynomial with integer coefficients. Let $m$ and $n$ be relatively prime positive integers. Then $t$ satisfies $f(x) \equiv 0 \pmod{mn}$ if and only if $t \equiv r \pmod{m}$ and $t \equiv s \pmod{n}$ for some solution $r$ of $f(x) \equiv 0 \pmod{m}$ and some solution $s$ of $f(x) \equiv 0 \pmod{n}$.*

**Example.** Consider the congruence $x^2 + 11x + 7 \equiv 0 \pmod{17^2 \cdot 719}$. Previous examples have shown that $x^2 + 11x + 7 \equiv 0 \pmod{17^2}$ has two solutions, $x = 116$ and $x = 162$, while $x^2 + 11x + 7 \equiv 0 \pmod{719}$ has solutions $x = 197$ and $x = 511$. Theorem 0.3.2 implies that all solutions of $x^2 + 11x + 7 \equiv 0 \pmod{17^2 \cdot 719}$ are obtained by solving the pair of congruences $x \equiv r \pmod{289}$ and $x \equiv s \pmod{719}$ for all combinations of $r = 116$ or 162 and $s = 197$ or 511. We can follow the method of Theorem 0.1.8, starting with the Euclidean algorithm applied to $m = 289$ and $n = 719$.

$$\begin{array}{rclcrcl} 719 &=& 289 \cdot 2 + 141 & & 141 &=& -2m + n \\ 289 &=& 141 \cdot 2 + 7 & & 7 &=& 5m - 2n \\ 141 &=& 7 \cdot 20 + 1 & & 1 &=& -102m + 41n \end{array}$$

We find that $1 = (289)(-102) + (719)(41) = -29478 + 29479$. By Theorem 0.1.8, $x \equiv 29479r - 29478s \pmod{17^2 \cdot 719}$ is the general solution of $x \equiv r \pmod{289}$ and $x \equiv s \pmod{719}$. The following table compiles these possibilities modulo $17^2 \cdot 719 = 207791$.

| $r$ | $s$ | $t = 29479r - 29478s$ | $t \bmod 207791$ |
|---|---|---|---|
| 116 | 197 | −2387602 | 105890 |
| 116 | 511 | −11643694 | 200393 |
| 162 | 197 | −1031568 | 7387 |
| 162 | 511 | −10287660 | 101890 |

Thus $x^2 + 11x + 7 \equiv 0 \pmod{17^2 \cdot 719}$ has four distinct solutions: 7387, 101890, 105890, and 200393. ♢

**Exercise 0.3.2.** Find all solutions of $x^2 + x - 1 \equiv 0 \pmod{m}$ for each of the following values of $m$. (Use results from Exercise 0.3.1 where possible.)

(a) $m = 55 = 5 \cdot 11$.

(b) $m = 209 = 11 \cdot 19$.

(c) $m = 605 = 5 \cdot 11^2$.

(d) $m = 2299 = 11^2 \cdot 19$.

**The Number of Solutions of a Quadratic Congruence.** When $f(x)$ is a quadratic polynomial and $m$ is a positive integer, we denote the number of solutions (in $\mathbb{Z}_m$) of the congruence $f(x) \equiv 0 \pmod{m}$ as $n_m(f)$. Our next two results show that we can calculate this value in terms of the discriminant of $f(x)$, given the prime factorization of $m$.

**Corollary 0.3.3.** *Let $f(x)$ be a quadratic polynomial with integer coefficients. If $m$ is a positive integer, let $n_m(f)$ be the number of solutions of $f(x) \equiv 0 \pmod{m}$ in $\mathbb{Z}_m$. Then*

$$n_m(f) = \prod_p n_{p^e}(f), \tag{0.3.2}$$

*where the product is taken over all primes $p$, and where $e = e_p(m)$ is the exponent of $p$ in $m$, that is, the largest integer so that $p^e$ divides $m$.*

If $m$ is a positive integer, then $e_p(m) = 0$ for all but finitely many primes. Since the congruence $f(x) \equiv 0 \pmod{1}$ always has one solution, the product in (0.3.2) is actually finite. Notice that if $n_{p^e}(f) = 0$ for any prime power $p^e$ dividing $m$, then $n_m(f) = 0$.

Our final theorem for these review sections provides a formula for $n_{p^e}(f)$ when $f(x)$ is a quadratic polynomial and $p$ is a prime number. To avoid writing the case of $p = 2$ separately it is convenient to extend the definition of the Legendre symbol as follows. (More precisely, we are defining a special case of the *Kronecker symbol*.)

**Definition.** If $\Delta$ is an integer congruent to 0 or 1 modulo 4, then

$$\left(\frac{\Delta}{2}\right) = \begin{cases} 1, & \text{if } \Delta \equiv 1 \pmod{8}, \\ -1, & \text{if } \Delta \equiv 5 \pmod{8}, \\ 0, & \text{if } \Delta \equiv 0 \pmod{4}. \end{cases}$$

**Theorem 0.3.4.** *Let $f(x) = ax^2 + bx + c$, with discriminant $\Delta = b^2 - 4ac$, and let $p$ be a prime number not dividing $a$. If $\Delta \neq 0$, let $\ell \geq 0$ be the largest integer for which $\Delta = p^{2\ell}\Delta_0$ with $\Delta_0 \equiv 0$ or $1 \pmod{4}$. Let $e$ be a nonnegative integer. If $e > 2\ell$, then the following statements are true.*

(1) *If* $\left(\frac{\Delta_0}{p}\right) = 1$, *then* $n_{p^e}(f) = 2p^\ell$.

(2) *If* $\left(\frac{\Delta_0}{p}\right) = -1$, *then* $n_{p^e}(f) = 0$.

(3) *If* $\left(\frac{\Delta_0}{p}\right) = 0$, *then* $n_{p^e}(f) = \begin{cases} p^\ell, & \text{if } e = 2\ell + 1, \\ 0, & \text{if } e > 2\ell + 1. \end{cases}$

*On the other hand, if $e \leq 2\ell$ is written as $e = 2k + r$ with $r = 0$ or $r = 1$, then $n_{p^e}(f) = p^k$. This equation also holds for all $e \geq 0$ if $\Delta = 0$.*

**Exercise 0.3.3.** Let $f(x) = x^2 + 18x + 1$. Use Theorem 0.3.4 to find the number of solutions of $f(x) \equiv 0 \pmod{2^e}$ for every integer $e \geq 0$. Verify that your results are correct by direct calculation with Theorem 0.3.1.

Theorem 0.3.4 and Corollary 0.3.3 allow us to find the number of solutions of an arbitrary quadratic congruence, as we illustrate with the following example to conclude this review of quadratic congruences.

**Example.** Let $f(x) = x^2 + 2x + 4$, with discriminant $\Delta = -12$. We derive a formula for $n_m(f)$, the number of solutions of $f(x) \equiv 0 \pmod{m}$, in terms of the prime factorization of $m$.

(1) For $p = 2$, we have that $\Delta = 2^2 \cdot -3$ with $-3 \equiv 1 \pmod 4$, so that $\ell = 1$ in the notation of Theorem 0.3.4. Since $-3 \equiv 5 \pmod 8$, then $n_{2^e}(f) = 0$ if $e > 2\ell = 2$. On the other hand, $n_{2^e}(f) = 1$, 1, or 2 for $e = 0$, 1, or 2, respectively.

(2) For $p = 3$, then $\ell = 0$ and $\Delta_0 = -12$. Since 3 divides $\Delta_0$, we have that $n_{3^e}(f) = 1$ if $e = 0$ or 1, but $n_{3^e}(f) = 0$ for $e > 1$.

(3) If $p > 3$ is a prime number, then $\left(\frac{-12}{p}\right) = \left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$ by Exercise 0.2.7. Theorem 0.3.4 implies that $f(x) \equiv 0 \pmod{p^e}$ has two solutions if $p \equiv 1 \pmod 3$ and no solutions if $p \equiv 2 \pmod 3$.

To combine these results via Corollary 0.3.3, let $m = 2^e \cdot 3^{e_0} \cdot p_1^{e_1} \cdots p_t^{e_t}$ with each $p_i$ a distinct prime greater than 3, with $e$ and $e_0$ nonnegative integers, and with $e_i$ a positive integer for $1 \le i \le t$. (We allow the possibility that $t = 0$.) If $e \ge 3$, $e_0 \ge 2$, or $p_i \equiv 2 \pmod 3$ for any $i$, then $n_m(f) = 0$. On the other hand,

$$n_m(f) = \begin{cases} 2^t, & \text{if } e < 2, \\ 2^{t+1}, & \text{if } e = 2, \end{cases}$$

when $e \le 2$, $e_0 \le 1$, and each $p_i \equiv 1 \pmod 3$. ◊

**Exercise 0.3.4.** If $f(x) = x^2 + x - 1$, find a formula in terms of the prime factorization of $m$ for the number of solutions of $f(x) \equiv 0 \pmod m$.

**Exercise 0.3.5.** Let $q = q_1 \cdot q_2 \cdots q_k$ be an odd positive integer, with each $q_i$ prime (not necessarily distinct). If $a$ is an integer, define the *Jacobi symbol* $\left(\frac{a}{q}\right)$ to be $\left(\frac{a}{q}\right) = \left(\frac{a}{q_1}\right) \cdot \left(\frac{a}{q_2}\right) \cdots \left(\frac{a}{q_k}\right)$. If $f(x)$ is a quadratic polynomial with discriminant $\Delta$, and $f(x) \equiv 0 \pmod q$ has a solution, show that $\left(\frac{\Delta}{q}\right) = 1$. Show that the converse of this statement is not always true.

# Part One: Quadratic Domains and Ideals

**Overview.** The three chapters of Part One cover many of the concepts described in the historical background of the Preface. Our overall goal is to motivate the definition of ideals in domains of quadratic integers, and to develop practical methods for calculations with those ideals.

We begin with the question of which integers can be represented as sums of two squares, which raises issues of divisibility in the domain of Gaussian integers. We establish the uniqueness of irreducible factorization in this domain and then demonstrate how it allows us to characterize the integers that can be expressed as a sum of two squares. In Chapter 2, we seek to apply this approach more broadly to representations of integers by an arbitrary quadratic form. This prompts a definition of quadratic numbers and quadratic integers, and the classification of domains of quadratic integers. Concepts of divisibility in the Gaussian integers carry over to this broader setting, but we will demonstrate that there are many examples of quadratic domains that lack *uniqueness* of irreducible factorization. As described in the Preface, this inspires the definition of ideals in Chapter 3. We will see that these ideals restore a form of unique irreducible factorization in many examples of quadratic domains, specifically in what we will define as *complete* quadratic domains.

In Part One, we also introduce an important innovation, "ideal number notation" for ideals of quadratic domains. To build naturally to this definition, we begin by assigning an "ideal form" to each Gaussian integer in Chapter 1. (We will see that this notation is somewhat analogous to polar coordinates as an alternative to rectangular coordinates for a point in the plane.) We demonstrate that ideal forms allow us to test divisibility of one Gaussian integer by another, and characterize irreducible elements and the irreducible factorization of an arbitrary Gaussian integer. We establish a necessary criterion for when an expression is an ideal form for a Gaussian integer, and show that this criterion is also sufficient by developing an algorithm to convert each eligible expression into the standard form for a Gaussian integer.

In Chapter 2, we generalize this notation to ideal forms of elements in an arbitrary quadratic domain, with similar applications to divisibility. We again note a necessary condition, in terms of a particular quadratic congruence, for an expression to be an ideal form for an element of a quadratic domain. However, we find that this criterion is generally not sufficient—in particular, it fails when the domain lacks uniqueness of irreducible factorization. In these cases, we informally define *ideal numbers* purely in terms of the ideal form notation, and we demonstrate that these additional factors appear to resolve examples of distinct irreducible factorizations in these quadratic domains.

The introduction of ideals in Chapter 3 makes this rather vague definition precise. We will see that ideal number notation allows us to classify all ideals of an arbitrary quadratic domain in terms of the solutions of a quadratic congruence modulo arbitrary integers. Using this notation, we find that we can describe ideal containment, precisely characterize prime ideals of a quadratic domain, and calculate, in a practical and systematic way, products and prime ideal factorizations of ideals in numerical form.

**Requirements for Part One.** The specifics of ideal number notation depend on properties of linear congruences, criteria for the existence of solutions of quadratic congruences, and methods of solving quadratic congruences, particularly with composite moduli. The preceding three sections should provide sufficient background for the required calculations, but more details appear in Appendix B when needed. We also use the terminology of divisibility in an arbitrary integral domain, such as units and associates, the distinction between irreducible and prime elements, and the definitions of Euclidean domains and unique factorization domains. We define these terms in the context of quadratic domains where required. More general background can be found in Appendix C.

# 1

# Gaussian Integers and Sums of Two Squares

(1) Which integers can be written as a sum of two (relatively prime) squares?

(2) In how many different ways can an integer be expressed as a sum of two squares?

These questions, dating back at least to Albert Girard (1595–1632) and Pierre de Fermat (1607–1665) in the seventeenth century, motivate some of the main concepts that we will encounter throughout this book. In §1.1, we will see that we can answer the first question using "elementary" methods, that is, in terms of the set of integers itself. We find in §1.2, however, that we can obtain these results more directly by working within a larger set of numbers, the *Gaussian integers*, in which we can generalize the concept of prime factorization of integers. We introduce an alternative notation for Gaussian integers in §1.3, and we demonstrate in §1.4 and §1.5 that these expressions help us describe irreducible factorization and multiplication of Gaussian integers in practice. In §1.6, we will use this approach to fully answer our second question, about the number of expressions for an arbitrary integer as a sum of two squares.

## 1.1 Sums of Two Squares

We say that $a$ is a sum of two squares if $a = q^2 + r^2$ for some integers $q$ and $r$. We also use the following terminology, which we will generalize in Chapter 4.

Table 1.1. Sums of Two Squares

| $x\backslash y$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | | | | | | | | | | | | |
| 1 | 1 | 2 | | | | | | | | | | | |
| 2 | 4 | 5 | 8 | | | | | | | | | | |
| 3 | 9 | 10 | 13 | 18 | | | | | | | | | |
| 4 | 16 | 17 | 20 | 25 | 32 | | | | | | | | |
| 5 | 25 | 26 | 29 | 34 | 41 | 50 | | | | | | | |
| 6 | 36 | 37 | 40 | 45 | 52 | 61 | 72 | | | | | | |
| 7 | 49 | 50 | 53 | 58 | 65 | 74 | 85 | 98 | | | | | |
| 8 | 64 | 65 | 68 | 73 | 80 | 89 | 100 | 113 | 128 | | | | |
| 9 | 81 | 82 | 85 | 90 | 97 | 106 | 117 | 130 | 145 | 162 | | | |
| 10 | 100 | 101 | 104 | 109 | 116 | 125 | 136 | 149 | 164 | 181 | 200 | | |
| 11 | 121 | 122 | 125 | 130 | 137 | 146 | 157 | 170 | 185 | 202 | 221 | 242 | |
| 12 | 144 | 145 | 148 | 153 | 160 | 169 | 180 | 193 | 208 | 225 | 244 | 265 | 288 |

**Definition.** Let $f(x, y) = x^2 + y^2$. We say that $f$ *represents* an integer $a$ if $f(q, r) = a$ for some integers $q$ and $r$, and that $f$ *properly represents* $a$ if $f(q, r) = a$ with $\gcd(q, r) = 1$. By the *number of representations* of $a$ as $x^2 + y^2$, we will mean the number of equations $q^2 + r^2 = a$ with $q \geq r \geq 0$.

We list in Table 1.1 all values of $f(x, y) = x^2+y^2$ for integers $0 \leq y \leq x \leq 12$. If $f(x, y) = a$, then $f(\pm x, \pm y) = a = f(\pm y, \pm x)$, so such a table would eventually include every integer that can be expressed as a sum of two squares if it could be extended indefinitely. There are only certain rows in this table in which an integer might appear. Since $0 \leq y^2 \leq x^2$, then $x^2 \leq x^2 + y^2 \leq 2x^2$. Thus if $f(x, y) = a$, it follows that $\sqrt{a/2} \leq x \leq \sqrt{a}$. For instance, if $a = 141$, then

$$8 < \sqrt{141/2} \leq x \leq \sqrt{141} < 12.$$

We do not see 141 in the rows with $9 \leq x \leq 11$, hence we can be sure that 141 is not a sum of two squares. For $a = 145$, we must have $9 \leq x \leq 12$, and we find two expressions for 145 as a sum of two squares: $9^2 + 8^2 = 145 = 12^2 + 1^2$.

**Exercise 1.1.1.** Find all ways of writing each of the following integers as a sum of two squares.

(a) $a = 313$.

(b) $a = 377$.

(c) $a = 433$.

If $f(x, y) = a$, then every square multiple of $a$ is likewise a sum of two squares, $f(gx, gy) = g^2 a$. Thus we can restrict our attention to proper representations of $a$ as a sum of two squares. If $a$ is *squarefree*, that is, not divisible

by a square other than 1, then every representation of $a$ must be proper. On the other hand, $45 = 6^2 + 3^2 = 3^2(2^2 + 1^2)$ has only an improper representation, while $50 = 7^2 + 1^2 = 5^2 + 5^2$ has both a proper and improper representation. In this section, we establish criteria for which integers can be expressed, properly or otherwise, as a sum of two squares. The following proves to be a key observation in obtaining these results.

**Proposition 1.1.1.** *If $m$ and $n$ are sums of two squares, then their product is also a sum of two squares.*

*Proof.* The following equations are verified by direct expansion:

$$(q^2 + r^2)(s^2 + t^2) = (qs + rt)^2 + (qt - rs)^2 = (qs - rt)^2 + (qt + rs)^2. \quad (1.1.1)$$

So if $m = q^2 + r^2$ and $n = s^2 + t^2$, then $mn$ can be written in two possibly different ways as a sum of two squares. □

**Example.** Since $13 = 3^2 + 2^2$ and $29 = 5^2 + 2^2$, we find that

$$13 \cdot 29 = (3 \cdot 5 + 2 \cdot 2)^2 + (3 \cdot 2 - 2 \cdot 5)^2 = (3 \cdot 5 - 2 \cdot 2)^2 + (3 \cdot 2 + 2 \cdot 5)^2.$$

Rearranging terms and changing signs, we obtain two equations $q^2 + r^2 = 377$ with $q \geq r \geq 0$: $377 = 19^2 + 4^2 = 16^2 + 11^2$. ◊

**Example.** With $13 = 3^2 + 2^2$ and $26 = 5^2 + 1^2$, we have that

$$13 \cdot 26 = (3 \cdot 5 + 2 \cdot 1)^2 + (3 \cdot 1 - 2 \cdot 5)^2 = (3 \cdot 5 - 2 \cdot 1)^2 + (3 \cdot 1 + 2 \cdot 5)^2.$$

That is, $338 = 17^2 + 7^2 = 13^2 + 13^2$. ◊

**Example.** For $10 = 3^2 + 1^2$ and $26 = 5^2 + 1^2$, we see that

$$10 \cdot 26 = (3 \cdot 5 + 1 \cdot 1)^2 + (3 \cdot 1 - 1 \cdot 5)^2 = (3 \cdot 5 - 1 \cdot 1)^2 + (3 \cdot 1 + 1 \cdot 5)^2.$$

Thus $260 = 16^2 + 2^2 = 14^2 + 8^2$. ◊

These examples illustrate that both, just one, or neither of the two expressions in equation (1.1.1) might be proper representations of $mn$. We will address this later in this section.

**Exercise 1.1.2.** Use Proposition 1.1.1 to find two different ways of writing each of the following integers $a$ as $a = q^2 + r^2$ with $q \geq r \geq 0$.

(a) $a = 481 = 13 \cdot 37$.

(b) $a = 493 = 17 \cdot 29$.

(c) $a = 697 = 17 \cdot 41$.

(d) $a = 949 = 13 \cdot 73$.

(e) $a = 1537 = 29 \cdot 53$.

(f) $a = 8633 = 89 \cdot 97$.

The following proposition provides a necessary condition for $a$ to be properly represented as a sum of two squares.

**Proposition 1.1.2.** *If $a = q^2 + r^2$ with $\gcd(q, r) = 1$, then there are integers $m$ and $k$ for which $am = k^2 + 1$. Thus if $a$ is properly represented by $x^2 + y^2$, then the congruence $x^2 + 1 \equiv 0 \pmod{a}$ has a solution.*

*Proof.* Since $\gcd(q, r) = 1$, there are integers $s$ and $t$ so that $qs + rt = 1$. Let $m = t^2 + s^2$ and $k = qt - rs$. Then

$$am = (q^2 + r^2)(t^2 + s^2) = (qt - rs)^2 + (qs + rt)^2 = k^2 + 1,$$

using equation (1.1.1), and so $k$ is a solution of $x^2 + 1 \equiv 0 \pmod{a}$. □

**Representations of Primes as Sums of Two Squares.** We show in the remainder of this section that the criterion of Proposition 1.1.2 is also sufficient for $a$ to be properly represented by $x^2 + y^2$. We begin with representations of prime numbers, approached indirectly with the following lemma.

**Lemma 1.1.3.** *Let $p$ be a prime number. Suppose that $ap$ is represented by $x^2 + y^2$ for some integer $a$ with $1 < a < p$. Then there is an integer $b$ with $1 \le b < a$ so that $bp$ is also represented by $x^2 + y^2$.*

*Proof.* Let $ap = q^2 + r^2$ for some integers $q$ and $r$. We can select integers $m$ and $n$ so that $m \equiv q \pmod{a}$ and $n \equiv r \pmod{a}$, with $m$ and $n$ as small as possible in absolute value. Notice as follows that $m$ and $n$ cannot both be 0. Otherwise $a$ divides both $q$ and $r$ so that $a^2$ divides $q^2 + r^2 = ap$. But then $a$ divides $p$, which is impossible given that $1 < a < p$ and $p$ is prime.

Now $m^2 + n^2 \equiv q^2 + r^2 \equiv 0 \pmod{a}$, so that $m^2 + n^2 = ab$ for some integer $b$, with $b \ge 1$ since $m$ and $n$ are not both 0. But $-\frac{a}{2} \le m, n \le \frac{a}{2}$ implies that $0 \le m^2, n^2 \le \frac{a^2}{4}$, and thus $ab = m^2 + n^2 \le \frac{a^2}{2}$. Therefore $b \le \frac{a}{2} < a$.

Notice that $ap \cdot ab = (q^2 + r^2)(m^2 + n^2)$, and so

$$a^2 \cdot bp = (qm + rn)^2 + (qn - rm)^2, \tag{1.1.2}$$

using equation (1.1.1). Since $m \equiv q \pmod{a}$ and $n \equiv r \pmod{a}$, we have that

$$qm + rn \equiv m^2 + n^2 \equiv 0 \pmod{a}$$

and

$$qn - rm \equiv mn - nm \equiv 0 \pmod{a}.$$

With $qm + rn$ and $qn - rm$ both divisible by $a$, we can cancel $a^2$ from both sides of (1.1.2) and conclude that

$$bp = \left(\frac{qm + rn}{a}\right)^2 + \left(\frac{qn - rm}{a}\right)^2.$$

So $bp = s^2 + t^2$ for some integers $s$ and $t$, and some $b$ with $1 \leq b < a$, as we wanted to show. □

The following theorem was stated without proof by Girard in 1625, and by Fermat in a letter to Mersenne dated December 25, 1640. (It is sometimes referred to as *Fermat's Christmas Theorem*.) Euler provided the first known proof in 1749.

**Theorem 1.1.4.** *Let $p$ be a prime number with $p \equiv 1 \pmod 4$. Then there are unique integers $s > t > 0$ for which $p = s^2 + t^2$.*

*Proof.* If $p \equiv 1 \pmod 4$, then $x^2 + 1 \equiv 0 \pmod p$ has a solution, so that $k^2 + 1^2 = ap$ for some integers $k$ and $a$. (This is a consequence of Exercise 0.2.4.) We can further assume that $1 \leq k \leq \frac{p-1}{2}$, since $k$ and $p - k$ are both solutions of $x^2 + 1 \equiv 0 \pmod p$. We then find that $0 < a < p$. If $a > 1$, then Lemma 1.1.3 implies that there is some $b$ with $1 \leq b < a$ and integers $s$ and $t$ so that $bp = s^2 + t^2$. If $b > 1$, we can repeat the application of Lemma 1.1.3 with $b$ in place of $a$. Eventually, we must obtain $b = 1$, so that $p = s^2 + t^2$, and we can assume as usual that $s \geq t \geq 0$. In fact, $s > t > 0$ since $p$ is odd and not a square.

To show uniqueness of this expression, suppose that $p = q^2 + r^2 = s^2 + t^2$ with $q > r > 0$ and $s > t > 0$. Then (1.1.1) implies that

$$p^2 = (qs + rt)^2 + (qt - rs)^2 = (qs - rt)^2 + (qt + rs)^2. \tag{1.1.3}$$

Note that $qs + rt$, $qs - rt$, and $qt + rs$ are all positive.

With $k^2 + 1 = ap$ so that $k^2 \equiv -1 \pmod p$, we have

$$q^2 \equiv -r^2 \equiv (kr)^2 \pmod p \quad \text{and} \quad s^2 \equiv -t^2 \equiv (kt)^2 \pmod p,$$

and thus $p$ divides both $q^2 - (kr)^2 = (q - kr)(q + kr)$ and $s^2 - (kt)^2 = (s - kt)(s + kt)$. Since $p$ is prime, it must divide at least one term in each product. Changing the sign of $k$ if necessary, we can assume without loss of generality that $p$ divides $q - kr$. We show as follows that then $p$ also divides $s - kt$. If instead $p$ divides $s + kt$, then $q \equiv kr \pmod p$ and $s \equiv -kt \pmod p$. But then

$$qs - rt \equiv (kr)(-kt) - rt \equiv -(k^2 + 1)rt \equiv 0 \pmod p,$$

since $p$ divides $k^2 + 1$, and

$$qt + rs \equiv krt + r(-kt) \equiv 0 \pmod p.$$

So (1.1.3) implies that

$$1 = \left(\frac{qs - rt}{p}\right)^2 + \left(\frac{qt + rs}{p}\right)^2,$$

with 1 the sum of the squares of two positive integers. This is impossible.

Thus $q \equiv kr \pmod{p}$ and $s \equiv kt \pmod{p}$, and we find that

$$qs + rt \equiv (kr)(kt) + rt \equiv (k^2 + 1)rt \equiv 0 \pmod{p}$$

and

$$qt - rs \equiv (kr)t - r(kt) \equiv 0 \pmod{p}.$$

Then (1.1.3) implies that

$$1 = \left(\frac{qs + rt}{p}\right)^2 + \left(\frac{qt - rs}{p}\right)^2.$$

Since $qs + rt > 0$, we must conclude that $qs + rt = p$ and $qt - rs = 0$. Then we have

$$pr = (qs + rt)r = q(rs) + r^2t = q(qt) + r^2t = (q^2 + r^2)t = pt,$$

so that $r = t$, and then $q = s$. Therefore the expression $p = s^2 + t^2$ is unique if $s > t > 0$. □

The following example illustrates how an equation $k^2 + 1 = ap$ eventually leads to a solution of $p = s^2 + t^2$, as in the first part of this proof.

**Example.** Let $p = 89$ and suppose we have found that $34^2 + 1^2 = 89 \cdot 13$. Applying Lemma 1.1.3 with $a = 13$, we find that $34 \equiv -5 \pmod{13}$ and $1 \equiv 1 \pmod{13}$ in minimal absolute value, so that $(-5)^2 + 1^2 = 26 = 13 \cdot 2$. So now by Proposition 1.1.1,

$$\begin{aligned}(89 \cdot 13) \cdot (13 \cdot 2) &= (34^2 + 1^2)((-5)^2 + 1^2) \\ &= (34(-5) + 1)^2 + (34 - (-5))^2 = (-169)^2 + 39^2.\end{aligned}$$

Both terms in the final sum are divisible by $a^2$, and so $89 \cdot 2 = (-13)^2 + 3^2$.

We now repeat the process with $a = 2$. Here we have $-13 \equiv 1 \pmod{2}$ and $3 \equiv 1 \pmod{2}$, and $1^2 + 1^2 = 2 \cdot 1$, so that

$$\begin{aligned}(89 \cdot 2) \cdot (2 \cdot 1) &= ((-13)^2 + 3^2)(1^2 + 1^2) \\ &= (-13 + 3)^2 + (-13 - 3)^2 = (-10)^2 + (-16)^2.\end{aligned}$$

We cancel $2^2$, and conclude that $89 = (-5)^2 + (-8)^2$, or $89 = 8^2 + 5^2$. ◊

**Exercise 1.1.3.** For each of the following primes $p$, verify that the given value of $k$ satisfies the congruence $x^2 + 1 \equiv 0 \pmod{p}$. Use that fact to write $p$ as a sum of two squares.

(a) $p = 229, k = 107$.

(b) $p = 277, k = 60$.

(c) $p = 337, k = 148$.

(d) $p = 541, k = 52$.

The preceding example may seem an absurdly circuitous method of representing a prime as a sum of two squares, which we have seen requires relatively little trial-and-error calculation in practice. However, it illustrates a reduction method that we will find recurring in various forms throughout this text. Taking a reverse approach, however, we can also use Proposition 1.1.2, together with a representation of $p$ as a sum of two squares, to solve the quadratic congruence $x^2 \equiv -1 \pmod{p}$, as the following example demonstrates.

**Example.** Let $p = 569$, a prime with $p \equiv 1 \pmod 4$, and suppose we have observed that $569 = 20^2 + 13^2$. Since $1 = 20(2) + 13(-3)$ by the Euclidean algorithm, then the proof of Proposition 1.1.2 shows that $x^2 + 1 \equiv 0 \pmod{569}$ has a solution $k = 20(-3) - 13(2) = -86$. ◊

**Exercise 1.1.4.** For each of the following primes $p$, use trial-and-error to find a way of writing $p$ as a sum of two squares. Use that expression to find a solution of $x^2 \equiv -1 \pmod{p}$, as in the preceding example.

(a) $p = 509$.

(b) $p = 757$.

(c) $p = 953$.

(d) $p = 1009$.

### Representations of Composite Integers as Sums of Two Squares.

Since $2 = 1^2 + 1^2$ and all primes $p \equiv 1 \pmod 4$ can be written as sums of two squares, then (1.1.1) implies that any product of these primes can also be represented as a sum of two squares, although not necessarily properly. The following lemma allows us to determine when proper representations exist.

**Lemma 1.1.5.** *Let $m = a^2 + b^2$ and $n = c^2 + d^2$, with $\gcd(a, b) = 1 = \gcd(c, d)$. Then $g = \gcd(ac + bd, ad - bc)$ and $h = \gcd(ac - bd, ad + bc)$ are common divisors of $m$ and $n$, and $\gcd(g, h)$ equals 1 or 2.*

*Proof.* Let $aq + br = 1$ and $cs + dt = 1$ for some integers $q$, $r$, $s$, and $t$. Then we find that

$$\begin{aligned}(ac + bd)(as + bt) + (ad - bc)(at - bs)\\ &= a^2cs + abct + abds + b^2dt + a^2dt - abds - abct + b^2cs\\ &= a^2cs + b^2dt + a^2dt + b^2cs = (a^2 + b^2)(cs + dt) = m \cdot 1 = m,\end{aligned}$$

and, in a similar way,

$$\begin{aligned}(ac + bd)(cq + dr) + (ad - bc)(dq - cr) &= n,\\ (ac - bd)(as - bt) + (ad + bc)(at + bs) &= m,\\ (ac - bd)(cq - dr) + (ad + bc)(cr + dq) &= n.\end{aligned}$$

Thus $m$ and $n$ can be expressed as combinations of $ac + bd$ and $ad - bc$, so that $g = \gcd(ac + bd, ad - bc)$ divides both $m$ and $n$. Likewise, $m$ and $n$ are combinations of $ac - bd$ and $ad + bc$, so that $h = \gcd(ac - bd, ad + bc)$ divides $m$ and $n$. Finally, one can verify that

$$\begin{aligned}(ac+bd)(qs+rt)+(ad-bc)(qt-rs)+(ac-bd)(qs-rt)+(ad+bc)(qt+rs)\\ &= 2acqs + 2adqt + 2bcrs + 2bdrt = 2(aq + br)(cs + dt) = 2.\end{aligned}$$

Thus $\gcd(g, h) = \gcd(ac + bd, ad - bc, ac - bd, ad + bc)$ divides 2. □

We can now prove our main result for this section.

**Theorem 1.1.6.** *Let $a$ be a positive integer. Then*

(1) *$a$ is properly represented by $x^2 + y^2$ if and only if $a$ is not divisible by 4 nor by any prime $p \equiv 3 \pmod 4$, and*

(2) *$a$ is represented by $x^2 + y^2$ if and only if the exponent in $a$ of every prime $p \equiv 3 \pmod 4$ is even.*

*Proof.* If $p \equiv 3 \pmod 4$, then $\left(\frac{-1}{p}\right) = -1$ so that $x^2 \equiv -1 \pmod p$ has no solution. A square is congruent to 0 or 1 modulo 4, so $x^2 \equiv -1 \pmod 4$ likewise has no solution. Thus if $a$ is divisible by 4 or a prime $p \equiv 3 \pmod 4$, then $x^2+1 \equiv 0 \pmod a$ cannot have a solution, and Proposition 1.1.2 implies that there is no proper representation of $a$ by $x^2 + y^2$. This establishes the necessity of condition (1). To show that this condition is sufficient, we show that if $p$ is prime with $p \equiv 1 \pmod 4$, then $p^e$ has a proper representation by $x^2 + y^2$ for all $e \geq 1$. We proceed by induction on $e$. We know that $p = q^2 + r^2$ with $\gcd(q, r) = 1$ by Theorem 1.1.4, so the statement is true when $e = 1$. Assume that $p^{e-1} = s^2 + t^2$ with $\gcd(s, t) = 1$ for some $e > 1$. Then (1.1.1) shows that

$$p^e = pp^{e-1} = (qs + rt)^2 + (qt - rs)^2 = (qs - rt)^2 + (qt + rs)^2.$$

Lemma 1.1.5 implies that $g = \gcd(qs+rt, qt-rs)$ and $h = \gcd(qs-rt, qt+rs)$ are both divisors of $p$, but that $g$ and $h$ cannot both equal $p$, since $\gcd(g,h)$ divides 2. So $p^e$ has at least one proper representation by $x^2+y^2$.

Now if $\gcd(a,b) = 1$, and $a = q^2+r^2$ and $b = s^2+t^2$ with $\gcd(q,r) = 1 = \gcd(s,t)$, then Lemma 1.1.5 implies immediately that $ab$ has at least one proper representation by $x^2+y^2$. So by an inductive argument on $k$, we see that if $a = 2^e \cdot p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$, with each $p_i \equiv 1 \pmod 4$ a distinct prime, each $e_i$ positive, and $e = 0$ or 1, then $x^2+y^2$ properly represents $a$.

For condition (2), suppose first that $a = q^2+r^2$ with $\gcd(q,r) = g$. If $q = gs$ and $r = gt$, then $a = g^2 b$, where $b = s^2+t^2$ with $\gcd(s,t) = 1$. If $p \equiv 3 \pmod 4$, then condition (1) shows that $p$ cannot divide $b$, and so the exponent of $p$ in $a$ equals the exponent of $p$ in $g^2$, which must be even. Conversely, suppose that the exponent of $p$ in $a$ is even for every prime $p \equiv 3 \pmod 4$. We can write $a = g^2 b$ with $b$ squarefree. Then $b$ is not divisible by 4 or any prime $p \equiv 3 \pmod 4$, so that $b = q^2+r^2$ for some $q$ and $r$ by condition (1). But now $a = (gq)^2 + (gr)^2$ is represented by $x^2+y^2$. □

**Exercise 1.1.5.** Find all ways of writing each of the following composite integers $a$ as a sum of two squares, $a = q^2+r^2$ with $q \geq r \geq 0$.

(a) $a = 125$.

(b) $a = 180$.

(c) $a = 325$.

(d) $a = 985$.

(e) $a = 1000$.

(f) $a = 27625$.

## 1.2 Gaussian Integers

In §1.1, we answered questions about sums of two squares in terms of integers themselves, although at times with rather convoluted arguments. In the remainder of Chapter 1, we take a different approach, reconsidering this problem in a particular subset of complex numbers. Our motivation is the observation that a sum of two squares of integers can also be written as a product of complex numbers, $q^2+r^2 = (q+ri)(q-ri)$. By writing the sum as a product, we can invoke properties of divisibility and factorization, which we review in this section, that make results about sums of two squares arise more naturally.

**Definition.** A complex number $v = q+ri$ is called a *Gaussian integer* if $q$ and $r$ are integers. We denote the set of all Gaussian integers as $\mathbb{Z}[i]$, and we may refer to elements of $\mathbb{Z}$ as *rational integers* for distinction.

The following definition, which applies to arbitrary complex numbers, will be useful in establishing properties of Gaussian integers.

**Definition.** If $x$ and $y$ are real numbers, then the *conjugate* of the complex number $z = x + yi$ is $\overline{z} = x - yi$, and the *norm* of $z$ is the real number $N(z) = z \cdot \overline{z} = x^2 + y^2$.

Notice that the norm of a Gaussian integer is a rational integer.

**Exercise 1.2.1.** If $w$ and $z$ are complex numbers, show that $\overline{w+z} = \overline{w} + \overline{z}$ and $\overline{w \cdot z} = \overline{w} \cdot \overline{z}$.

**Proposition 1.2.1.** *If $w$ and $z$ are complex numbers, then $N(w \cdot z) = N(w) \cdot N(z)$.*

*Proof.* Assuming the second equation in Exercise 1.2.1, then

$$N(w \cdot z) = (w \cdot z) \cdot (\overline{w \cdot z}) = (w \cdot z) \cdot (\overline{w} \cdot \overline{z}) = (w \cdot \overline{w}) \cdot (z \cdot \overline{z}) = N(w) \cdot N(z),$$

as we wanted to show. □

**Definition.** Let $u$, $v$, and $w$ be Gaussian integers. Then we say that

(1) $v$ *divides* $w$ if $w = v \cdot z$ for some $z$ in $\mathbb{Z}[i]$;

(2) $u$ is a *unit* in $\mathbb{Z}[i]$ if $u$ divides 1;

(3) $v$ and $w$ are *associates* in $\mathbb{Z}[i]$ if $v$ divides $w$ and $w$ divides $v$.

**Exercise 1.2.2.** Let $m$ be a rational integer. Show that $m$ divides $v = q + ri$ in $\mathbb{Z}[i]$ if and only if $m$ divides $q$ and $m$ divides $r$ in $\mathbb{Z}$.

A consequence of Exercise 1.2.2 is that there is no ambiguity in the statement "$m$ divides $n$" when $m$ and $n$ are integers—the claim is true in $\mathbb{Z}[i]$ precisely when it is true in $\mathbb{Z}$.

**Exercise 1.2.3.** Let $u$, $v$, and $w$ be Gaussian integers. Show that the following statements are true.

(a) If $v$ divides $w$ in $\mathbb{Z}[i]$, then $N(v)$ divides $N(w)$ in $\mathbb{Z}$.

(b) $u$ is a unit in $\mathbb{Z}[i]$ if and only if $N(u) = 1$.

(c) If $v$ and $w$ are associates in $\mathbb{Z}[i]$, then $N(v) = N(w)$.

**Example.** The Gaussian integer $v = 2 + i$ does not divide $w = 7 + 13i$, since $N(v) = 5$ does not divide $N(w) = 218$. The converse of Exercise 1.2.3(a) is not true in general, however. For instance, $N(2 + i) = 5$ divides $N(3 + i) = 10$, but we can show as follows that $2 + i$ does not divide $3 + i$ in $\mathbb{Z}[i]$. If $3 + i = (2 + i)(s + ti) = (2s - t) + (s + 2t)i$, so that $2s - t = 3$ and $s + 2t = 1$, we find that $5s = 2(2s - t) + (s + 2t) = 7$, but then $s$ is not an integer. ◊

**Exercise 1.2.4.** Use Exercise 1.2.3(b) to show that there are precisely four units in $\mathbb{Z}[i]$: 1, $-1$, $i$, and $-i$.

**Exercise 1.2.5.** Show that $v$ and $w$ are associates in $\mathbb{Z}[i]$ if and only if $w = uv$ for some unit $u$ of $\mathbb{Z}[i]$. Show that each nonzero element $v = a + bi$ in $\mathbb{Z}[i]$ has four associates: $a + bi$, $-a - bi$, $-b + ai$, and $b - ai$.

Notice that $\overline{v} = a - bi$ is typically not an associate of $v$.

**Exercise 1.2.6.** Define a relation $\sim$ on $\mathbb{Z}[i]$ by saying that $v \sim w$ if and only if $v$ is an associate of $w$.

(a) Show that $\sim$ is an equivalence relation on $\mathbb{Z}[i]$.

(b) Show that if $u \sim v$ and $w \sim z$, then $uw \sim vz$.

(c) Show that if $u \sim v$ and $w \sim z$, then $u$ divides $w$ if and only if $v$ divides $z$.

**Irreducible Factorization in the Gaussian Integers.** In this subsection, we outline a proof that Gaussian integers have a form of unique prime factorization. The role analogous to prime numbers in the rational integers is played by irreducible Gaussian integers, defined as follows.

**Definition.** Let $w$ be an element of $\mathbb{Z}[i]$ that is neither zero nor a unit. We say that $w$ is *reducible* in $\mathbb{Z}[i]$ if it is possible to write $w = u \cdot v$ for some $u$ and $v$ in $\mathbb{Z}[i]$ with neither $u$ nor $v$ a unit. If no such factorization is possible, we say that $w$ is *irreducible* in $\mathbb{Z}[i]$.

**Exercise 1.2.7.** If $N(w)$ is prime in $\mathbb{Z}$, show that $w$ is irreducible in $\mathbb{Z}[i]$.

**Exercise 1.2.8.** Let $w$ be a reducible Gaussian integer. Show that $w$ can be written in some way as a product of irreducible elements of $\mathbb{Z}[i]$. (Hint: If not, we can assume that $N(w)$ is as small as possible among all reducible Gaussian integers $w$ that cannot be so expressed. Use the fact that $w$ is a product of Gaussian integers that are not units to derive a contradiction.)

The irreducible factorization described in Exercise 1.2.8 is essentially unique. Proposition 1.2.3, a division algorithm for Gaussian integers, is the key to establishing this claim.

**Lemma 1.2.2.** *For every complex number $w$, there is a Gaussian integer $v$ so that $N(w - v) < 1$.*

*Proof.* Let $w = x + yi$ with $x, y$ in $\mathbb{R}$. Let $q$ and $r$ be the closest rational integers to $x$ and $y$, respectively, so that $|x - q| \leq \frac{1}{2}$ and $|y - r| \leq \frac{1}{2}$. Then $v = q + ri$ is

an element of $\mathbb{Z}[i]$ and

$$N(w-v) = N((x-q)+(y-r)i) = (x-q)^2+(y-r)^2 \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2,$$

which is strictly smaller than 1. □

**Proposition 1.2.3.** *If $v$ and $w$ are elements of $\mathbb{Z}[i]$ with $w \neq 0$, then there are elements $u$ and $z$ in $\mathbb{Z}[i]$ so that $v = wz + u$, with $N(u) < N(w)$.*

*Proof.* Since $v/w$ is a complex number, Lemma 1.2.2 implies the existence of a Gaussian integer $z$ for which $N\left(\frac{v}{w} - z\right) < 1$. Let $u$ be the Gaussian integer $v - wz$. We have that

$$N(u) = N(v-wz) = N(w) \cdot N\left(\frac{v}{w} - z\right) < N(w) \cdot 1 = N(w).$$

So $v = wz + u$ with $N(u) < N(w)$. □

**Example.** Let $v = 23+6i$ and $w = 7-3i$. Following the method of the preceding proofs, we have

$$\frac{v}{w} = \frac{23+6i}{7-3i} \cdot \frac{7+3i}{7+3i} = \frac{143+111i}{58} \approx (2.47)+(1.91)i.$$

Selecting the integers closest to these rational coordinates, we can let $z = 2+2i$. Now if

$$v - wz = (23+6i) - (7-3i)(2+2i) = (23+6i) - (20+8i) = 3-2i = u,$$

then $N(u) = 13 < N(w) = 58$. The quotient and remainder on division of $v$ by $w$ are generally not unique under this condition. For example, if $z = 3+2i$, then $v - wz = -4+i = u$ also satisfies $N(u) < N(w)$. ◊

**Exercise 1.2.9.** For each pair $v$ and $w$ below, use the method of Proposition 1.2.3 to write $v = wz + u$ with $N(u) < N(w)$.

(a) $v = 37 - 10i$ and $w = 4 + i$.

(b) $v = 13 + 19i$ and $w = 3 + 4i$.

(c) $v = 41 + 9i$ and $w = 9 + 7i$.

The division algorithm of Proposition 1.2.3 allows us to derive a Euclidean algorithm on Gaussian integers. We make the following claim, needed in the proof of Theorem 1.2.4, which we demonstrate with an example: if $u$ is an irreducible Gaussian integer and $z$ is an element of $\mathbb{Z}[i]$ not divisible by $u$, then there are Gaussian integers $v$ and $w$ so that $1 = uv + zw$.

**Example.** Let $u = 5 + 4i$, irreducible in $\mathbb{Z}[i]$ since $N(u) = 41$ is prime, and let $z = 23 + 36i$. Here

$$\frac{z}{u} = \frac{23 + 36i}{5 + 4i} \cdot \frac{5 - 4i}{5 - 4i} = \frac{259 + 88i}{41}.$$

The closest rational integers to $\frac{259}{41}$ and $\frac{88}{41}$ are 6 and 2, respectively, and we find that $(23 + 36i) - (6 + 2i)(5 + 4i) = 1 + 2i$. Now as in the Euclidean algorithm on integers, we divide the divisor of the first equation by this nonzero remainder. In this case,

$$\frac{5 + 4i}{1 + 2i} \cdot \frac{1 - 2i}{1 - 2i} = \frac{13 - 6i}{5},$$

with 3 and $-1$ the closest integers to $\frac{13}{5}$ and $\frac{-6}{5}$, respectively, and we calculate that $(5 + 4i) - (3 - i)(1 + 2i) = -i$, a unit in $\mathbb{Z}[i]$. We determine that

$$1 = i \cdot -i = i \cdot [u - (3 - i)(z - (6 + 2i)u)] = u \cdot 21i + z(-1 - 3i)$$

by substituting for $1 + 2i$ and multiplying by $i$. ◊

**Theorem 1.2.4.** *Let $u$ be an irreducible Gaussian integer. If $u$ divides a product $zy$ of Gaussian integers, then $u$ divides $z$ or $u$ divides $y$.*

*Proof.* Let $u$ be irreducible in $\mathbb{Z}[i]$. Suppose that $u$ divides $zy$, but that $u$ does not divide $z$. Then, as noted above, we can write $1 = uv + zw$ for some $v$ and $w$ in $\mathbb{Z}[i]$. But now

$$y = y \cdot 1 = y(uv + zw) = u(vy) + (zy)w.$$

Since $u$ divides $zy$, we conclude that $u$ divides $y$. □

**Exercise 1.2.10.** Show that every Gaussian integer that is neither zero nor a unit can be written *uniquely* as a product of irreducible elements, aside from the order of the factors and multiplication by units. (Note that an irreducible Gaussian integer is regarded as a product of irreducible elements with just one factor. Hint: Suppose that $w$ is an element of smallest norm in $\mathbb{Z}[i]$ that can be written in two distinct ways as products of irreducible elements: $w = u_1 \cdot u_2 \cdots u_k$ and $w = z_1 \cdot z_2 \cdots z_\ell$. Use Theorem 1.2.4 to show that $u_1$ must divide $z_i$ for some $1 \le i \le \ell$, and derive a contradiction.)

**Classification of Irreducible Gaussian Integers.** The following corollary of Theorem 1.2.4 allows us to classify all irreducible Gaussian integers.

**Corollary 1.2.5.** *Let $z$ be an irreducible element in $\mathbb{Z}[i]$. Then $z$ divides some rational prime, that is, some prime number $p$ in $\mathbb{Z}$.*

*Proof.* Let $N(z) = z \cdot \overline{z} = a$, an element of $\mathbb{Z}$. We know that $a > 1$ because $z$ is neither zero nor a unit in $\mathbb{Z}[i]$. So $a$ can be factored as a product of rational primes, $a = p_1 p_2 \cdots p_k$. Since $z$ is irreducible and $z$ divides $a$, Theorem 1.2.4 implies that $z$ divides at least one term in this product. That is, $z$ divides some rational prime. □

Therefore we can produce all irreducible Gaussian integers by factoring each rational prime as an element of $\mathbb{Z}[i]$. The following theorem gives us a criterion for when such a factorization occurs.

**Theorem 1.2.6.** *Let $p$ be a prime number. Then $p$ is reducible as an element of $\mathbb{Z}[i]$ if and only if the congruence $x^2 + 1 \equiv 0 \pmod{p}$ has a solution. If so, then there is an element $z$ in $\mathbb{Z}[i]$ so that $p = z \cdot \overline{z}$, with both $z$ and $\overline{z}$ irreducible in $\mathbb{Z}[i]$.*

*Proof.* Suppose first that $p$ is reducible in $\mathbb{Z}[i]$, say that $p = z \cdot w$ with neither $z$ nor $w$ a unit. Then $N(p) = p^2 = N(z) \cdot N(w)$ with $N(z) \neq 1$ and $N(w) \neq 1$, so that $N(z) = p = N(w)$. If $z = q + ri$, then $q^2 + r^2 = p$, so that $x^2 + 1 \equiv 0 \pmod{p}$ has a solution by Proposition 1.1.2.

Conversely, suppose that $k$ satisfies the congruence $x^2 + 1 \equiv 0 \pmod{p}$. Then $p$ divides $k^2 + 1 = (k + i)(k - i)$. If $p$ were irreducible in $\mathbb{Z}[i]$, then $p$ would divide a term in this product, impossible by Exercise 1.2.2. So $p$ is reducible in $\mathbb{Z}[i]$, and we conclude that $p = z \cdot w$ with $N(z) = p = N(w)$ as above. Since $N(z) = z \cdot \overline{z} = p = z \cdot w$, it follows that $w = \overline{z}$. Thus $p = z \cdot \overline{z}$ in $\mathbb{Z}[i]$, with both $z$ and $\overline{z}$ irreducible in $\mathbb{Z}[i]$ by Exercise 1.2.7. □

Since $x^2 + 1 \equiv 0 \pmod{p}$ always has a solution when $p \equiv 1 \pmod{4}$, we obtain the following statement, which we proved in §1.1 by a more indirect argument, as a corollary of this result.

**Corollary 1.2.7.** *If $p \equiv 1 \pmod{4}$ is a prime number, then $x^2 + y^2 = p$ has a unique integer solution $(x, y) = (q, r)$ with $q > r > 0$.*

*Proof.* Theorem 1.2.6 shows that $p = z \cdot \overline{z} = N(z)$ for some irreducible element $z$ in $\mathbb{Z}[i]$. If $z = q + ri$, then $N(z) = q^2 + r^2$, so that $x^2 + y^2 = p$ has an integer solution. If we assume that $q > r > 0$, which is true for exactly one of the associates of $z$ or one of the associates of $\overline{z}$, then the uniqueness of the irreducible factorization of $p$ shows that this solution is unique. □

**Corollary 1.2.8.** *The irreducible elements in $\mathbb{Z}[i]$ consist precisely of the following elements and their associates.*

(1) *$p$, where $p$ is a rational prime congruent to 3 modulo 4.*
(2) *$q + ri$ and $q - ri$, where $q^2 + r^2 = p \equiv 1 \pmod{4}$ is prime and $q > r > 0$.*
(3) *$1 + i$.*

*Proof.* If $p \equiv 3 \pmod 4$, then $x^2 + 1 \equiv 0 \pmod p$ has no solution, and $p$ is irreducible in $\mathbb{Z}[i]$ by Theorem 1.2.6. If $p \equiv 1 \pmod 4$, then $p = (q + ri)(q - ri)$ for some unique $q > r > 0$ as noted in Corollary 1.2.7. Here $q + ri$ and $q - ri$ are not associates, since $q \neq r$. Finally, $2 = (1+i)(1-i)$ in $\mathbb{Z}[i]$, with $1-i = -i(1+i)$ an associate of $1+i$. So aside from unit multiples, 2 has just one irreducible factor in $\mathbb{Z}[i]$. □

**Example.** The rational integer $n = 9724 = 2^2 \cdot 11 \cdot 13 \cdot 17$ factors as

$$(1 + i)^2 \cdot (1 - i)^2 \cdot 11 \cdot (3 + 2i) \cdot (3 - 2i) \cdot (4 + i) \cdot (4 - i)$$

in $\mathbb{Z}[i]$. Aside from unit multiples, this factorization into irreducible Gaussian integers is unique. ◊

**Example.** Suppose we wish to write $\upsilon = 73 - 23i$ as a product of irreducible elements in $\mathbb{Z}[i]$. Notice first that $N(\upsilon) = \upsilon\overline{\upsilon} = 73^2 + (-23)^2 = 5858 = 2 \cdot 29 \cdot 101$ in $\mathbb{Z}$. Each of these rational primes factors in $\mathbb{Z}[i]$. We find that

$$N(\upsilon) = \upsilon\overline{\upsilon} = (1 + i)(1 - i)(5 + 2i)(5 - 2i)(10 + i)(10 - i).$$

By unique factorization, $\upsilon$ and $\overline{\upsilon}$ must contain these same factors. The associate elements $1+i$ and $1-i$ both divide $\upsilon$, and we find that $73-23i = (1+i)(25-48i)$. Now either $5 + 2i$ or $5 - 2i$ divides $25 - 48i$. We find that the assumption that $25 - 48i = (5 + 2i)(s + ti) = (5s - 2t) + (2s + 5t)i$ leads to the conclusion that $5(25) + 2(-48) = 5(5s - 2t) + 2(2s + 5t)$, that is, $29 = 29s$, so that $s = 1$, and then $t = -10$. (On the other hand, if $25-48i = (5-2i)(s+ti) = (5s+2t)+(-2s+5t)i$, then $5(25) - 2(-48) = 5(5s + 2t) - 2(-2s + 5t)$, so that $221 = 29s$. In this case, $s$ is not an integer.) So

$$73 - 23i = (1 + i)(5 + 2i)(1 - 10i) = (1 - i)(5 + 2i)(10 + i),$$

among other expressions. ◊

As we see here, we can write $\upsilon$ in different forms using multiplication by units. But there are no essentially distinct factorizations of $\upsilon$. In §1.4, we will establish criteria for divisibility of Gaussian integers that allow us to avoid the trial-and-error approach of this example.

**Exercise 1.2.11.** Write each $\upsilon$ below as a product of irreducible Gaussian integers.

(a) $\upsilon = 850$.

(b) $\upsilon = 4125$.

(c) $\upsilon = 37 - 12i$.

(d) $\upsilon = -11 + 27i$.

## 1.3 Ideal Form for Gaussian Integers

In this section, we introduce an alternative notation for Gaussian integers, which we call *ideal form* in anticipation of the introduction of ideals in Chapter 3. We will demonstrate in the remainder of Chapter 1 that ideal forms help describe properties of divisibility and irreducible factorization in $\mathbb{Z}[i]$, and we will see in later chapters that this notation generalizes to much broader settings, as do the techniques that we develop here. This proves to be a most valuable tool in our study of quadratic number theory.

If $v$ is a nonzero Gaussian integer, we can write $v = g(q + ri)$ with $g$ a positive rational integer and $\gcd(q, r) = 1$. If we let $a = N(q + ri) = q^2 + r^2$, then $\gcd(r, a) = 1$ since any prime common divisor of $r$ and $a$ would divide $q^2$, and thus divide $q$. So the linear congruence $rx \equiv q \pmod{a}$ has a unique solution modulo $a$. We use this observation to introduce the following notation and terminology.

**Definition.** Let $v = g(q + ri)$ be a Gaussian integer with $\gcd(q, r) = 1$ and $g$ positive. Let $a = q^2 + r^2$ and let $k$ satisfy $rk \equiv q \pmod{a}$. In this case, we call the expression $g[a : k]$ an *ideal form* for $v$. We refer to $g$, $a$, and $k$, respectively, as the *divisor*, the *subnorm*, and the *character* of this ideal form, or of the Gaussian integer $v$. If $g = 1$, we say that $v$ is *primitive*, and we write an ideal form for $v$ simply as $[a : k]$.

Note that if $v$ has ideal form $g[a : k]$, then the norm of $v$ is $N(v) = g^2 a$. The divisor $g$ and subnorm $a$ of an ideal form are uniquely determined by $v$, while the character $k$ is unique only modulo $a$. We will usually select $k$ to be as small as possible in absolute value, that is, with $-\frac{a}{2} < k \leq \frac{a}{2}$, but we will see that there are advantages in allowing the character of $v$ to take on other integers congruent to $k$ modulo $a$. (See in particular the factorization formula in Theorem 1.4.2 and the reduction algorithm of Theorem 1.5.3.)

**Exercise 1.3.1.** If a Gaussian integer $v$ has ideal form $g[a : k]$, show that $\overline{v}$, the conjugate of $v$, has ideal form $g[a : -k]$.

We will show in Corollary 1.3.5 that Gaussian integers $v$ and $w$ have the same ideal form if and only if $v$ and $w$ are associates in $\mathbb{Z}[i]$. So we might view an ideal form for $v$ as an alternative expression for the set of associates of $v$. These associates are interchangeable when considering properties of divisibility and factorization in $\mathbb{Z}[i]$ (see Exercise 1.2.6), which constitute our main application of ideal forms. Thus we may occasionally blur the distinction between associate elements of $\mathbb{Z}[i]$, and write that $v$ is equal to its ideal form, that is, $v = g[a : k]$, with the understanding that $v$ can be replaced by any of its associates.

Table 1.2. Ideal Forms for Gaussian Integers

| $q+ri$ | $[a:k]$ | $q+ri$ | $[a:k]$ | $q+ri$ | $[a:k]$ | $q+ri$ | $[a:k]$ |
|---|---|---|---|---|---|---|---|
| $1+0i$ | $[1:0]$ | $5+i$ | $[26:5]$ | $7+2i$ | $[53:-23]$ | $7+5i$ | $[74:31]$ |
| $1+i$ | $[2:1]$ | $5-i$ | $[26:-5]$ | $7-2i$ | $[53:23]$ | $7-5i$ | $[74:-31]$ |
| $2+i$ | $[5:2]$ | $5+2i$ | $[29:-12]$ | $7+3i$ | $[58:-17]$ | $9+i$ | $[82:9]$ |
| $2-i$ | $[5:-2]$ | $5-2i$ | $[29:12]$ | $7-3i$ | $[58:17]$ | $9-i$ | $[82:-9]$ |
| $3+i$ | $[10:3]$ | $5+3i$ | $[34:13]$ | $6+5i$ | $[61:-11]$ | $7+6i$ | $[85:-13]$ |
| $3-i$ | $[10:-3]$ | $5-3i$ | $[34:13]$ | $6-5i$ | $[61:11]$ | $7-6i$ | $[85:13]$ |
| $3+2i$ | $[13:-5]$ | $6+i$ | $[37:6]$ | $7+4i$ | $[65:18]$ | $9+2i$ | $[85:-38]$ |
| $3-2i$ | $[13:5]$ | $6-i$ | $[37:-6]$ | $7-4i$ | $[65:-18]$ | $9-2i$ | $[85:38]$ |
| $4+i$ | $[17:4]$ | $5+4i$ | $[41:-9]$ | $8+i$ | $[65:8]$ | $8+5i$ | $[89:-34]$ |
| $4-i$ | $[17:-4]$ | $5-4i$ | $[41:9]$ | $8-i$ | $[65:-8]$ | $8-5i$ | $[89:34]$ |
| $4+3i$ | $[25:-7]$ | $7+i$ | $[50:7]$ | $8+3i$ | $[73:27]$ | $9+4i$ | $[97:-22]$ |
| $4-3i$ | $[25:7]$ | $7-i$ | $[50:-7]$ | $8-3i$ | $[73:-27]$ | $9-4i$ | $[97:22]$ |

**Example.** The rational integer $1 = 1 + 0i$ can be expressed in ideal form as $[1 : 0]$. (Every integer satisfies the congruence $0 \cdot x \equiv 1 \pmod 1$, with 0 the smallest solution in absolute value.) More generally, a positive rational integer $n$ can be expressed as $n[1 : 0]$. ♢

In Table 1.2, we list an ideal form $[a : k]$, with $k$ minimal in absolute value, for each primitive Gaussian integer $q + ri$ with $q \geq |r|$ having subnorm $a < 100$. (This restriction on $q$ and $r$ provides exactly one representative of each associate class of elements of $\mathbb{Z}[i]$.) For example, if $v = 7 + 6i$, then $a = 7^2 + 6^2 = 85$, and $k$ is a solution of $6x \equiv 7 \pmod{85}$. Using the method of Theorem 0.1.7, we find that $k = -13$, since $6(-13) = -78 \equiv 7 \pmod{85}$. One can confirm the other table entries in a similar way.

As an aside, we note a similarity between ideal form for a Gaussian integer and polar coordinates for a point in the plane. Every complex number $x + yi$ can be identified with the point $P$ having rectangular coordinates $(x, y)$. (For a Gaussian integer, both coordinates are integers.) If $r$ is the distance from the origin to $P$, and $\theta$ is the angle formed by the positive $x$-axis and the ray from the origin through $P$, then $(r, \theta)$ is a pair of polar coordinates for $P$. For example, if $P$ is the point $(7, 6)$, corresponding to the Gaussian integer $v = 7 + 6i$, we have that $r = \sqrt{7^2 + 6^2} = \sqrt{85}$, with $\theta$ satisfying the equation $\tan\theta = 6/7$ or, equivalently, $\cot\theta = 7/6$. Notice that if $[a : k]$ is an ideal form for $v$, then $a = r^2$, while $k$ could be viewed as $7/6$ modulo 85, that is, a solution of $6x \equiv 7 \pmod{85}$.

This connection between ideal forms and polar coordinates is not exact. As noted above, $v = 7 + 6i$ has the same ideal form as any of its associates, such as $i \cdot v = -6 + 7i$, while $(7, 6)$ and $(-6, 7)$ cannot be given the same polar coordinates. The analogy is more a philosophical one—just as polar coordinates can be more convenient than rectangular coordinates when defining certain curves in

the plane, so we will see that ideal forms have some advantages in describing the divisibility and factorization aspects of Gaussian integers.

**Example.** Let $v = 33+39i = 3(11+13i)$, with $\gcd(11, 13) = 1$. Here $11^2+13^2 = 290$, and we find that $13x \equiv 11 \pmod{290}$ has $k = 11 \cdot 67 = 737 \equiv -133 \pmod{290}$ as its unique solution. So $3[290 : -133]$ is an ideal form for $v$. ◊

Note, by way of caution, that factoring out the common term of 3 is necessary in this example. Here $33^2 + 39^2 = 2610$, and $39x \equiv 33 \pmod{2610}$ does have a solution, in fact, three distinct solutions, $x = -133$, $x = 737$, and $x = -1003$ modulo 2610. But $[2610 : k]$ is not a correct ideal form for $v = 33 + 39i$, nor in fact for any Gaussian integer, when $k = -133$, $k = 737$, or $k = -1003$, as we demonstrate following the next proposition.

**Proposition 1.3.1.** *If $g[a : k]$ is an ideal form for a Gaussian integer $v = g(q+ri)$, then $k^2 + 1 \equiv 0 \pmod{a}$ and $qk \equiv -r \pmod{a}$.*

*Proof.* If $v = g(q + ri)$ has ideal form $g[a : k]$, then $rk \equiv q \pmod{a}$, and thus

$$r^2(k^2 + 1) = (rk)^2 + r^2 \equiv q^2 + r^2 \pmod{a}.$$

But $a = q^2 + r^2$ by the definition of ideal forms, so that $a$ divides $r^2(k^2 + 1)$. Since $\gcd(r, a) = 1$, it follows that $k^2 + 1 \equiv 0 \pmod{a}$. Also, $rk \equiv q \pmod{a}$ implies that $rk^2 \equiv qk \pmod{a}$. But then $k^2 \equiv -1 \pmod{a}$ implies that $qk \equiv -r \pmod{a}$. □

**Example.** There is no Gaussian integer having ideal form $[2610 : -133]$, since 2610 does not divide $(-133)^2 + 1 = 17690$. Gaussian integers having ideal form $[2610 : 737]$ or $[2610 : -1003]$ are similarly ruled out. ◊

In the proof of Theorem 1.1.6, we noted that $x^2 + 1 \equiv 0 \pmod{a}$ has a solution $k$ if and only if $a$ is not divisible by 4 nor by a prime $p \equiv 3 \pmod 4$. Proposition 1.3.1 shows that this is a necessary condition for $g[a : k]$ to be an ideal form of a Gaussian integer. In §1.5, we will find that this condition is also sufficient to ensure the existence of a Gaussian integer with ideal form $g[a : k]$.

**Example.** The congruence $x^2 + 1 \equiv 0 \pmod{109}$ has two solutions, $x = 33$ and $x = -33$. Thus $[109 : 33]$ and $[109 : -33]$ are *potentially* ideal forms for Gaussian integers. However, $[109 : k]$ is not an ideal form if $k$ is not congruent to $\pm 33$ modulo 109. ◊

**Exercise 1.3.2.** Find an ideal form for each Gaussian integer $w$ below.

(a) $w = 11 + 3i$.

(b) $w = 9 - 7i$.

(c) $w = 13 + 5i$.

(d) $w = -11 + 27i$.

(e) $w = 14 + 16i$.

(f) $w = 141 + 3i$.

**Exercise 1.3.3.** If $v$ has ideal form $g[a : k]$, use Proposition 1.3.1 to show that $i \cdot v$ also has ideal form $g[a : k]$.

**Divisibility of Gaussian Integers Using Ideal Forms.** The following theorem states a divisibility criterion for Gaussian integers using ideal forms.

**Theorem 1.3.2.** *Let $v$ and $w$ be nonzero Gaussian integers having ideal forms $g[a : k]$ and $h[b : \ell]$, respectively. Then $v$ divides $w$ in $\mathbb{Z}[i]$ if and only if*

$$g \text{ divides } h, \quad ag \text{ divides } bh, \quad \text{and} \quad h\ell \equiv hk \pmod{ag}. \tag{1.3.1}$$

**Example.** From Table 1.2, we see that $v = 2 + i$ and $w = 3 + i$ have ideal forms $[5 : 2]$ and $[10 : 3]$, respectively. Thus $v$ does not divide $w$, although 5 divides 10, since 3 is not congruent to 2 modulo 5. (This confirms a direct calculation in an example in §1.2.) On the other hand, $v$ divides $z = 3 - i$, which has ideal form $[10 : -3]$, since 5 divides 10 and $-3 \equiv 2 \pmod 5$. ♢

**Exercise 1.3.4.** Let $w$ be a Gaussian integer with ideal form $h[b : \ell]$. Show that $v = 1 + i$ divides $w$ if and only if $h$ is even or $b$ is even.

We prove Theorem 1.3.2 after the following preliminary observations.

**Lemma 1.3.3.** *Let $v$ and $w$ be Gaussian integers having ideal forms $g[a : k]$ and $h[b : \ell]$, respectively. If $v$ divides $w$ in $\mathbb{Z}[i]$, then $g$ divides $h$ in $\mathbb{Z}$.*

*Proof.* Note that $g$ divides $v$ in $\mathbb{Z}[i]$ by the definition of ideal forms. So if $v$ divides $w$, then $g$ must also divide $w$. We can write $w = h(m + ni)$ for some integers $m$ and $n$ with $\gcd(m, n) = 1$, so that there are integers $s$ and $t$ for which $ms + nt = 1$. Now $g$ divides $hm$ and $g$ divides $hn$ (see Exercise 1.2.2), and so $g$ divides $(hm)s + (hn)t = h(ms + nt) = h$. □

**Exercise 1.3.5.** Let $v$ and $w$ be Gaussian integers having ideal forms $g[a : k]$ and $h[b : \ell]$, respectively. Show that $v$ divides $w$ if and only if $v/g$ divides $w/g$, and that these Gaussian integers have ideal forms $[a : k]$ and $\frac{h}{g}[b : \ell]$, respectively. Show that when $g$ divides $h$, then $ag$ divides $bh$ if and only if $a$ divides $b \cdot \frac{h}{g}$, and $h\ell \equiv hk \pmod{ag}$ if and only if $\frac{h}{g} \cdot \ell \equiv \frac{h}{g} \cdot k \pmod{a}$.

Exercise 1.3.5 allows us to restrict our attention to divisibility of a typical Gaussian integer by a *primitive* Gaussian integer, as we will now do.

**Lemma 1.3.4.** *Let* $[a : k]$ *be an ideal form for* $v$*, a primitive Gaussian integer. Then* $v$ *divides* $w = m + ni$ *if and only if* $nk \equiv m \pmod{a}$.

*Proof.* Let $v = q + ri$, and suppose first that $v$ divides $w$ in $\mathbb{Z}[i]$. Then

$$w = m + ni = (q + ri)(s + ti) = (qs - rt) + (qt + rs)i$$

for some rational integers $s$ and $t$. It follows that $a$ divides

$$nk - m = (qt + rs)k - (qs - rt) = s(rk - q) + t(qk + r),$$

since $rk \equiv q \pmod{a}$ by the definition of ideal forms, and $qk \equiv -r \pmod{a}$ by Proposition 1.3.1.

Conversely, suppose that $nk \equiv m \pmod{a}$. With $rk \equiv q \pmod{a}$ by definition, and with $k^2 + 1 \equiv 0 \pmod{a}$ by Proposition 1.3.1, we find that

$$mq + nr \equiv nk \cdot rk + nr \equiv nr(k^2 + 1) \equiv 0 \pmod{a}$$

and

$$nq - mr \equiv nrk - nkr \equiv 0 \pmod{a}.$$

Thus $s = \frac{1}{a}(mq + nr)$ and $t = \frac{1}{a}(nq - mr)$ are integers. Now with $q^2 + r^2 = a$, again by the definition of ideal forms, we calculate that $(q + ri)(s + ti) = m + ni$, and so $v$ divides $w$. We leave this verification to the reader. □

**Example.** The Gaussian integer $1+i$ has ideal form $[2 : 1]$. Lemma 1.3.4 implies that $1 + i$ divides $m + ni$ if and only if $n \cdot 1 \equiv m \pmod{2}$, that is, if and only if $m$ and $n$ have the same parity. ◊

*Proof of Theorem* 1.3.2. Let $v$ and $w$ be Gaussian integers having ideal forms $[a : k]$ and $h[b : \ell]$, respectively. (As noted following Exercise 1.3.5, we can assume that $v$ is primitive.) We can write $w$ as $h(s + ti)$, where $b = s^2 + t^2$ and $t\ell \equiv s \pmod{b}$. Then applying Lemma 1.3.4, it will suffice to show that $htk \equiv hs \pmod{a}$ if and only if $a$ divides $bh$ and $h\ell \equiv hk \pmod{a}$.

Suppose first that $a$ divides $bh$ and $h\ell \equiv hk \pmod{a}$, which implies that $ht\ell \equiv htk \pmod{a}$. Then $t\ell \equiv s \pmod{b}$ implies that $ht\ell \equiv hs \pmod{bh}$, and so $ht\ell \equiv hs \pmod{a}$. We conclude that $htk \equiv hs \pmod{a}$, as we wanted to show.

Conversely, suppose that $htk \equiv hs \pmod{a}$. Notice that then

$$hs^2 = (hs)s \equiv (htk)s \equiv (hs)(tk) \equiv (htk)(tk) \equiv ht^2k^2 \pmod{a}.$$

We then find that $a$ divides $bh$ since

$$bh = (s^2 + t^2)h = hs^2 + ht^2 \equiv ht^2(k^2 + 1) \equiv 0 \pmod{a},$$

using Proposition 1.3.1. With $t\ell \equiv s \pmod{b}$, then $ht\ell \equiv hs \pmod{bh}$, and it follows that $ht\ell \equiv htk \pmod{a}$ since we have established that $a$ divides $bh$. Now $ht\ell \equiv htk \pmod{a}$ implies that $t\ell \equiv tk \pmod{a'}$, where $a' = a/\gcd(a, h)$. (Here we use the congruence cancellation property of Proposition 0.1.6.) We can argue as follows that $a'$ and $t$ can have no prime common divisor. If $p$ divides $a'$, then the exponent of $p$ in $h$ must be strictly smaller than the exponent of $p$ in $a$. Since $a$ divides $bh$, it follows that then $p$ divides $b$. But since $b = s^2 + t^2$ with $\gcd(s, t) = 1$, then $p$ cannot also divide $t$. So Proposition 0.1.6 implies in turn that $\ell \equiv k \pmod{a'}$, and then $h\ell \equiv hk \pmod{a}$ by properties of congruence. This completes our proof. □

We conclude this section with the following important consequence of our divisibility criterion, to which we have already alluded.

**Corollary 1.3.5.** *Gaussian integers $v$ and $w$ can be expressed the same way in ideal form if and only if $v$ and $w$ are associates in $\mathbb{Z}[i]$.*

*Proof.* Suppose that $v$ and $w$ have ideal forms $g[a : k]$ and $h[b : \ell]$. If $g = h$, $a = b$, and $\ell \equiv k \pmod{a}$, then Theorem 1.3.2 shows that $v$ divides $w$ and $w$ divides $v$. Thus $v$ and $w$ are associates by definition. Conversely, suppose that $v$ divides $w$ and $w$ divides $v$. Applying (1.3.1), then $g$ divides $h$ and $h$ divides $g$, which implies that $g = h$ since the divisor of a Gaussian integer is positive. Similarly $ag$ divides $bh$ and $bh$ divides $ag$, which implies in the same way that $a = b$. Finally, with $g = h$, we find that $h\ell \equiv hk \pmod{ag}$ if and only if $\ell \equiv k \pmod{a}$. So $v$ and $w$ have the same ideal form. □

**Exercise 1.3.6.** In each part below, use the criterion of Theorem 1.3.2 to determine whether $v$ divides $w$. (Each $w$ appears in Exercise 1.3.2. An ideal form for each primitive $v$ appears in Table 1.2.)

(a) $v = 3 + 2i$ and $w = 11 + 3i$.

(b) $v = 3 - 2i$ and $w = 11 + 3i$.

(c) $v = 3 + 2i$ and $w = 9 - 7i$.

(d) $v = 3 - 2i$ and $w = 9 - 7i$.

(e) $v = 3 + 2i$ and $w = 13 + 5i$.

(f) $v = 4 + i$ and $w = -11 + 27i$.

(g) $v = 4 - i$ and $w = -11 + 27i$.

(h) $v = 4 - 3i$ and $w = -11 + 27i$.

(i) $v = 4 + 3i$ and $w = -11 + 27i$.

(j) $v = 1 + i$ and $w = 14 + 16i$.

(k) $v = 2 + 2i$ and $w = 14 + 16i$.

(l) $v = 2 - i$ and $w = 141 + 3i$.

(m) $v = 2 + i$ and $w = 141 + 3i$.

(n) $v = 3 + 2i$ and $w = 141 + 3i$.

(o) $v = 3 - 2i$ and $w = 141 + 3i$.

(p) $v = 4 + i$ and $w = 141 + 3i$.

(q) $v = 4 - i$ and $w = 141 + 3i$.

## 1.4 Factorization and Multiplication with Ideal Forms

In §1.3, we saw that an ideal form of a Gaussian integer $v$ represents the equivalence class of all associates of $v$. We noted, from Exercise 1.2.6, that the divisibility relation and multiplication operation are well-defined on this collection of classes. In this section, we develop some methods and formulas that allow us to factor and multiply these ideal form expressions, and so likewise the underlying Gaussian integers, up to unit multiples.

**Irreducible Factorization Using Ideal Forms.** In §1.2, we showed that every nonzero Gaussian integer can be written uniquely, aside from the order of the factors and multiplication by units, as a product of irreducible elements of $\mathbb{Z}[i]$. In this subsection, we will see that, given an ideal form for a Gaussian integer $v$, this factorization is obtained directly from the prime factorization of a corresponding rational integer, namely $N(v)$. If $v$ is irreducible in $\mathbb{Z}[i]$, then each associate of $v$ is also irreducible. So we can refer to an ideal form itself as irreducible, as in the following proposition classifying these elements.

**Proposition 1.4.1.** *Every irreducible Gaussian integer can be expressed in ideal form in one of the following ways.*

(1) *If* $p \equiv 3 \pmod 4$ *is a rational prime, then* $p[1 : 0]$ *is an irreducible ideal form in* $\mathbb{Z}[i]$.

(2) *If* $p \equiv 1 \pmod 4$ *is a rational prime, and* $k^2 + 1 \equiv 0 \pmod p$*, then* $[p : k]$ *and* $[p : -k]$ *are distinct irreducible ideal forms for Gaussian integers. In this case,* $[p : k] \cdot [p : -k] = p[1 : 0]$.

(3) *The ideal form* $[2 : 1]$ *is irreducible, and* $[2 : 1]^2 = 2[1 : 0]$.

*Proof.* We use the classification of irreducible elements in $\mathbb{Z}[i]$ from Corollary 1.2.8.

(1) If $p \equiv 3 \pmod 4$, then $p$ is irreducible in $\mathbb{Z}[i]$. We noted in §1.3 that $p[1 : 0]$ is an ideal form for the rational integer $p$.

(2) If $p \equiv 1 \pmod 4$, then there are unique integers $q > r > 0$ so that $p = q^2+r^2$. In this case, $p = v\overline{v}$, where $v = q+ri$ and $\overline{v} = q-ri$ are irreducible in $\mathbb{Z}[i]$. Since $N(v) = p$ it is possible to express $v$ in ideal form as $[p : k]$ for some integer $k$, and then $\overline{v}$ has ideal form $[p : -k]$. (See Exercise 1.3.1.) Proposition 1.3.1 shows that $k$ and $-k$ satisfy $x^2 + 1 \equiv 0 \pmod p$. The equation $v\overline{v} = p$ can be expressed as $[p : k] \cdot [p : -k] = p[1 : 0]$.

(3) The Gaussian integer $v = 1 + i$ is irreducible, and $(1 + i)(1 - i) = 2$, with $\overline{v} = 1 - i$ an associate of $v$. Here $[2 : 1]$ is an ideal form for both $v$ and $\overline{v}$, so we can express this factorization of 2 as $[2 : 1]^2 = 2[1 : 0]$. □

We can thus factor every rational integer $n$ as a product of ideal forms, if we can solve $x^2 \equiv -1 \pmod p$ for each prime factor $p$ of $n$.

**Example.** Let $n = 147900 = 2^2 \cdot 3 \cdot 5^2 \cdot 17 \cdot 29$. Here 3 is irreducible, while each of the other prime divisors of $n$ factors further in $\mathbb{Z}[i]$. We can express the unique irreducible factorization of $n$ in ideal form as follows:

$$[2 : 1]^4 \cdot 3[1 : 0] \cdot [5 : 2]^2 \cdot [5 : -2]^2 \cdot [17 : 4] \cdot [17 : -4] \cdot [29 : 12] \cdot [29 : -12].$$

For instance, $k = 12$ is a solution of $x^2 \equiv -1 \pmod{29}$, so that $[29 : 12]$ and $[29 : -12]$ are the unique irreducible factors of $29[1 : 0]$. In practice, we will typically write an irreducible factor $p[1 : 0]$ simply as $p$, and regard it as a factor of the *divisor* of an ideal form, that is,

$$n = 3 \cdot [2 : 1]^4 \cdot [5 : 2]^2 \cdot [5 : -2]^2 \cdot [17 : 4] \cdot [17 : -4] \cdot [29 : 12] \cdot [29 : -12].$$

(If we use Table 1.2 to translate these ideal forms into standard expressions for Gaussian integers, their product might equal an associate of $n$, rather than $n$ itself.) ◊

We can factor a primitive Gaussian integer according to the following theorem.

**Theorem 1.4.2.** *Let $v$ be a primitive Gaussian integer having ideal form $[a : k]$. If $a = p_1 \cdot p_2 \cdots p_n$ with each $p_i$ a prime number (not necessarily distinct) in $\mathbb{Z}$, then in $\mathbb{Z}[i]$,*

$$[a : k] = [p_1 : k] \cdot [p_2 : k] \cdots [p_n : k]. \tag{1.4.1}$$

*Proof.* Since $[a : k]$ is an ideal form for a Gaussian integer $v$, then $k$ satisfies the congruence $x^2+1 \equiv 0 \pmod a$. If $p$ is any prime divisor of $a$, then $k$ also satisfies $x^2 + 1 \equiv 0 \pmod p$, so that $[p : k]$ is an ideal form for some irreducible element

$u$ of $\mathbb{Z}[i]$, as in Proposition 1.4.1. Then Theorem 1.3.2 shows that $u$ divides $v$, say with $v = u \cdot w$ for some $w$ in $\mathbb{Z}[i]$. Here $w$ is primitive, and since $a = N(v) = N(u \cdot w) = N(u) \cdot N(w)$, we must have $N(w) = \frac{a}{p}$. So $w$ has ideal form $[\frac{a}{p} : \ell]$ for some integer $\ell$. But since $w$ divides $v$, we also have $\ell \equiv k \pmod{\frac{a}{p}}$, and so we can write $w$ as $[\frac{a}{p} : k]$. Continuing in this way produces the irreducible factorization of $v$ in (1.4.1). □

**Example.** Since $1525^2 + 1$ is divisible by 5858, there might be a Gaussian integer $v$ having ideal form $[5858 : 1525]$. We find that $5858 = 2 \cdot 29 \cdot 101$ in $\mathbb{Z}$, and so assuming that $v$ exists, it must factor as

$$\begin{aligned}[5858 : 1525] &= [2 : 1525] \cdot [29 : 1525] \cdot [101 : 1525] \\ &= [2 : 1] \cdot [29 : -12] \cdot [101 : 10].\end{aligned}$$

(We use the ideal form representatives having minimal character in absolute value in the final expression.) In fact, $[5858 : 1525]$ is an ideal form for $v = 73 - 23i$, since $73^2 + (-23)^2 = 5858$ with $-23 \cdot 1525 \equiv 73 \pmod{5858}$. In §1.2, we found that $73 - 23i = (1-i)(5+2i)(10+i)$ by trial-and-error. It can be verified that these irreducible factors have ideal form $[2 : 1]$, $[29 : -12]$, and $[101 : 10]$, respectively. ◊

**Example.** Let $v = 45 + 60i = 15(3 + 4i)$, which has ideal form $15[25 : 7]$ by direct calculation. Here $15 = 3 \cdot 5$, with 3 irreducible, and with $5[1 : 0] = [5 : 2] \cdot [5 : -2]$. Since $[25 : 7] = [5 : 7] \cdot [5 : 7] = [5 : 2] \cdot [5 : 2]$, the irreducible factorization of $v = 45 + 60i$ in ideal form is $3 \cdot [5 : 2]^3 \cdot [5 : -2]$. ◊

**Exercise 1.4.1.** In each part below, a Gaussian integer $v$ is presented in standard form and ideal form. Find the factorization of each $v$ as a product of irreducible Gaussian integers in ideal form, write each of those factors in standard form using Table 1.2, and verify that the product of those factors equals (an associate of) $v$.

(a) $v = 11 + 3i = [130 : 47]$.

(b) $v = 9 - 7i = [130 : -57]$.

(c) $v = 13 + 5i = [194 : -75]$.

(d) $v = -11 + 27i = [850 : 157]$.

(e) $v = 14 + 22i = 2[170 : 47]$.

(f) $v = 141 + 3i = 3[2210 : 47]$.

**Multiplication of Ideal Forms.** We can also multiply Gaussian integers presented in ideal form, without converting them into standard form. (More precisely, we are multiplying classes of associates of Gaussian integers, a well-defined operation.) In this subsection, we demonstrate that this multiplication follows the same procedures used to solve a quadratic congruence modulo a composite value, as outlined in Theorems 0.3.1 and 0.3.2.

**Lemma 1.4.3.** *Let $v$ and $w$ be primitive Gaussian integers having ideal forms $[a : k]$ and $[b : \ell]$, respectively. Suppose that $vw$ has ideal form $g[c : m]$. Then $g$ is a common divisor of $a$ and $b$.*

*Proof.* If $vw$ can be expressed as $g[c : m]$, then

$$g^2c = N(vw) = N(v) \cdot N(w) = ab.$$

On the other hand, since $v$ and $w$ divide $vw$, Theorem 1.3.2 shows that $a$ and $b$ both divide $gc$. If $gc = as$, then $ab = g^2c = as \cdot g$, so that $b = gs$. Similarly, if $gc = bt$, we find that $a = gt$. So $g$ is a common divisor of $a$ and $b$. □

**Proposition 1.4.4.** *Let $v$ and $w$ be primitive Gaussian integers having ideal forms $[a : k]$ and $[b : \ell]$, respectively. If $\gcd(a, b) = 1$, then $vw$ has ideal form $[ab : m]$, where $m \equiv k \pmod{a}$ and $m \equiv \ell \pmod{b}$.*

*Proof.* Lemma 1.4.3 shows that $vw$ is primitive. With $N(vw) = ab$, then $vw$ has ideal form $[ab : m]$ for some $m$. Theorem 1.3.2 implies that $m \equiv k \pmod{a}$ and $m \equiv \ell \pmod{b}$, since $v$ and $w$ divide $vw$. □

If $\gcd(a, b) = 1$, the Chinese Remainder Theorem implies that there is an integer $m$, unique modulo $ab$, satisfying $m \equiv k \pmod{a}$ and $m \equiv \ell \pmod{b}$. Thus the ideal form of $vw$ is uniquely determined by that pair of congruences.

**Example.** Table 1.2 shows that $v = 5 - 3i$ and $w = 5 + 2i$ have ideal forms $[34 : -13]$ and $[29 : -12]$, respectively. Here $\gcd(34, 29) = 1$ and $34 \cdot 29 = 986$, and $m = 191$ satisfies $m \equiv -13 \pmod{34}$ and $m \equiv -12 \pmod{29}$, using the method of Theorem 0.1.8. So Proposition 1.4.4 implies that $vw$ has ideal form $[986 : 191]$. We can verify this claim directly, noting that

$$(5 - 3i)(5 + 2i) = 31 - 5i,$$

with $31^2 + (-5)^2 = 986$ and $-5 \cdot 191 \equiv 31 \pmod{986}$. ◊

**Proposition 1.4.5.** *Let $v$ be an irreducible Gaussian integer of prime norm $p \equiv 1 \pmod{4}$, written as $[p : k]$ in ideal form. Then for every positive integer $e$, we can write $v^e$ in ideal form as $[p^e : k_e]$, where $k_e \equiv k \pmod{p}$ satisfies $x^2 + 1 \equiv 0 \pmod{p^e}$.*

*Proof.* We proceed by induction on $e$. If $e = 1$, then $\upsilon = q + ri$ can be written as $[p : k]$ for some $k$ by Proposition 1.4.1. Suppose that for some $e \geq 1$, we know that $\upsilon^e = s + ti$ is given by $[p^e : k_e]$, where $k_e \equiv k \pmod{p}$ satisfies $x^2 + 1 \equiv 0 \pmod{p^e}$. Then write $\upsilon^{e+1} = (qs - rt) + (qt + rs)i$ as $g[c : m]$ in ideal form. Lemma 1.4.3 implies that $g$ divides $\gcd(p, p^e) = p$. If $g = p$, then $p$ divides $qt + rs$. This is impossible because $qt + rs \equiv rkt + rkt \equiv 2rtk \pmod{p}$, but we know that $p$ is odd, $p$ does not divide $k$ since $k^2 \equiv -1 \pmod{p}$, and $p$ divides neither $r$ nor $t$ because $rk \equiv q \pmod{p}$ and $tk_e \equiv s \pmod{p^e}$ by the definition of ideal forms, while $q + ri$ and $s + ti$ are primitive. So $\upsilon^{e+1}$ has ideal form $[c : m]$ with $c = N(\upsilon^{e+1}) = p^{e+1}$. Proposition 1.3.1 implies that $m$ satisfies $x^2 + 1 \equiv 0 \pmod{p^{e+1}}$, and since $\upsilon$ divides $\upsilon^{e+1}$, then $m \equiv k \pmod{p}$ by Theorem 1.3.2. The result follows for all $e \geq 1$ by induction. □

When $p \equiv 1 \pmod 4$, so that $x^2 + 1 \equiv 0 \pmod{p}$ has two distinct solutions, $k$ and $-k$, then $x^2 + 1 \equiv 0 \pmod{p^e}$ has precisely two solutions for every $e > 1$, one congruent to $k$ modulo $p$ and one congruent to $-k$ modulo $p$. Thus we can follow the procedure of Theorem 0.3.1, which we illustrate with the following example, to calculate powers of an irreducible Gaussian integer of norm $p$ in ideal form.

**Example.** Let $\upsilon = 3 + 2i$, with ideal form $[13 : -5]$ as in Table 1.2. If $f(x) = x^2 + 1$, then the unique solution of $x^2 + 1 \equiv 0 \pmod{13^2}$ congruent to $-5$ modulo 13 has the form $-5 + 13t$, where $t$ satisfies

$$f'(-5) \cdot t \equiv -\frac{f(-5)}{13} \pmod{13},$$

that is, $-10t \equiv -2 \pmod{13}$. This congruence has $t = -5$ as its unique solution modulo 13, and since $-5 + 13(-5) = -70$, then $\upsilon^2$ has ideal form $[169 : -70]$. Similarly, $-70 + 169(-1) = -239$ is the unique solution of $x^2 + 1 \equiv 0 \pmod{13^3}$ congruent to $-5$ modulo 13, and so $\upsilon^3$ has ideal form $[2197 : -239]$. We can verify that $\upsilon^2 = 5 + 12i$ with $5^2 + 12^2 = 169$ and $12 \cdot -70 \equiv 5 \pmod{169}$, and that $\upsilon^3 = -9 + 46i$ with $(-9)^2 + 46^2 = 2197$ and $46 \cdot -239 \equiv -9 \pmod{2197}$. ◊

We can now calculate any product of ideal forms with a combination of the factorization result of Theorem 1.4.2 and the multiplication methods of Propositions 1.4.1, 1.4.4, and 1.4.5. We illustrate this approach with two examples to conclude this section.

**Example.** Suppose that $\upsilon$ and $w$ are Gaussian integers having ideal forms $[1625 : 307]$ and $[425 : -132]$, respectively. (Since 1625 divides $307^2 + 1$ and 425 divides $(-132)^2 + 1$, it is possible that such elements $\upsilon$ and $w$ exist.) Using Theorem 1.4.2, and simplifying irreducible factors, we have that

$$[1625 : 307] \cdot [425 : -132] = \left([13 : -5] \cdot [5 : 2]^3\right)\left([17 : 4] \cdot [5 : -2]^2\right).$$

Now $[5 : 2] \cdot [5 : -2] = 5[1 : 0]$ by Proposition 1.4.1, so we find that $vw$ has ideal form

$$5^2 \cdot [5 : 2] \cdot [13 : -5] \cdot [17 : 4] = 25[1105 : 242].$$

Here we use two applications of Proposition 1.4.4, since 242 is the unique solution of $x \equiv 2 \pmod 5$, $x \equiv -5 \pmod{13}$, and $x \equiv 4 \pmod{17}$ modulo 1105. ◊

**Example.** Suppose that $v$ and $w$ are Gaussian integers having ideal forms $[1625 : 307]$ and $[425 : 157]$, respectively. Here we find that

$$[1625 : 307] \cdot [425 : 157] = \left([13 : -5] \cdot [5 : 2]^3\right)\left([17 : 4] \cdot [5 : 2]^2\right).$$

Using the procedure of Theorem 0.3.1, we find that $x = -1068$ is the unique solution of $x^2 \equiv -1 \pmod{5^5}$ with $x \equiv 2 \pmod 5$, and so $vw$ has ideal form

$$[3125 : -1068] \cdot [13 : -5] \cdot [17 : 4] = [690625 : 86432],$$

using the Chinese Remainder Theorem. ◊

**Exercise 1.4.2.** For each pair $v$ and $w$ below, use Theorem 1.4.2 and Propositions 1.4.4 and 1.4.5 as needed to write $vw$ in ideal form. Then calculate $vw$ directly, in standard Gaussian integer form, and verify that $vw$ can be expressed in that ideal form.

(a) $v = 3 + 4i = [25 : 7]$ and $w = 1 + 8i = [65 : -8]$.

(b) $v = 3 + 4i = [25 : 7]$ and $w = 8 + i = [65 : 8]$.

(c) $v = 3 + 2i = [13 : -5]$ and $w = 1 + 8i = [65 : -8]$.

(d) $v = 3 + 2i = [13 : -5]$ and $w = 8 + i = [65 : 8]$.

(e) $v = 2 + 5i = [29 : 12]$ and $w = 5 + 4i = [41 : -9]$.

(f) $v = 2 + 5i = [29 : 12]$ and $w = 7 + 3i = [58 : -17]$.

(g) $v = 2 + 5i = [29 : 12]$ and $w = 3 + 7i = [58 : 17]$.

(h) $v = 7 + 4i = [65 : 18]$ and $w = 1 + 8i = [65 : -8]$.

(i) $v = 7 + 4i = [65 : 18]$ and $w = 8 + i = [65 : 8]$.

(j) $v = 7 + 4i = [65 : 18]$ and $w = 6 + 7i = [85 : 13]$.

## 1.5 Reduction of Ideal Forms for Gaussian Integers

In Proposition 1.3.1, we found that if $g[a : k]$ is an ideal form for a Gaussian integer, then $k$ satisfies the congruence $x^2 + 1 \equiv 0 \pmod{a}$, giving us a necessary condition for the existence of an ideal form expression. In this section, we establish that this condition is also sufficient, under the assumption that $a$ is positive, and we develop an algorithm that converts an allowed ideal form into a corresponding Gaussian integer in standard form. The following observation is our starting point.

**Proposition 1.5.1.** *Let $a$ be a positive integer, and let $k$ be an integer for which $a$ divides $k^2 + 1$, say with $k^2 + 1 = ac$. Suppose that $[c : -k]$ is an ideal form for some Gaussian integer $w$. Then $v = \frac{1}{c}(k + i)w$ is a Gaussian integer, and $[a : k]$ is an ideal form for $v$.*

*Proof.* Let $w = s + ti$ be a Gaussian integer with ideal form $[c : -k]$. Then $c = s^2 + t^2$ and $t(-k) \equiv s \pmod{c}$ by definition, and Proposition 1.3.1 implies that $sk \equiv t \pmod{c}$. It follows that

$$v = \frac{1}{c} \cdot (k + i)w = \frac{1}{c} \cdot (k + i)(s + ti) = \frac{ks - t}{c} + \frac{kt + s}{c}i$$

is a Gaussian integer. If $q = \frac{ks-t}{c}$ and $r = \frac{kt+s}{c}$, then

$$q(-t) + rs = \frac{1}{c} \cdot (-kst + t^2 + kst + s^2) = \frac{1}{c} \cdot (s^2 + t^2) = 1,$$

which implies that $\gcd(q, r) = 1$ and $v$ is primitive. Furthermore,

$$q^2 + r^2 = \frac{1}{c^2} \cdot (k^2s^2 - 2kst + t^2 + k^2t^2 + 2kst + s^2) = \frac{1}{c^2} \cdot (k^2 + 1)(s^2 + t^2) = a,$$

since $k^2 + 1 = ac$ and $s^2 + t^2 = c$, and

$$kr - q = \frac{1}{c} \cdot (k^2t + ks - ks + t) = \frac{1}{c} \cdot (k^2 + 1)t = \frac{1}{c} \cdot ac \cdot t = at,$$

implying that $rk \equiv q \pmod{a}$. Therefore, $[a : k]$ is an ideal form for $v = q + ri$ by definition. □

**Example.** In an example in §1.3, we noted that $[109 : 33]$ is potentially an ideal form for some Gaussian integer. In fact, if $a = 109$ and $k = 33$, then $k^2 + 1 = 1090 = ac$ with $c = 10$. Now $[c : -k] = [10 : -33] = [10 : -3]$ is an ideal form for a Gaussian integer, such as $w = 3 - i$ in Table 1.2. Thus

$$v = \frac{1}{c} \cdot (k + i)w = \frac{1}{10} \cdot (33 + i)(3 - i) = \frac{1}{10} \cdot (100 - 30i) = 10 - 3i$$

is a Gaussian integer with ideal form $[109 : 33]$, as we can verify by direct calculation. The same is true for any associate of $v$. ◊

**Exercise 1.5.1.** Use Proposition 1.5.1 to find a Gaussian integer having ideal form $[370 : 43]$.

**Corollary 1.5.2.** *If $a$ and $g$ are positive integers, and $a$ divides $k^2 + 1$ for some integer $k$, then $g[a : k]$ is an ideal form for some Gaussian integer.*

*Proof.* It suffices to establish this statement when $g = 1$. If the claim is not true, we can assume that $a$ is as small as possible so that $a$ divides $k^2 + 1$ for some $k$, but $[a : k]$ is not an ideal form for any Gaussian integer. Here $a > 1$, since we have seen that $[1 : 0]$ is an ideal form for $v = 1$, and $k \equiv 0 \pmod 1$ for all integers $k$. We can also assume that $-\frac{a}{2} < k \le \frac{a}{2}$, since $[a : \ell] = [a : k]$ if $\ell \equiv k \pmod a$.

Now let $k^2 + 1 = ac$ for some integer $c$. Since $|k| \le \frac{a}{2}$ and $a \ge 2$, then

$$ac = k^2 + 1 \le \frac{a^2}{4} + 1 = \frac{a^2 + 4}{4} \le \frac{a^2 + a^2}{4}, \qquad \text{that is,} \qquad c \le \frac{a}{2} < a.$$

But $c$ divides $(-k)^2 + 1 = ac$, so that $[c : -k]$ is an ideal form for some Gaussian integer $w$ by our assumption. Thus $[a : k]$ must also be an ideal form for some Gaussian integer by Proposition 1.5.1, namely $v = \frac{1}{c}(k + i)w$. □

**A Reduction Algorithm for Ideal Forms.** We can repeat the approach of Proposition 1.5.1 to develop an algorithm that converts an ideal form into the standard expression for a Gaussian integer. We describe this *reduction algorithm* for $[a : k]$ in the following theorem.

**Theorem 1.5.3.** *Let $a > 1$ be an integer, and let $k$ be an integer with $|k| \le \frac{a}{2}$ for which $a$ divides $k^2 + 1$. Let $a_0 = a$ and $k_0 = k$, and for $j \ge 0$, let $a_{j+1} = \frac{1}{a_j}(k_j^2 + 1)$ and select $k_{j+1}$ so that $k_{j+1} \equiv -k_j \pmod{a_{j+1}}$ with $k_{j+1}$ minimal in absolute value. Then there is an $n > 0$ so that $a_n = 1$. In that case, $[a : k]$ is an ideal form for a Gaussian integer*

$$v = \frac{1}{a_1} \cdot (k_0 + i) \cdot \frac{1}{a_2} \cdot (k_1 + i) \cdots \frac{1}{a_n} \cdot (k_{n-1} + i). \tag{1.5.1}$$

*Proof.* Since $k_j$ is selected to be minimal in absolute value modulo $a_j$ for every $i$, we can see by the same argument as in the proof of Corollary 1.5.2 that $a_j \ge a_{j+1}$ for all $i \ge 0$, with strict inequality as long as $a_j > 1$. There must be some $n$ for which $a_n = 1$ and $k_n = 0$, since otherwise we obtain an infinite sequence of strictly decreasing positive integers. Let $v_n = 1$, a Gaussian integer with ideal form $[a_n : k_n] = [1 : 0]$.

Now, applying Proposition 1.5.1 repeatedly, we find that $[a_{n-1} : k_{n-1}]$ is an ideal form for the Gaussian integer

$$v_{n-1} = \frac{1}{a_n} \cdot (k_{n-1} + i)v_n = \frac{1}{a_n} \cdot (k_{n-1} + i),$$

and then $[a_{n-2} : k_{n-2}]$ is an ideal form for

$$\upsilon_{n-2} = \frac{1}{a_{n-1}} \cdot (k_{n-2} + i)\upsilon_{n-1} = \frac{1}{a_{n-1}} \cdot (k_{n-2} + i) \cdot \frac{1}{a_n} \cdot (k_{n-1} + i),$$

and so forth, eventually obtaining equation (1.5.1) for $\upsilon_0 = \upsilon$. □

**Example.** Let $a = 2210 = 2 \cdot 5 \cdot 13 \cdot 17$. Here $x^2 + 1 \equiv 0 \pmod{2210}$ has eight solutions, which we obtain by solving $x \equiv 1 \pmod 2$, $x \equiv \pm 2 \pmod 5$, $x \equiv \pm 5 \pmod{13}$, and $x \equiv \pm 4 \pmod{17}$ simultaneously. There are thus eight (associate classes of) Gaussian integers having ideal form $[2210 : k]$. Applying the Chinese Remainder Theorem (Theorem 0.1.8) repeatedly, we find the following possibilities for $k$: $\pm 47$, $\pm 463$, $\pm 837$, and $\pm 863$. If $[a : k]$ is an ideal form for a Gaussian integer $\upsilon$, then $[a : -k]$ is an ideal form for $\overline{\upsilon}$ (Exercise 1.3.1), so we can let $k$ be positive. As a first example, when $k = 47$, we find that $k^2 + 1 = 2210 \cdot 1$, and conclude that $[2210 : 47]$ is an ideal form for $\upsilon = 47 + i$.

For $k = 463$, we find that $k^2 + 1 = 2210 \cdot 97$, with $-463 \equiv 22 \pmod{97}$. Then $22^2 + 1 = 97 \cdot 5$, with $-22 \equiv -2 \pmod 5$, and so forth. The following table summarizes these calculations.

| $j$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| $a$ | 2210 | 97 | 5 | 1 |
| $k$ | 463 | 22 | $-2$ | 0 |

Theorem 1.5.3 implies that $[2210 : 463]$ is an ideal form for

$$\upsilon = \frac{1}{97} \cdot (463 + i) \cdot \frac{1}{5} \cdot (22 + i) \cdot \frac{1}{1} \cdot (-2 + i) = \frac{1}{97} \cdot (463 + i) \cdot (-9 + 4i) = -43 + 19i.$$

(Note that by calculating these products from the right, we can cancel the fractions as we go along.)

For $k = 837$, we find that $k^2 + 1 = 2210 \cdot 317$ and $-837 \equiv 114 \pmod{317}$, and continue the calculations in the following table.

| $j$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| $a$ | 2210 | 317 | 41 | 2 | 1 |
| $k$ | 837 | 114 | 9 | 1 | 0 |

Here we find that $[2210 : 837]$ is an ideal form for

$$\begin{aligned}\upsilon &= \frac{1}{317} \cdot (837 + i) \cdot \frac{1}{41} \cdot (114 + i) \cdot \frac{1}{2} \cdot (9 + i) \cdot (1 + i) \\ &= \frac{1}{317} \cdot (837 + i) \cdot \frac{1}{41} \cdot (114 + i) \cdot (4 + 5i) = \frac{1}{317} \cdot (837 + i) \cdot (11 + 14i) = 29 + 37i.\end{aligned}$$

Finally for $k = 863$, we obtain the following table by applying the reduction algorithm.

| $j$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| $a$ | 2210 | 337 | 65 | 5 | 1 |
| $k$ | 863 | 148 | $-18$ | $-2$ | 0 |

Here $[2210 : 863]$ is an ideal form for

$$\upsilon = \frac{1}{337} \cdot (863+i) \cdot \frac{1}{65} \cdot (148+i) \cdot \frac{1}{5} \cdot (-18+i) \cdot (-2+i)$$
$$= \frac{1}{337} \cdot (863+i) \cdot \frac{1}{65} \cdot (148+i) \cdot (7-4i) = \frac{1}{337} \cdot (863+i) \cdot (16-9i) = 41-23i.$$

Using the factorization method of Theorem 1.4.2, we have:

$$\begin{aligned} [2210 : 47] &= [2 : 1] \cdot [5 : 2] \cdot [13 : -5] \cdot [17 : -4], \\ [2210 : 463] &= [2 : 1] \cdot [5 : -2] \cdot [13 : -5] \cdot [17 : 4], \\ [2210 : 837] &= [2 : 1] \cdot [5 : 2] \cdot [13 : 5] \cdot [17 : 4], \\ [2210 : 863] &= [2 : 1] \cdot [5 : -2] \cdot [13 : 5] \cdot [17 : -4]. \end{aligned}$$

These expressions correspond to the following irreducible factorizations of the Gaussian integers constructed in this example:

$$\begin{aligned} 47+i &\sim (1+i)(2+i)(3+2i)(4-i), \\ -43+19i &\sim (1+i)(2-i)(3+2i)(4+i), \\ 29+37i &\sim (1+i)(2+i)(3-2i)(4+i), \\ 41-23i &\sim (1+i)(2-i)(3-2i)(4-i). \end{aligned}$$

(Here we use Table 1.2, and write $\upsilon \sim w$ to mean that $\upsilon$ is an associate of $w$ in $\mathbb{Z}[i]$. We leave the verification of these claims to the reader.) ♢

**Exercise 1.5.2.** Use the algorithm of Theorem 1.5.3 to find a Gaussian integer $\upsilon$ having the given ideal form.

(a) $[97 : 22]$.

(b) $[145 : 17]$.

(c) $[205 : 32]$.

(d) $[205 : 73]$.

(e) $[377 : 70]$.

(f) $[377 : 99]$.

(g) $[425 : 132]$.

(h) $[425 : 157]$.

(i) $[493 : 157]$.

(j) $[493 : 191]$.

**Exercise 1.5.3.** Find all ideal forms $[290 : k]$ of Gaussian integers. (That is, find all solutions $k$ of $x^2 + 1 \equiv 0 \pmod{290}$.) For each one, use the algorithm of Theorem 1.5.3 to find a Gaussian integer $\upsilon$ having that ideal form.

**Exercise 1.5.4.** Find all ideal forms of Gaussian integers having norm $1625 = 5^3 \cdot 13$. (Note that these can have the form $[1625 : k]$ or $5[65 : k]$.) For each one, find a Gaussian integer $v$ having that ideal form.

## 1.6 Sums of Two Squares Revisited

We conclude Chapter 1 by returning to the topic of sums of two squares. In particular, we answer a question with which we began: In how many different ways can an integer be expressed as a sum of two squares? The following theorem connects proper representations of integers to ideal forms for Gaussian integers, and thus to solutions of a particular quadratic congruence, which we are able to count.

**Theorem 1.6.1.** *Let $a$ be a positive integer. Then there is a one-to-one correspondence between integers $\frac{a}{2} \geq k \geq 0$ for which $k^2 + 1 \equiv 0 \pmod{a}$ and solutions $q^2 + r^2 = a$ with $q \geq r \geq 0$ and $\gcd(q, r) = 1$.*

*Proof.* Let $k$ be a solution of $x^2 + 1 \equiv 0 \pmod{a}$ for which $\frac{a}{2} \geq k \geq 0$. Theorem 1.5.3 implies that $[a : k]$ is an ideal form for a primitive Gaussian integer $v$, and then $[a : -k]$ is an ideal form for $\overline{v}$. Among the associates of $v$ and of $\overline{v}$, there is precisely one element $q + ri$ with $q \geq r \geq 0$, and then $N(v) = N(\overline{v}) = q^2 + r^2 = a$. Since Corollary 1.3.5 shows that Gaussian integers have the same ideal form if and only if they are associates, the mapping that sends $k$ to the pair $(q, r)$ is well-defined and injective. On the other hand, if $(q, r)$ is an ordered pair for which $q^2 + r^2 = a$, with $q \geq r \geq 0$ and $\gcd(q, r) = 1$, then $rx \equiv q \pmod{a}$ has a solution $k$, which also satisfies $x^2 + 1 \equiv 0 \pmod{a}$ by Proposition 1.3.1. Since $-k$ is also a solution of the quadratic congruence, we can assume that $\frac{a}{2} \geq k \geq 0$. So our mapping is also surjective. □

**Example.** Suppose we find that $k = 82$ satisfies $x^2 + 1 \equiv 0 \pmod{a}$, where $a = 269$. We can apply the reduction algorithm of Theorem 1.5.3 to construct a solution of $x^2 + y^2 = 269$. Here $82^2 + 1 = 6725 = 269 \cdot 25$, so we can let $v = \frac{1}{25} \cdot (82 + i)w$, where $w$ is a Gaussian integer with ideal form $[25 : -82] = [25 : -7]$. Continuing in this way to find a similar expression for $w$, we are led to the equation

$$v = \frac{1}{25} \cdot (82 + i) \cdot \frac{1}{2} \cdot (-7 + i) \cdot \frac{1}{1} \cdot (1 + i) = \frac{1}{25} \cdot (82 + i) \cdot (-4 - 3i) = -13 - 10i.$$

Among the associates of $v$ and $\overline{v}$ is $13 + 10i$, and so $269 = 13^2 + 10^2$. ◊

**Exercise 1.6.1.** Verify that $k = 353$ satisfies $x^2 + 1 \equiv 0 \pmod{733}$, and use that fact to find an expression for 733 as a sum of two squares.

**Exercise 1.6.2.** Verify that $k = 133$ and $k = 621$ are both solutions of $x^2 + 1 \equiv 0 \pmod{1769}$. Use those values to find two expressions for 1769 as sums of two squares.

The reader might recognize a similarity between these examples and those in §1.1 in which we used a solution of $x^2+1 \equiv 0 \pmod{p}$ to construct an expression for $p$ as $q^2+r^2$. It should again be acknowledged that trial-and-error is generally a quicker and easier approach to finding solutions of $x^2 + y^2 = a$ in practice, when they are known to exist. Theorem 1.6.1 does, however, provide the following formula for the number of proper representations of an integer $a$ by $x^2 + y^2$.

**Theorem 1.6.2.** *Let $a$ be a positive integer written as*

$$a = 2^e \cdot p_1^{e_1} \cdot p_2^{e_2} \cdots p_n^{e_n}, \tag{1.6.1}$$

*where $e = 0$ or 1, each $p_i$ is a distinct prime congruent to 1 modulo 4, and each $e_i$ is positive. Then the number of proper representations of $a$ as $x^2 + y^2$ with $x \geq y \geq 0$ is $2^{n-1}$ if $n$ is positive, and is 1 if $n = 0$. If $a$ cannot be written in this form, then there are no proper representations of $a$ by $x^2 + y^2$.*

*Proof.* If $a$ is given by equation (1.6.1), then $x^2 + 1 \equiv 0 \pmod{a}$ has $2^n$ distinct solutions. (See Theorem 0.3.4 and Corollary 0.3.3.) If we assume that $0 \leq k \leq \frac{a}{2}$, then $k \equiv -k \pmod{a}$ only when $k = 0$ or $k = \frac{a}{2}$. But $k = 0$ satisfies $x^2 \equiv -1 \pmod{a}$ if and only if $a = 1$, while $k = \frac{a}{2}$ is a solution if and only if $a = 2$. So if $a$ has $n$ prime divisors $p \equiv 1 \pmod{4}$ as in (1.6.1), then $x^2 \equiv -1 \pmod{a}$ has only one solution if $n = 0$ (so that $a = 1$ or $a = 2$), but $2^{n-1}$ distinct pairs of solutions $k$ and $-k$ if $n > 0$. □

In practice, when $a$ has more than one prime divisor $p \equiv 1 \pmod{4}$, we can also apply unique factorization in $\mathbb{Z}[i]$ to construct proper representations, or more general representations, of $a$ by $x^2 + y^2$. Every rational integer $a$ is also a Gaussian integer, so can be expressed uniquely as a product of irreducible elements of $\mathbb{Z}[i]$. If $a = N(\upsilon) = \upsilon\overline{\upsilon}$ for some $\upsilon = q + ri$ in $\mathbb{Z}[i]$, then the irreducible factors of $a$ must appear in the factorizations of $\upsilon$ and $\overline{\upsilon}$. But by properties of conjugates, we also have that if $\upsilon = \upsilon_1 \cdot \upsilon_2 \cdots \upsilon_n$, then $\overline{\upsilon} = \overline{\upsilon_1} \cdot \overline{\upsilon_2} \cdots \overline{\upsilon_n}$. So there are restrictions on how the irreducible elements in $a$ can be divided between $\upsilon$ and $\overline{\upsilon}$ that help us describe the ways of writing $n$ as a sum of two squares.

**Example.** The irreducible factorization of $a = 10414625 = 5^3 \cdot 13^2 \cdot 17 \cdot 29$ in $\mathbb{Z}[i]$ is

$$a = (2+i)^3 \cdot (2-i)^3 \cdot (3+2i)^2 \cdot (3-2i)^2 \cdot (4+i) \cdot (4-i) \cdot (5+2i) \cdot (5-2i).$$

If we write $a = \upsilon\overline{\upsilon} = (q+ri)(q-ri)$ with $\gcd(q, r) = 1$, then $\upsilon$ cannot be divisible by both $2 + i$ and $2 - i$ or by both $3 + 2i$ and $3 - 2i$. We can assume, by relabeling

$v$ and $\overline{v}$ if necessary, that $(2+i)^3$ divides $v$. Then we have eight possibilities for $v$ and so for solutions $q^2+r^2=a$ with $\gcd(q,r)=1$ and $q \geq r \geq 0$. For example, the factorization

$$(2+i)^3 \cdot (3+2i)^2 \cdot (4+i) \cdot (5+2i) = -3223 - 164i$$

provides the proper solution $(x,y)=(3223,164)$ of $x^2+y^2=a$. Similarly,

$$(2+i)^3 \cdot (3+2i)^2 \cdot (4+i) \cdot (5-2i) = -2447 + 2104i$$

yields the solution $(x,y)=(2447,1204)$. ◊

**Exercise 1.6.3.** Find the remaining proper representations of $a = 10414625$ by $x^2+y^2$.

**Exercise 1.6.4.** Find all proper representations of each of the following integers by $x^2+y^2$.

(a) $a = 305 = 5 \cdot 61$.

(b) $a = 493 = 17 \cdot 29$.

(c) $a = 754 = 2 \cdot 13 \cdot 29$.

(d) $a = 1885 = 5 \cdot 13 \cdot 29$.

(e) $a = 1898 = 2 \cdot 13 \cdot 73$.

(f) $a = 7565 = 5 \cdot 17 \cdot 89$.

(g) $a = 15170 = 2 \cdot 5 \cdot 37 \cdot 41$.

The *total* number of representations of $a$ by $x^2+y^2$ with $x \geq y \geq 0$ is the sum of the number of *proper* representations of $\frac{a}{g^2}$, as $g^2$ varies over all square divisors of $a$. (If $\frac{a}{g^2} = q^2+r^2$, then $a = (gq)^2+(gr)^2$.) We can also calculate the number of representations of $a$ by $x^2+y^2$ using irreducible factorization of $a$, obtaining the following general formula.

**Theorem 1.6.3.** *Let $a$ be a positive integer written as*

$$a = 2^e \cdot p_1^{e_1} \cdots p_n^{e_n} \cdot q_1^{f_1} \cdots q_\ell^{f_\ell}, \tag{1.6.2}$$

*where each $p_i$ and $q_j$ is a distinct prime with $p_i \equiv 1 \pmod 4$ and $q_j \equiv 3 \pmod 4$, each $e_i$ and $f_i$ is a positive integer, and $e \geq 0$. Let $m = (e_1+1)(e_2+1)\cdots(e_n+1)$ if $n$ is positive and let $m=1$ if $n=0$. If each $f_i$ is even, then the number of representations of $a$ by $x^2+y^2$ with $x \geq y \geq 0$ is $\left\lfloor \frac{m+1}{2} \right\rfloor$. If instead any $f_i$ is odd, then $a$ has no representations by $x^2+y^2$.*

Here $\left\lfloor \frac{m+1}{2} \right\rfloor$ is the largest integer less than or equal to $\frac{m+1}{2}$, an example of the *floor* function.

*Proof.* Using ideal form, we can write $2 = 2[1 : 0] = [2 : 1]^2$, and each $p_i$ in equation (1.6.2) as $[p_i : k_i] \cdot [p_i : -k_i]$ for some $k_i$. Each $q_i$, on the other hand, is irreducible in $\mathbb{Z}[i]$. So the unique irreducible factorization of $a = a[1 : 0]$ is as follows:

$$a = q_1^{f_1} \cdots q_\ell^{f_\ell} \cdot [2 : 1]^{2e} \cdot [p_1 : k_1]^{e_1} \cdot [p_1 : -k_1]^{e_1} \cdots [p_n : k_n]^{e_n} \cdot [p_n : -k_n]^{e_n}.$$

We would like to count the number of distinct ways of writing $a$ as a product of a Gaussian integer and its conjugate, $\upsilon \cdot \overline{\upsilon}$. Since $\overline{q_i} = q_i$, there are no such products if any $f_i$ is odd. So we will assume that each $f_i$ is even, and to simplify notation write $q_1^{f_1} \cdots q_\ell^{f_\ell}$ as $q^2$. Each possibility for $\upsilon$ is

$$\upsilon = q \cdot [2 : 1]^e \cdot [p_1 : k_1]^{t_1} \cdot [p_1 : -k_1]^{e_1 - t_1} \cdots [p_n : k_n]^{t_n} \cdot [p_n : -k_n]^{e_n - t_n},$$

where $0 \le t_i \le e_i$ for $1 \le i \le n$. Note that $m = (e_1 + 1)(e_2 + 1) \cdots (e_n + 1)$ is the total number of possibilities for these values of $t_i$. If any $e_i$ is odd, so that $m$ is even, we find that each $\upsilon$ is the same as some $\overline{\upsilon}$ for a different selection of $t_i$ values (namely, when $t_i$ is replaced by $e_i - t_i$ for $1 \le i \le n$), and so the number of distinct possibilities for $\upsilon$ is $\frac{m}{2}$. On the other hand, if each $e_i$ is even, we find that $\upsilon = \overline{\upsilon}$ when $t_i = \frac{e_i}{2}$ for all $i$. In this case, $m$ is odd, and there are $\frac{m+1}{2}$ distinct possibilities for $\upsilon$. The number of distinct representations of $a$ by $x^2 + y^2$ can be written as $\left\lfloor \frac{m+1}{2} \right\rfloor$ in both cases. □

**Example.** We illustrate the argument above with $a = 4225 = 5^2 \cdot 13^2$. The irreducible factorization of $a$ in $\mathbb{Z}[i]$ is

$$4225 = [5 : 2]^2 \cdot [5 : -2]^2 \cdot [13 : 5]^2 \cdot [13 : -5]^2 = (2+i)^2 \cdot (2-i)^2 \cdot (3-2i)^2 \cdot (3+2i)^2.$$

There are $m = (2 + 1)(2 + 1) = 9$ choices we can make for $\upsilon$ so that $a = \upsilon \cdot \overline{\upsilon}$, which we present in standard form in the table below.

| Factorization of $\upsilon$ | $\upsilon$ |
|---|---|
| $(2 + i)^2 \cdot (3 - 2i)^2$ | $63 - 16i$ |
| $(2 + i)^2 \cdot (3 - 2i) \cdot (3 + 2i)$ | $39 + 52i$ |
| $(2 + i)^2 \cdot (3 + 2i)^2$ | $-33 + 56i$ |
| $(2 + i) \cdot (2 - i) \cdot (3 - 2i)^2$ | $25 - 60i$ |
| $(2 + i) \cdot (2 - i) \cdot (3 - 2i) \cdot (3 + 2i)$ | $65 + 0i$ |
| $(2 + i) \cdot (2 - i) \cdot (3 + 2i)^2$ | $25 + 60i$ |
| $(2 - i)^2 \cdot (3 - 2i)^2$ | $-33 - 56i$ |
| $(2 - i)^2 \cdot (3 - 2i) \cdot (3 + 2i)$ | $39 - 52i$ |
| $(2 - i)^2 \cdot (3 + 2i)^2$ | $63 + 16i$ |

As we see, for each choice except one, there is another that gives us essentially the same solution. So there are $\left\lfloor \frac{m+1}{2} \right\rfloor = 5$ distinct representations of $a$ by $x^2+y^2$ with $x \geq y \geq 0$:

$$63^2 + 16^2, \qquad 52^2 + 39^2, \qquad 56^2 + 33^2, \qquad 60^2 + 25^2, \qquad 65^2 + 0^2.$$

As Theorem 1.6.1 claims, only $2^{2-1} = 2$ of these representations are proper. ◊

**Exercise 1.6.5.** Find all representations (proper or improper) of each of the following integers by $x^2+y^2$. Verify in each case that the formulas of Theorems 1.6.2 and 1.6.3 for the number of representations are correct.

(a) $a = 3250 = 2 \cdot 5^3 \cdot 13$.

(b) $a = 3825 = 3^2 \cdot 5^2 \cdot 17$.

(c) $a = 12025 = 5^2 \cdot 13 \cdot 37$.

(d) $a = 357773 = 13^2 \cdot 29 \cdot 73$.

(e) $a = 359125 = 5^3 \cdot 13^2 \cdot 17$.

(f) $a = 585000 = 2^3 \cdot 3^2 \cdot 5^4 \cdot 13$.

(g) $a = 903125 = 5^5 \cdot 17^2$.

**Exercise 1.6.6.** Find all representations of $a = 10414625$ by $x^2+y^2$. (The proper representations of $a$ by $x^2 + y^2$ were obtained in Exercise 1.6.3.)

## Gaussian Integers and Sums of Two Squares—Review

In this chapter, we introduced a key theme of this text—questions that are phrased purely in terms of integers might be answered more directly by appealing to a larger set of numbers, one with some properties in common with the set of integers. In particular, we saw that the problem of determining which integers can be expressed as a sum of two squares, and in how many ways, can be naturally approached in terms of factorization in the set of *Gaussian integers*, $\mathbb{Z}[i]$. We saw that $\mathbb{Z}[i]$ has properties of divisibility and irreducible factorization analogous to those in $\mathbb{Z}$ itself. In particular, we established the crucial result that irreducible factorization of Gaussian integers is unique, similarly to prime factorization of integers. Using this fact, we classified all irreducible elements in $\mathbb{Z}[i]$, and found that the number of representations of a rational integer $a$ as $x^2 + y^2$ is essentially the number of ways of arranging factors in the unique irreducible factorization of $a$ in $\mathbb{Z}[i]$.

In Chapter 1, we also introduced a notational device that we will find recurring, in different settings and with variations, throughout the text. We summarize key aspects of this notation as follows.

(1) If $v = g(q + ri)$ is a Gaussian integer with $\gcd(q, r) = 1$, we also express $v$ in *ideal form* as $g[a : k]$, where $a = q^2 + r^2$ and $k$ satisfies the linear congruence $rk \equiv q \pmod{a}$.

(2) If $g[a : k]$ is an ideal form for some Gaussian integer, then $k$ satisfies the quadratic congruence $x^2 + 1 \equiv 0 \pmod{a}$ (Proposition 1.3.1).

(3) There is a simple criterion for divisibility of one Gaussian integer by another using ideal forms (Theorem 1.3.2).

(4) Irreducible Gaussian integers can be classified in ideal form in terms of solutions of $x^2 + 1 \equiv 0 \pmod{p}$, where $p$ is prime (Proposition 1.4.1).

(5) Irreducible factorization of a Gaussian integer $v = g[a : k]$ in ideal form depends in a very straightforward way on the prime factorizations of $g$ and $a$ in $\mathbb{Z}$ (Theorem 1.4.2).

(6) Multiplication of Gaussian integers given in ideal form follows the same techniques used for solving quadratic congruences modulo composite values (Propositions 1.4.4 and 1.4.5).

(7) There is an algorithm for converting $g[a : k]$ into standard form for a Gaussian integer that holds in all cases where $a$ is a positive integer and $k$ satisfies $x^2 + 1 \equiv 0 \pmod{a}$ (Theorem 1.5.3).

In Chapter 2, we generalize the Gaussian integers to infinitely many other sets, which we call *quadratic domains*. We will see that the definition of ideal forms extends in a similar way to all such examples, with analogous conclusions about factorization and multiplication. But we will find that a key property of Gaussian integers, *uniqueness* of irreducible factorization, does not hold in all such cases. The adjustments necessary to compensate for this fact lead to the most important concepts of quadratic number theory.

# 2

# Quadratic Domains

In Chapter 1, we found that questions about which integers are sums of two squares can be approached in a direct way as applications of factorization in the set of Gaussian integers. We now broaden our viewpoint to the following more general question. Let $a$, $b$, and $c$ be integers, and consider the function of two variables $f(x, y) = ax^2 + bxy + cy^2$. Which values of $m$ can be expressed as $f(q, r)$ for some integers $q$ and $r$, particularly with $\gcd(q, r) = 1$?

Based on our approach to sums of two squares, it might again be natural to approach this problem in terms of factorization within sets containing other types of real or complex numbers. For instance, if $f(x, y) = x^2 + xy - y^2$, then direct calculation shows that

$$f(q, r) = \left(\left(q + \tfrac{1}{2}r\right) + \tfrac{\sqrt{5}}{2}r\right)\left(\left(q + \tfrac{1}{2}r\right) - \tfrac{\sqrt{5}}{2}r\right),$$

so we might be led to consider numbers such as this. In this chapter, we make a precise definition of the type of numbers that arise in this way, and so introduce domains of quadratic integers (or *quadratic domains*), our main setting for the study of quadratic number theory. We will see that many of the concepts that we found useful with Gaussian integers carry over to more general quadratic domains. In particular, we will generalize the notation of ideal forms to arbitrary quadratic integers, and will again find that this allows some computational methods for multiplication and factorization with these types of numbers. However, we will find that a key property of $\mathbb{Z}[i]$, unique irreducible factorization, is the exception, rather than the rule, in quadratic domains. While this fact makes the immediate generalization of results about sums of two squares unclear, we will also introduce, through the terminology of *ideal numbers*, a way in which a type

of unique irreducible factorization can be recaptured in every quadratic domain. (We regard some concepts in this chapter as motivation for more precise definitions that we introduce in Chapter 3 and beyond.)

## 2.1 Quadratic Numbers and Quadratic Integers

A complex number $v$ is *rational* if and only if $f(v) = 0$ for some nonzero linear polynomial $f(x) = ax + b$ with coefficients in $\mathbb{Z}$. In this case, $v$ is an *integer* if the leading coefficient of this polynomial is $a = 1$. We define our numbers of main interest by extending this rather trivial observation to the next simplest type of polynomial.

**Definition.** A complex number $v$ is called a *quadratic number* if $f(v) = 0$ for some polynomial $f(x) = ax^2 + bx + c$ with $a$, $b$, and $c$ integers and $a \neq 0$. If we further assume that $f(x)$ is *monic*, that is, $a = 1$, then we say that $v$ is a *quadratic integer*.

**Example.** The real number $\sqrt{2}$ is a quadratic integer, since it is a root of $f(x) = x^2 - 2$. ◊

**Example.** If $f(x) = 3x^2 - 5x + 4$, then its roots, $v = \frac{5+\sqrt{-23}}{6}$ and $w = \frac{5-\sqrt{-23}}{6}$, are quadratic numbers. (We could also write $\sqrt{-23}$ as $i\sqrt{23}$, but for the numbers defined here, we will most often simply write $\sqrt{d}$, whether $d$ is positive or negative.) ◊

More generally, a complex number $v$ is called an *algebraic number* if $f(v) = 0$ for some nonzero polynomial $f(x)$ having integer coefficients with no restriction on the degree of $f(x)$, and an *algebraic integer* if we can take $f(x)$ to be monic. *Algebraic number theory* might be viewed as the study of these types of numbers. In this book, we restrict our attention to the simplest type of algebraic numbers (beyond rational numbers themselves), where we can develop some particularly useful computational methods.

**Proposition 2.1.1.** *If $r$ is a rational number, then $r$ is a quadratic number. In this case, $r$ is a quadratic integer if and only if $r$ is an integer in the usual sense.*

*Proof.* We can write a rational number as $r = m/n$ with $m$ and $n$ relatively prime integers and $n > 0$. Then $f(x) = nx^2 - mx$ is a polynomial with integer coefficients for which $f(r) = 0$. Suppose we also have $g(r) = 0$ for some monic polynomial $g(x) = x^2 + bx + c$ with $b$ and $c$ in $\mathbb{Z}$. Then $m^2 = -bmn - cn^2$, and any prime divisor of $n$ must also divide $m^2$, and thus divide $m$. If $\gcd(m, n) = 1$, then $n = 1$, and so $r = m$ is an integer. □

As we did when working with Gaussian integers, we often refer to elements of $\mathbb{Z}$ as *rational integers*. Proposition 2.1.1 states that these are precisely the "integers" among rational numbers. Recall that the *discriminant* of a polynomial $f(x) = ax^2 + bx + c$ is $\Delta = b^2 - 4ac$. If $a \neq 0$, then there are two complex roots of $f(x)$,

$$\upsilon = \frac{-b + \sqrt{\Delta}}{2a} \qquad \text{and} \qquad \overline{\upsilon} = \frac{-b - \sqrt{\Delta}}{2a},$$

as can be verified by direct calculation, or derived via the process of completing the square. Note that $\upsilon$ and $\overline{\upsilon}$ are real numbers if $\Delta \geq 0$, are rational numbers if $\Delta$ is the square of an integer, and are equal if $\Delta = 0$. With this formula in mind, we can classify all quadratic numbers as follows.

**Proposition 2.1.2.** *A complex number $\upsilon$ is a quadratic number if and only if there are rational numbers $q$ and $r$ and a squarefree integer $d \neq 1$ such that $\upsilon = q + r\sqrt{d}$.*

Recall that an integer $d$ is *squarefree* if it is not divisible by the square of an integer larger than 1.

*Proof.* Suppose that $\upsilon$ is a quadratic number, say with $f(\upsilon) = 0$ for some $f(x) = ax^2 + bx + c$ having integer coefficients, $a \neq 0$. If $\Delta = b^2 - 4ac = t^2$ for some integer $t$, then $\upsilon = \frac{-b \pm t}{2a} = q$ is rational, and we can write $\upsilon = q + 0\sqrt{d}$ for any squarefree $d \neq 1$. Otherwise, let $t^2$ be the largest square dividing $\Delta$, so that $\Delta = t^2 d$ with $d \neq 1$ squarefree. Then $\upsilon = q + r\sqrt{d}$ with $q = \frac{-b}{2a}$ and $r = \pm\frac{t}{2a}$ rational numbers.

Conversely, suppose that $\upsilon = q + r\sqrt{d}$, where $q$ and $r$ are rational and $d \neq 1$ is a squarefree integer. Let $\overline{\upsilon} = q - r\sqrt{d}$. Then $\upsilon$ is a root of

$$f(x) = (x - \upsilon)(x - \overline{\upsilon}) = x^2 - (\upsilon + \overline{\upsilon})x + \upsilon\overline{\upsilon} = x^2 - 2qx + (q^2 - r^2 d), \quad (2.1.1)$$

a polynomial with rational coefficients. If we write $q = \frac{m}{s}$ and $r = \frac{n}{s}$ for some integers $m$, $n$, and $s$, then $g(\upsilon) = 0$, where

$$g(x) = s^2 x^2 - 2msx + (m^2 - n^2 d)$$

has integer coefficients. Thus $\upsilon$ is a quadratic number by definition. □

**Definition.** If $d \neq 1$ is a fixed squarefree integer, let

$$\mathbb{Q}(\sqrt{d}) = \{q + r\sqrt{d} \mid q, r \in \mathbb{Q}\}.$$

We refer to $\mathbb{Q}(\sqrt{d})$ as a *quadratic field*. If $\upsilon = q + r\sqrt{d}$ is in $\mathbb{Q}(\sqrt{d})$, we call $\overline{\upsilon} = q - r\sqrt{d}$ the *conjugate* of $\upsilon$, and define the *norm* of $\upsilon$ to be $N(\upsilon) = \upsilon\overline{\upsilon}$.

**Exercise 2.1.1.** Let $v$ and $w$ be elements of a quadratic field $\mathbb{Q}(\sqrt{d})$.

(a) Show that $\overline{v+w} = \overline{v} + \overline{w}$.

(b) Show that $\overline{vw} = \overline{v} \cdot \overline{w}$.

(c) Show that $N(vw) = N(v) \cdot N(w)$.

(d) Show that $N(v) = 0$ if and only if $v = 0$ in $\mathbb{Q}(\sqrt{d})$.

The following exercise verifies that a quadratic field $\mathbb{Q}(\sqrt{d})$ has all the algebraic properties of a *field*, specifically a subfield of the complex numbers. See Appendix C for more details on this terminology.

**Exercise 2.1.2.** Let $\mathbb{Q}(\sqrt{d}) = \{q + r\sqrt{d} \mid q, r \in \mathbb{Q}\}$, where $d$ is a squarefree integer.

(a) Show that $\mathbb{Q}(\sqrt{d})$ is closed under addition and subtraction, and contains 0.

(b) Show that $\mathbb{Q}(\sqrt{d})$ is closed under multiplication, and contains 1.

(c) Show that if $v \neq 0$ in $\mathbb{Q}(\sqrt{d})$, then $v$ has an inverse in $\mathbb{Q}(\sqrt{d})$ under multiplication. (Hint: Use parts (c) and (d) of Exercise 2.1.1.)

**Classification of Quadratic Integers.** We can characterize the subset of integers in an arbitrary quadratic field using the following statement.

**Proposition 2.1.3.** *Let $v$ be an element of $\mathbb{Q}(\sqrt{d})$ for some squarefree $d \neq 1$, and let $\overline{v}$ be its conjugate. Then $v$ is a quadratic integer if and only if $v + \overline{v}$ and $v\overline{v}$ are rational integers.*

*Proof.* We saw in equation (2.1.1) that $v$ is a root of the polynomial $f(x) = x^2 - (v + \overline{v})x + v\overline{v}$. If $v + \overline{v}$ and $v\overline{v}$ are rational integers, then $f(x)$ is a monic polynomial with integer coefficients, and $v$ is a quadratic integer by definition. Conversely, suppose that $v$ is a quadratic integer, say with $g(v) = 0$ for some $g(x) = x^2 + bx + c$ with $b$ and $c$ in $\mathbb{Z}$. If $v$ is a rational number, then $v$ is an integer by Proposition 2.1.1. In this case, $\overline{v} = v$, and so $v + \overline{v}$ and $v\overline{v}$ are both integers. So assume that $v$ is not a rational number. Now since $v$ is a root of both $f(x)$ and $g(x)$, we find that $bv + c = -v^2 = -(v + \overline{v})v + v\overline{v}$. It follows that $v + \overline{v} = -b$ and $v\overline{v} = c$ must both be integers, since otherwise we could solve for $v$ as a rational number, contrary to assumption. □

**Corollary 2.1.4.** *Let $v = q + r\sqrt{d}$ be an element of $\mathbb{Q}(\sqrt{d})$ for some squarefree $d \neq 1$.*

(1) *If* $d \equiv 2$ *or* $3 \pmod 4$*, then* $\upsilon$ *is a quadratic integer if and only if* $q$ *and* $r$ *are integers.*
(2) *If* $d \equiv 1 \pmod 4$*, then* $\upsilon$ *is a quadratic integer if and only if* $q = \frac{m}{2}$ *and* $r = \frac{n}{2}$ *for integers* $m$ *and* $n$ *with* $m \equiv n \pmod 2$*.*

*Proof.* Suppose that $\upsilon = q + r\sqrt{d}$ is a quadratic integer. Proposition 2.1.3 then implies that $\upsilon + \overline{\upsilon} = 2q = m$ and $\upsilon\overline{\upsilon} = q^2 - dr^2 = t$ are integers. Substituting $q = \frac{m}{2}$ into the second equation, we find that $4dr^2 = m^2 - 4t$ is an integer. Since $d$ is squarefree, this implies that $r = \frac{n}{2}$ for some integer $n$. So now we find that $4t = m^2 - dn^2$. If $m$ is even, then $dn^2 \equiv 0 \pmod 4$, and this implies that $n$ must also be even, again using the fact that $d$ is squarefree. In this case, $q$ and $r$ are both integers, and there is no restriction on $d$. On the other hand, if $m$ is odd, then $1 - dn^2 \equiv 0 \pmod 4$, which implies that $n$ is also odd, and that $d \equiv 1 \pmod 4$. So if $d \equiv 2$ or $3 \pmod 4$, then $q$ and $r$ are integers, while if $d \equiv 1 \pmod 4$, then $q$ and $r$ are either both integers or both "half integers," that is, odd integers divided by 2. Both cases are expressed by saying that $q = \frac{m}{2}$ and $r = \frac{n}{2}$ with $m \equiv n \pmod 2$. □

**Example.** The real number $\upsilon = \frac{3+7\sqrt{5}}{2} = \frac{3}{2} + \frac{7}{2}\sqrt{5}$ is a quadratic integer, since $5 \equiv 1 \pmod 4$ and $3 \equiv 7 \pmod 2$. Specifically, we find that $\upsilon + \overline{\upsilon} = 3$ and $\upsilon\overline{\upsilon} = \frac{3^2-5\cdot 7^2}{4} = -59$, so that $\upsilon$ is a root of $f(x) = x^2 - 3x - 59$, a monic polynomial with integer coefficients. On the other hand, the complex number $\upsilon = \frac{3+7\sqrt{-5}}{2} = \frac{3}{2} + \frac{7}{2}\sqrt{-5}$ is a quadratic number, but not a quadratic integer. Here we find that $\upsilon + \overline{\upsilon} = 3$, but that $\upsilon\overline{\upsilon} = \frac{3^2+5\cdot 7^2}{4} = \frac{127}{2}$ is not an integer. So $\upsilon$ is a root of $f(x) = x^2 - 3x + \frac{127}{2}$, or of $g(x) = 2x^2 - 6x + 127$, but there is no *monic* quadratic polynomial with *integer* coefficients having $\upsilon$ as a root. ◊

**The Discriminant of a Quadratic Number.** We conclude this section with a definition that will be useful in classifying sets of quadratic integers in §2.2. We begin with the following observation.

**Proposition 2.1.5.** *Let* $\upsilon$ *be a quadratic number that is not rational. Then there is a unique polynomial* $f(x) = ax^2 + bx + c$ *for which* $f(\upsilon) = 0$ *under the assumption that* $a$*,* $b$*, and* $c$ *are integers with no prime common divisor and* $a$ *is positive. If* $g(x)$ *is a polynomial with rational coefficients, then* $g(\upsilon) = 0$ *if and only if* $f(x)$ *divides* $g(x)$*.*

We write $\gcd(a, b, c) = 1$ to mean that there is no prime common divisor of all three of $a$, $b$, and $c$. Any two of $a$, $b$, and $c$ might have a common divisor other than 1.

*Proof.* If $\upsilon$ is a quadratic number, then by definition $\upsilon$ is a root of some quadratic polynomial $f(x) = ax^2 + bx + c$ with integer coefficients. We may assume that $\gcd(a, b, c) = 1$ and $a > 0$ by factoring out any common divisors of all coefficients and multiplying by $-1$ if necessary. (This does not affect the assumption that $f(\upsilon) = 0$.) To show uniqueness of $f(x)$ under this condition, it suffices to establish the final claim of Proposition 2.1.5. Here we will assume that if $g(x)$ is a polynomial with rational coefficients, then $g(x) = f(x) \cdot q(x) + r(x)$, where $q(x)$ and $r(x) = sx+t$ also have rational coefficients. (In practice, $q(x)$ and $r(x)$ can be found by long division of $g(x)$ by $f(x)$.) But now $g(\upsilon) = f(\upsilon) \cdot q(\upsilon) + r(\upsilon) = r(\upsilon)$, so that $g(\upsilon) = 0$ if and only if $s\upsilon + t = 0$. If $\upsilon$ is not rational, this is impossible unless $s = 0 = t$. □

**Definition.** If $\upsilon$ is a quadratic number, but not rational, we refer to the unique polynomial $f(x) = ax^2 + bx + c$ with $\gcd(a, b, c) = 1$ and $a > 0$ for which $f(\upsilon) = 0$ as the *minimum polynomial* of $\upsilon$. We define the *discriminant* of $\upsilon$ to be $\Delta(\upsilon) = b^2 - 4ac$, that is, the discriminant of the minimum polynomial of $\upsilon$. It is convenient to define the *(quadratic) discriminant* of a rational number to be 0.

If a quadratic number $\upsilon$ is not rational, we can now say that $\upsilon$ is a quadratic integer if and only if its minimum polynomial is monic. Notice that when $\upsilon$ is not rational, then $\Delta(\upsilon)$ is not a square.

**Example.** Let $\upsilon = \frac{5+\sqrt{7}}{3}$, so that $\overline{\upsilon} = \frac{5-\sqrt{7}}{3}$. Then $\upsilon + \overline{\upsilon} = \frac{10}{3}$ and $\upsilon\overline{\upsilon} = \frac{25-7}{9} = 2$, and equation (2.1.1) shows that $\upsilon$ is a root of $g(x) = x^2 - \frac{10}{3}x + 2$. The minimum polynomial of $\upsilon$ is $f(x) = 3g(x) = 3x^2 - 10x + 6$, and the discriminant of $\upsilon$ is $\Delta(\upsilon) = (-10)^2 - 4 \cdot 3 \cdot 6 = 100 - 72 = 28$. ♢

**Exercise 2.1.3.** Find the minimum polynomial $f(x)$ of each of the following quadratic numbers $\upsilon$, and calculate the discriminant of each $\upsilon$.

(a) $\upsilon = \frac{1}{3} - \frac{7}{5}\sqrt{3}$.

(b) $\upsilon = \frac{3}{2} + \frac{5}{2}\sqrt{-19}$.

(c) $\upsilon = \frac{2}{7} + \frac{1}{3}\sqrt{-29}$.

(d) $\upsilon = \frac{1}{5} - \frac{2}{3}\sqrt{41}$.

The following expression for $\Delta(\upsilon)$ will also be useful when $\upsilon$ is a quadratic integer.

**Proposition 2.1.6.** *Let $\upsilon$ be a quadratic integer, with $\overline{\upsilon}$ its conjugate, as defined in the appropriate quadratic field $\mathbb{Q}(\sqrt{d})$. Then the discriminant of $\upsilon$ is given by $\Delta(\upsilon) = (\upsilon - \overline{\upsilon})^2$.*

*Proof.* If $\upsilon$ is a quadratic integer, then $\upsilon + \overline{\upsilon}$ and $\upsilon\overline{\upsilon}$ are both rational integers, and $\upsilon$ is a root of $f(x) = x^2 - (\upsilon + \overline{\upsilon})x + \upsilon\overline{\upsilon}$, a monic polynomial with integer coefficients. If $\upsilon$ is not rational, then $f(x)$ is the minimum polynomial of $\upsilon$, and so the discriminant of $\upsilon$ is

$$\Delta(\upsilon) = (\upsilon + \overline{\upsilon})^2 - 4\upsilon\overline{\upsilon} = \upsilon^2 - 2\upsilon\overline{\upsilon} + \overline{\upsilon}^2 = (\upsilon - \overline{\upsilon})^2.$$

If $\upsilon$ is rational, then $\overline{\upsilon} = \upsilon$ and so $\Delta(\upsilon) = 0 = (\upsilon - \overline{\upsilon})^2$ in this case as well. □

## 2.2 Domains of Quadratic Integers

In Corollary 2.1.4, we characterized the collection of quadratic integers in an arbitrary quadratic field $\mathbb{Q}(\sqrt{d})$, but saw that the form of these elements varies depending on $d$ modulo 4. We now introduce unified terminology and notation for all such sets of quadratic integers, along with certain subsets of those collections. We will use this notation throughout the remainder of the text, so for convenient reference, we gather several definitions as follows.

**Definition.** If $d \neq 1$ is a squarefree integer and $\gamma$ is a positive integer, let

$$\Delta = \Delta(d, \gamma) = \begin{cases} d\gamma^2, & \text{if } d \equiv 1 \pmod 4, \\ 4d\gamma^2, & \text{if } d \equiv 2 \text{ or } 3 \pmod 4. \end{cases} \tag{2.2.1}$$

We say in this case that $\Delta$ is a *discriminant*, specifically the discriminant with *squarefree part* $d = d_\Delta$ and *index* $\gamma = \gamma_\Delta$. When $\gamma = 1$, we say that $\Delta$ is a *primitive discriminant*. For $\Delta = \Delta(d, \gamma)$, let

$$z = z_\Delta = \frac{\varepsilon + \sqrt{\Delta}}{2}, \quad \text{where} \quad \varepsilon = \varepsilon_\Delta = \begin{cases} \gamma, & \text{if } d \equiv 1 \pmod 4, \\ 0, & \text{if } d \equiv 2 \text{ or } 3 \pmod 4, \end{cases} \tag{2.2.2}$$

that is,

$$z = \begin{cases} \gamma \cdot \frac{1+\sqrt{d}}{2}, & \text{if } d \equiv 1 \pmod 4, \\ \gamma \cdot \sqrt{d}, & \text{if } d \equiv 2 \text{ or } 3 \pmod 4. \end{cases} \tag{2.2.3}$$

We call $z_\Delta$ and $\varepsilon_\Delta$ the *basis element* and the *basis index* of the discriminant $\Delta$, respectively. Then we define the *quadratic domain of discriminant* $\Delta$ to be

$$D = D_\Delta = \{q + rz \mid q, r \in \mathbb{Z}\}. \tag{2.2.4}$$

The *conjugate* of $\upsilon = q + rz$ in $D$ is $\overline{\upsilon} = q + r\overline{z}$, where $\overline{z} = \frac{\varepsilon - \sqrt{\Delta}}{2}$, and the *norm* of $\upsilon$ in $D$ is

$$N(\upsilon) = \upsilon\overline{\upsilon} = q^2 + qr(z + \overline{z}) + r^2(z\overline{z}) = q^2 + \varepsilon qr + \left(\frac{\varepsilon^2 - \Delta}{4}\right) r^2. \tag{2.2.5}$$

We define the *principal form* of discriminant $\Delta$ to be

$$\phi(x,y) = \phi_\Delta(x,y) = x^2 + \varepsilon xy + \left(\frac{\varepsilon^2 - \Delta}{4}\right) y^2. \tag{2.2.6}$$

It will be convenient to denote $\phi(x,1)$ simply as $\phi(x)$, so that

$$\phi(x) = \phi_\Delta(x) = x^2 + \varepsilon x + \frac{\varepsilon^2 - \Delta}{4}, \tag{2.2.7}$$

and call $\phi(x)$ the *principal polynomial* of discriminant $\Delta$.

We make some observations about these definitions before looking at examples. If $\Delta$ is a discriminant, then $\Delta$ is congruent either to 0 or 1 modulo 4 and is not a square. Conversely, given an integer $\Delta$ with these properties, we can write $\Delta = \Delta(d,\gamma)$, where $d$ is the squarefree part of $\Delta$ (that is, $\Delta$ divided by its largest square divisor) and $\gamma$ is the largest integer so that $\Delta = \gamma^2\Delta_0$ with $\Delta_0$ also a discriminant. Note that $\Delta$ is a discriminant precisely when $\Delta = b^2 - 4ac$ for some polynomial $f(x) = ax^2 + bx + c$ whose roots are not rational.

We find that $\overline{z} = \varepsilon - z$, and so if $\upsilon = q + rz$ is in $D$, then $\overline{\upsilon} = (q + \varepsilon r) - rz$ is also in $D$. If $\Delta = \Delta(d,\gamma)$, then $\varepsilon = \varepsilon_\Delta$ is odd precisely when $d \equiv 1 \pmod 4$ and $\gamma$ is odd. In any case, $\varepsilon$ has the same parity as $\Delta$, and $\varepsilon^2 \equiv \Delta \pmod 4$. Therefore the norm of an element of $D_\Delta$ is always a rational integer, and the principal form $\phi(x,y)$ has integer coefficients. Observe also that $N(q + rz) = \phi(q,r)$ for every pair of integers $q$ and $r$. The discriminant of the principal polynomial $\phi(x)$ is $\varepsilon^2 - 4 \cdot \frac{\varepsilon^2 - \Delta}{4} = \Delta$, as claimed in our terminology.

**Example.** If $d = -1$ and $\gamma = 1$, then we have $\Delta = \Delta(d,\gamma) = -4$ since $d \equiv 3 \pmod 4$. So $\varepsilon = 0$ and $z = \sqrt{-1}$, and thus $D_{-4} = \{q + ri \mid q,r \in \mathbb{Z}\}$, the set of Gaussian integers. We will continue to denote this set as $\mathbb{Z}[i]$ also. By equation (2.2.5), the norm of an element $\upsilon = q + rz = q + ri$ is $N(\upsilon) = q^2 + r^2$, and by (2.2.7), the principal polynomial of discriminant $\Delta = -4$ is $\phi(x) = x^2 + 1$. ♢

**Example.** If $d = -3$ and $\gamma = 1$, then $\Delta = -3$ since $d \equiv 1 \pmod 4$. Here $\varepsilon = 1$ and $z = \frac{1+\sqrt{-3}}{2}$. This complex number is often written as $\omega$, so we may also denote $D_{-3} = \{q + r\omega \mid q,r \in \mathbb{Z}\}$ as $\mathbb{Z}[\omega]$. The norm of $\upsilon = q + rz$ is $N(\upsilon) = q^2 + qr + r^2$, and $\phi(x) = x^2 + x + 1$. ♢

**Example.** Let $\Delta = \Delta(-3,2) = -12$. Here $\varepsilon = 2$ and $z = \frac{2+\sqrt{-12}}{2} = 1 + \sqrt{-3} = 2\omega$, with $\omega$ as in the preceding example. So $D_{-12}$ consists of all $q + 2r\omega$ with $q$ and $r$ integers. Note also that

$$D_{-12} = \left\{(q + r) + r\sqrt{-3} \mid q,r \in \mathbb{Z}\right\} = \left\{s + t\sqrt{-3} \mid s,t \in \mathbb{Z}\right\},$$

so we may denote this set as $\mathbb{Z}[\sqrt{-3}]$. (But $z_{-12} \neq \sqrt{-3}$.) The norm of $v = q + rz$ in $D_{-12}$ is $N(v) = q^2 + 2qr + 4r^2$, and $\phi(x) = x^2 + 2x + 4$. $\Diamond$

**Example.** If $d = 5$ and $\gamma = 1$, then $\Delta = 5$ since $d \equiv 1 \pmod 4$. So $\varepsilon = 1$ and $z = \frac{1+\sqrt{5}}{2}$. This real number is often called the *golden ratio*, and denoted as $\varphi$, so we also write $D_5$ as $\mathbb{Z}[\varphi]$. The norm of $v = q + rz$ in $D_5$ is $N(v) = q^2 + qr - r^2$, and $\phi(x) = x^2 + x - 1$. $\Diamond$

**Exercise 2.2.1.** For each pair $d$ and $\gamma$ below, calculate $\Delta = \Delta(d, \gamma)$, describe the basis element $z = z_\Delta$, give a formula for the norm of a typical element $q + rz$ in $D_\Delta$, and find the principal polynomial of discriminant $\Delta$.

(a) $d = -7$ and $\gamma = 1$.

(b) $d = -7$ and $\gamma = 2$.

(c) $d = 7$ and $\gamma = 1$.

(d) $d = 17$ and $\gamma = 1$.

**Exercise 2.2.2.** For each discriminant $\Delta$ below, write $\Delta$ as $\Delta(d, \gamma)$ for some integers $d$ and $\gamma$, describe the basis element $z = z_\Delta$, give a formula for the norm of a typical element $q+rz$ in $D_\Delta$, and find the principal polynomial of discriminant $\Delta$.

(a) $\Delta = 45$.

(b) $\Delta = -63$.

(c) $\Delta = -84$.

(d) $\Delta = 84$.

(e) $\Delta = -88$.

(f) $\Delta = 88$.

(g) $\Delta = -99$.

(h) $\Delta = 297$.

(i) $\Delta = 300$.

(j) $\Delta = -300$.

**Exercise 2.2.3.** Let $v$ and $w$ be elements of a quadratic domain $D_\Delta$. Show that $\overline{v + w} = \overline{v} + \overline{w}$ and that $\overline{v \cdot w} = \overline{v} \cdot \overline{w}$. Show that $N(v \cdot w) = N(v) \cdot N(w)$.

**Exercise 2.2.4.** Let $\phi(x)$ be the principal polynomial and let $\varepsilon = \varepsilon_\Delta$ be the basis index of some discriminant $\Delta$. Show that $\phi(k) = \phi(-k - \varepsilon)$ for all integers $k$.

**Exercise 2.2.5.** Let $v = a + bz$ be an element of a quadratic domain $D = D_\Delta$, with $\overline{v}$ the conjugate of $v$, and let $\Delta(v)$ be the discriminant of $v$. Show that the norm of $v$ satisfies $N(v) = \dfrac{(v+\overline{v})^2 - \Delta(v)}{4}$.

**Properties of Quadratic Domains.** In this subsection, we compile several general properties of the sets $D_\Delta$. Since each $D_\Delta$ is a subset of the complex numbers, the following exercise and proposition show that $D_\Delta$ has the algebraic properties of an *integral domain*, and so justify the terminology of $D_\Delta$ as a quadratic domain. (See Appendix C for the definition of an integral domain.)

**Exercise 2.2.6.** Show that every quadratic domain $D = D_\Delta$ is closed under addition, contains 1, and contains the negative of each of its elements.

**Proposition 2.2.1.** *If $\Delta$ is a discriminant, then the set $D_\Delta$ is closed under multiplication.*

*Proof.* First note that $z = \frac{\varepsilon+\sqrt{\Delta}}{2}$ is a root of

$$(x-z)(x-\overline{z}) = x^2 - (z+\overline{z})x + z\overline{z} = x^2 - \varepsilon x + \frac{\varepsilon^2 - \Delta}{4},$$

a polynomial with integer coefficients. It follows that $z^2 = -\frac{\varepsilon^2-\Delta}{4} + \varepsilon z$ is an element of $D_\Delta$, and so

$$(q+rz)(s+tz) = \left(qs - \frac{\varepsilon^2-\Delta}{4}\cdot rt\right) + (qt + rs + \varepsilon rt)z \tag{2.2.8}$$

is in $D_\Delta$ for all integers $q$, $r$, $s$, and $t$. □

Our next result shows that every element of a quadratic domain is a quadratic integer.

**Proposition 2.2.2.** *Let $D = D_\Delta$ be the quadratic domain of discriminant $\Delta = \Delta(d,\gamma)$. Then $D$ consists precisely of all quadratic integers in $\mathbb{Q}(\sqrt{d})$ whose discriminant is a square multiple of $\Delta$.*

*Proof.* We leave to the reader the verification that when $\Delta = \Delta(d,\gamma)$ for some squarefree integer $d \neq 1$ and positive integer $\gamma$, then $D = D_\Delta$ is a subset of $\mathbb{Q}(\sqrt{d})$. Let $v = q+rz$ be in $D$, so that $\overline{v} = q+r\overline{z}$. If $z = \frac{\varepsilon+\sqrt{\Delta}}{2}$ and $\overline{z} = \frac{\varepsilon-\sqrt{\Delta}}{2}$, then $z+\overline{z} = \varepsilon$ and $z-\overline{z} = \sqrt{\Delta}$. We have already seen that $v\overline{v} = N(v)$ is an integer, and we find that $v+\overline{v} = 2q + r(z+\overline{z}) = 2q + \varepsilon r$ is also an integer. So $v$ is a quadratic integer by Proposition 2.1.3. The discriminant of $v$ is $(v-\overline{v})^2 = r^2(z-\overline{z})^2 = r^2\Delta$ by Proposition 2.1.6.

Conversely, suppose that $v$ is a quadratic integer, say that $f(v) = 0$ for $f(x) = x^2 + bx + c$, and that $b^2 - 4c = r^2\Delta$ for some integer $r$ and fixed discriminant $\Delta$. We can select the sign of $r$ so that $v = \frac{-b+r\sqrt{\Delta}}{2}$. Then we find that $v = q + rz$, where $q = \frac{-b-r\varepsilon}{2}$, with $\varepsilon = \varepsilon_\Delta$ and $z = z_\Delta$. If $b$ is odd, then $r$ and $\Delta$ are both odd, so that $r\varepsilon$ is odd. If $b$ is even, then $r$ is even or $\Delta$ is even, and we find that $r\varepsilon$ is even in either case. So $q$ is an integer, and $v$ is an element of the quadratic domain of discriminant $\Delta$. □

**Proposition 2.2.3.** *Let $\Delta = \Delta(d, 1)$ be a primitive discriminant. Then $D_\Delta$ is the set of all quadratic integers in the quadratic field $\mathbb{Q}(\sqrt{d})$.*

*Proof.* If $d \equiv 2$ or $3 \pmod 4$, then $z = \sqrt{d}$ as in equation (2.2.3), and the quadratic integers in $\mathbb{Q}(\sqrt{d})$ are precisely of the form $q + r\sqrt{d} = q + rz$ with $q$ and $r$ integers. If $d \equiv 1 \pmod 4$, then $z = \frac{1+\sqrt{d}}{2}$, again by equation (2.2.3), and the quadratic integers in $\mathbb{Q}(\sqrt{d})$ are precisely of the form $v = \frac{m+n\sqrt{d}}{2}$, where $m \equiv n \pmod 2$. In this case, $\frac{m+n\sqrt{d}}{2} = \frac{m-n}{2} + nz$ is in $D_\Delta$ since $\frac{m-n}{2}$ is an integer. Conversely, any $q + rz$ is equal to $\frac{(2q+r)+r\sqrt{d}}{2}$, a quadratic integer in $\mathbb{Q}(\sqrt{d})$. □

On the other hand, if $\Delta = \Delta(d, \gamma)$ with $\gamma > 1$, then $D_\Delta$ is a proper subset of the domain of all quadratic integers in $\mathbb{Q}(\sqrt{d})$. The following proposition describes this situation.

**Proposition 2.2.4.** *Let $\Delta = \Delta(d, 1)$ and let $\Delta_\gamma = \Delta(d, \gamma)$ for some squarefree integer $d \neq 1$ and positive integer $\gamma$. Let $D = \{q + rz \mid q, r \in \mathbb{Z}\}$ be the quadratic domain of discriminant $\Delta$. Then $D_\gamma = \{q + \gamma rz \mid q, r \in \mathbb{Z}\}$ is the quadratic domain of discriminant $\Delta_\gamma$. That is, $D_\gamma$ is the set of all elements of $D$ in which the coefficient of $z$ is divisible by $\gamma$.*

*Proof.* Let $\varepsilon = \varepsilon_\Delta$ and $z = z_\Delta$ be defined for the discriminant $\Delta$ as in (2.2.2), and likewise let $\varepsilon_\gamma = \varepsilon_{\Delta_\gamma}$ and $z_\gamma = z_{\Delta_\gamma}$. We find that $\varepsilon_\gamma = \gamma \cdot \varepsilon$ and $\Delta_\gamma = \gamma^2 \cdot \Delta$, and so $z_\gamma = \frac{\varepsilon_\gamma + \sqrt{\Delta_\gamma}}{2} = \gamma \cdot z$. Thus

$$D_\gamma = \{q + rz_\gamma \mid q, r \in \mathbb{Z}\} = \{q + \gamma rz \mid q, r \in \mathbb{Z}\},$$

as we wanted to show. □

We summarize the preceding two propositions with the following terminology.

**Definition.** Let $d \neq 1$ be squarefree. If $\Delta = \Delta(d, 1)$, then we refer to $D_\Delta$ as a *complete* quadratic domain. If $\Delta = \Delta(d, \gamma)$ with $\gamma > 1$, we call $D_\Delta$ a *quadratic subdomain*.

**Exercise 2.2.7.** Let $\Delta = \Delta(d, 1)$ and $\Delta_\gamma = \Delta(d, \gamma)$ for some squarefree integer $d \neq 1$ and some positive integer $\gamma$. Let $\phi(x)$ and $\phi_\gamma(x)$ be the principal polynomials of discriminant $\Delta$ and $\Delta_\gamma$, respectively. Show that $\phi_\gamma(\gamma x) = \gamma^2\phi(x)$ and $\phi'_\gamma(\gamma x) = \gamma\phi'(x)$ for all $x$.

**Exercise 2.2.8.** Let $D$ and $D_\gamma$ be the quadratic domains of discriminant $\Delta = \Delta(d, 1)$ and $\Delta_\gamma = \Delta(d, \gamma)$, respectively, where $d \neq 1$ is squarefree and $\gamma$ is a positive integer. Let $v$ be an element of $D_\gamma$, and so an element of $D$ as in Proposition 2.2.4. Show that the value of $N(v)$ is independent of whether $v$ is regarded as an element of $D_\gamma$ or an element of $D$.

**Divisibility in Quadratic Domains.** Concepts of divisibility apply in every integral domain, and so in every quadratic domain, as we have already seen with the domain of Gaussian integers. To conclude this section, we recall some definitions and mention some particular results that hold in quadratic domains.

**Definition.** Let $u$, $v$, and $w$ be elements of a quadratic domain $D$. Then

(1) $v$ *divides* $w$ if $w = vy$ for some $y$ in $D$,

(2) $u$ is a *unit* if $u$ divides 1,

(3) $v$ and $w$ in $D$ are *associates* if $v$ divides $w$ and $w$ divides $v$.

**Exercise 2.2.9.** Let $u$, $v$, and $w$ be elements of a quadratic domain $D$. Show that the following statements are true.

(a) If $v$ divides $w$ in $D$, then $N(v)$ divides $N(w)$ in $\mathbb{Z}$.

(b) $u$ is a unit in $D$ if and only if $N(u) = \pm 1$.

(c) If $u$ is a unit in $D$, then $\pm u^n$ is a unit in $D$ for every integer $n$.

(d) If $v$ and $w$ are associates in $D$, then $N(v) = \pm N(w)$.

We can completely describe the units in $D_\Delta$ when $\Delta$ is negative.

**Proposition 2.2.5.** *Let $D = D_\Delta = \{q + rz \mid q, r \in \mathbb{Z}\}$, where $\Delta$ is negative. Then the set of units in $D$ is*

(1) $\{1, -1, z, -z, 1 - z, -1 + z\}$, *if* $\Delta = -3$,

(2) $\{1, -1, z, -z\}$, *if* $\Delta = -4$,

(3) $\{1, -1\}$, *if* $\Delta < -4$.

*Proof.* Note that

$$N(q+rz) = q^2 + \varepsilon \cdot qr + \frac{\varepsilon^2 - \Delta}{4} \cdot r^2 = \frac{(2q+\varepsilon r)^2 - \Delta r^2}{4}$$

by equation (2.2.5). If $\Delta$ is negative, it follows that $N(v) \geq 0$ for all $v$ in $D$. So we can find all units of $D$ by solving $(2q+\varepsilon r)^2 - \Delta r^2 = 4$. If $\Delta < -4$, then $r$ must equal 0, and so $q = \pm 1$. If $\Delta = -4$, then $\varepsilon = 0$, and the equation becomes $q^2 + r^2 = 1$, with solutions $q = \pm 1$ and $r = 0$, or $q = 0$ and $r = \pm 1$. Finally, if $\Delta = -3$, then $\varepsilon = 1$, and we need to solve $(2q+r)^2 + 3r^2 = 4$. The only solutions occur when $r = 0$ and $2q + r = \pm 2$, or $r = \pm 1$ and $2q + r = \pm 1$. Solving each possibility for $q$ yields the six elements listed in case (1). □

**Exercise 2.2.10.** Show that the six units in $D_{-3}$ are precisely the distinct integer powers of $z = z_{-3} = \frac{1+\sqrt{-3}}{2}$.

The situation is more complicated when $\Delta$ is positive. For instance, if $\Delta = 8$, so that $\varepsilon = 0$ and $z = \frac{0+\sqrt{8}}{2} = \sqrt{2}$, we find that $u = 1+z$ is a unit in $D = D_8$, since $N(u) = 1^2 - 2 \cdot 1^2 = -1$. Here $u$ is a real number greater than 1, so it follows that $u^m < u^n$ when $m < n$. But then Exercise 2.2.9(c) shows that there are infinitely many units in $D$. We will prove that the set of units in $D_\Delta$ is always infinite when $\Delta$ is positive, and describe a method of finding all these units, in §11.2.

**Definition.** Let $D$ be a quadratic domain, and let $w$ be an element of $D$ that is neither zero nor a unit. Then we say that $w$ is *reducible* in $D$ if it is possible to write $w = uv$ for some $u$ and $v$ in $D$, neither a unit. We say that $w$ is *irreducible* in $D$ otherwise, that is, if when $w = uv$ in $D$, then either $u$ or $v$ must be a unit.

We can often use the following proposition to establish that an element of a quadratic domain is irreducible.

**Proposition 2.2.6.** *Let $w$ be an element of a quadratic domain $D$ with $|N(w)| = n > 1$. If there is no element $v$ in $D$ for which $|N(v)| = d$ is a divisor of $n$ with $1 < d < n$, then $w$ is irreducible in $D$.*

In particular, if $|N(w)| = p$ is a rational prime, then $w$ is irreducible in $D$.

*Proof.* Note that if $|N(w)| > 1$, then $w$ is neither zero nor a unit in $D$. Suppose that $w = uv$ in $D$, so that $n = N(w) = N(uv) = N(u) \cdot N(v)$. By the assumption in this proposition, we must conclude that $|N(u)| = 1$ and $|N(v)| = n$, or vice versa. So either $u$ or $v$ must be a unit in $D$, and $w$ is irreducible in $D$ by definition. □

**Proposition 2.2.7.** *Let $D$ be a quadratic domain, and let $w$ be an element of $D$ that is neither zero nor a unit. Then $w$ can be written as a product of irreducible elements in $D$.*

*Proof.* If $w$ cannot be written as a product of irreducible elements, we can assume that $|N(w)| > 1$ is minimal among elements with that property. Now $w$ itself is reducible, since otherwise we regard it as a product of irreducible elements with just one term. So we can write $w = uv$ with neither $u$ nor $v$ a unit in $D$. But then $N(w) = N(u) \cdot N(v)$, with $1 < |N(u)|, |N(v)| < |N(w)|$. By our assumption that $|N(w)|$ is minimal, both $u$ and $v$ can be written as products of irreducible elements. But then $w = uv$ is likewise a product of irreducible elements, contrary to assumption. □

In the domain of Gaussian integers, we saw that this irreducible factorization is *unique*, aside from the order of the factors and multiplication by units. It is an important fact, which we will demonstrate in §2.5, that there are many other examples of quadratic domains in which this property does not hold. In §2.3, we first introduce an alternative notation for quadratic integers, which will be useful in further describing properties of divisibility.

## 2.3 Ideal Form for Quadratic Integers

In Chapter 1, ideal form notation proved to be a useful method of describing irreducible factorization in the domain of Gaussian integers, $\mathbb{Z}[i]$. In this section, we see that this notation generalizes to all quadratic domains, with similar applications to divisibility in $D_\Delta$.

**Definition.** Let $D = D_\Delta$ be the quadratic domain of some discriminant $\Delta = \Delta(d, \gamma)$. Let $v$ be a nonzero element of $D$, written as $v = g(q + rz)$ with $g$ a positive integer and $\gcd(q, r) = 1$. Let $a$ be the norm of $q + rz$ and let $k$ satisfy the congruence $rk \equiv q \pmod{a}$. Then we say that $g[a : k]$ is an *ideal form* for $v$ in $D$ and we refer to $g$, $a$, and $k$ as the *divisor*, the *subnorm*, and the *character* of this ideal form, respectively. If $g = 1$, we say that $v$ is *primitive*, and write this ideal form as $[a : k]$.

**Exercise 2.3.1.** Let $v$ be an element of a quadratic domain $D_\Delta$. Show that if $v$ has ideal form $g[a : k]$, then $\overline{v}$ has ideal form $g[a : -k - \varepsilon]$, where $\varepsilon = \varepsilon_\Delta$ is the basis index of $\Delta$ as defined in (2.2.2).

In most cases when we use ideal form notation for a quadratic integer, the quadratic domain in which we work will be clear from the context. But we may also write $g[a : k]$ as $g[a : k]_\Delta$, if necessary, to emphasize that we refer to an ideal form for an element $v$ in $D_\Delta$.

Equation (2.2.5) shows that if $N(q+rz) = a$, then any prime common divisor of $a$ and $r$ must also divide $q$. So if $\gcd(q, r) = 1$, then the congruence $rx \equiv q \pmod{a}$ has a unique solution $k$ modulo $a$. It is typically convenient to select the

character $k$ of an ideal form so that $2k+\varepsilon$ is minimal in absolute value, but we can replace $k$ by any integer to which it is congruent modulo $a$. We always take the divisor $g$ of an ideal form to be positive, but when $\Delta$ is positive, then the subnorm $a = N(q + rz)$ might be negative. In the definition above, and in similar general statements below, we write $rx \equiv q \pmod{a}$ rather than $rx \equiv q \pmod{|a|}$ to simplify notation, but we will write the modulus as a positive integer in specific cases, as in the following example.

**Example.** In $D = D_5$, the norm of $v = q+rz$ is $N(v) = q^2+qr-r^2$. If $v = -3+4z$, then $N(v) = (-3)^2 - 3 \cdot 4 - 4^2 = -19$. Since $4x \equiv -3 \pmod{19}$ has $k = 4$ as a solution, we can write an ideal form for $v$ as $[-19 : 4]$. ◊

**Example.** In $D = D_{-3}$, the norm of $v = q + rz$ is $N(v) = q^2 + qr + r^2$. To write $v = 10 + 6z$ in ideal form, we first note that $v = 2(5 + 3z)$ with $5 + 3z$ primitive. Now $a = N(5 + 3z) = 49$, and the congruence $3x \equiv 5 \pmod{49}$ has $k = 18$ as a solution, so we can write an ideal form for $v$ as $2[49 : 18]$. ◊

As we saw with a similar example in the Gaussian integers, factoring out common divisors from the coefficients of $v$ is a necessary step. In this example, $N(v) = 10^2+10\cdot 6+6^2 = 196$, and $6x \equiv 10 \pmod{196}$ has two distinct solutions, $-31$ and 67, modulo 196. However, neither $[196 : -31]$ nor $[196 : 67]$ can be an ideal form for an element of $D_{-3}$, as we demonstrate after the following proposition.

**Proposition 2.3.1.** *Let $\phi(x)$ be the principal polynomial of some discriminant $\Delta$. If $g[a : k]$ is an ideal form for some element $v$ of the quadratic domain $D = D_\Delta$, then $a$ divides $\phi(k)$.*

*Proof.* Let $v = g(q + rz)$, so that $\gcd(q, r) = 1$, $N(q + rz) = a$, and $rk \equiv q \pmod{a}$. We find that

$$r^2\phi(k) = r^2\left(k^2 + \varepsilon k + \frac{\varepsilon^2 - \Delta}{4}\right) = (rk)^2 + \varepsilon(rk)r + \left(\frac{\varepsilon^2 - \Delta}{4}\right)r^2$$

is congruent to

$$q^2 + \varepsilon qr + \left(\frac{\varepsilon^2 - \Delta}{4}\right)r^2 = N(q + rz) = a$$

modulo $a$, using equations (2.2.5) and (2.2.7). Since $\gcd(r, a) = 1$, it follows that $a$ divides $\phi(k)$. □

**Example.** The principal polynomial of discriminant $\Delta = -3$ is $\phi(x) = x^2+x+1$. Since $a = 196$ divides neither $\phi(-31) = 931$ nor $\phi(67) = 4557$, no element of $D_{-3}$ can have ideal form $[196 : -31]$ or $[196 : 67]$. ◊

**Exercise 2.3.2.** In each part, find an ideal form for the element $v = q + rz$ in the given quadratic domain $D_\Delta$. (Here $z$ is the basis element of discriminant $\Delta$.)

(a) $v = 3 + 5z$ in $D_{-8}$.

(b) $v = 3 + 5z$ in $D_{-3}$.

(c) $v = 3 + 5z$ in $D_8$.

(d) $v = 3 + 5z$ in $D_{12}$.

(e) $v = 5 + 2z$ in $D_{-8}$.

(f) $v = 7 + 3z$ in $D_{12}$.

(g) $v = 5 - z$ in $D_{-20}$.

(h) $v = 15 + 6z$ in $D_{-23}$.

(i) $v = 14 - 6z$ in $D_{-24}$.

(j) $v = 27 - 12z$ in $D_{24}$.

**Ideal Forms and Divisibility.** Our next results generalize divisibility criteria that we saw in the domain of Gaussian integers, using ideal forms, to all other quadratic domains. We follow the same approach that we developed in $\mathbb{Z}[i]$, and leave some details for the reader.

**Exercise 2.3.3.** Let $v$ and $w$ be elements of $D_\Delta$ for some discriminant $\Delta$. Suppose that $v$ and $w$ have ideal forms $g[a : k]$ and $h[b : \ell]$, respectively. Show that if $v$ divides $w$ in $D_\Delta$, then $g$ divides $h$ in $\mathbb{Z}$. (Hint: Use the same argument as in the proof of Lemma 1.3.3.)

Using Exercise 2.3.3, we can restrict our attention to divisibility by $v$ when $v$ is a *primitive* quadratic integer.

**Lemma 2.3.2.** *Let $v$ be a primitive element of a quadratic domain $D = D_\Delta$, with $[a : k]$ an ideal form for $v$. Then $v$ divides an element $w = m + nz$ in $D$ if and only if $nk \equiv m \pmod{a}$.*

*Proof.* Let $v = q + rz$, with ideal form $[a : k]$, so that $N(q + rz) = a$ and $rk \equiv q \pmod{a}$. Suppose that $v$ divides $w$, say with $m + nz = (q + rz)(s + tz)$ for some integers $s$ and $t$. Then $m = qs - \frac{\varepsilon^2 - \Delta}{4} rt$ and $n = qt + rs + \varepsilon rt$, using equation (2.2.8), so that

$$\begin{aligned} nk - m &= (qtk + rsk + \varepsilon rtk) - \left(qs - \frac{\varepsilon^2 - \Delta}{4} rt\right) \\ &\equiv rtk^2 + rsk + \varepsilon rtk - rks + \frac{\varepsilon^2 - \Delta}{4} rt \equiv rt \cdot \phi(k) \pmod{a}. \end{aligned}$$

Since $k$ satisfies $\phi(x) \equiv 0 \pmod{a}$ by Proposition 2.3.1, then $nk \equiv m \pmod{a}$.

Conversely, suppose that $rk \equiv q \pmod{a}$ and $nk \equiv m \pmod{a}$, and consider

$$(m + nz)(q + r\overline{z}) = \left(mq + \varepsilon mr + \frac{\varepsilon^2 - \Delta}{4} \cdot nr\right) + (nq - mr)z. \tag{2.3.1}$$

(Here we use equation (2.2.8) and the fact that $\overline{z} = \varepsilon - z$.) Now we find that

$$mq + \varepsilon mr + \frac{\varepsilon^2 - \Delta}{4} \cdot nr \equiv nr \cdot \phi(k) \equiv 0 \pmod{a}$$

and

$$nq - mr \equiv nrk - nkr \equiv 0 \pmod{a},$$

so that

$$s = \frac{1}{a}\left(mq + \varepsilon mr + \frac{\varepsilon^2 - \Delta}{4} \cdot nr\right) \quad \text{and} \quad t = \frac{nq - mr}{a}$$

are integers. Multiplying both sides of equation (2.3.1) by $q + rz$ and using the fact that $a = (q + rz)(q + r\overline{z})$, we obtain the equation $m + nz = (q + rz)(s + tz)$. So $v$ divides $w$. □

**Theorem 2.3.3.** *Let $v$ and $w$ be elements of a quadratic domain $D = D_\Delta$, written in ideal form as $g[a : k]$ and $h[b : \ell]$, respectively. Then $v$ divides $w$ in $D$ if and only if*

$$g \text{ divides } h, \quad ag \text{ divides } bh, \quad \text{and} \quad h\ell \equiv hk \pmod{ag}.$$

*Proof.* As noted above, we can assume that $v$ is primitive, so that $g = 1$. Write $w = h(m+nz)$ with $\gcd(m, n) = 1$, $N(m+nz) = b$, and $n\ell \equiv m \pmod{b}$, so that $w$ has ideal form $h[b : \ell]$. We have seen that in this case $b$ and $n$ can have no prime common divisor. Suppose first that $a$ divides $bh$ and $h\ell \equiv hk \pmod{a}$. By Lemma 2.3.2, to show that $v$ divides $w$, it suffices to show that $hnk \equiv hm \pmod{a}$. But $n\ell \equiv m \pmod{b}$ implies that $hn\ell \equiv hm \pmod{bh}$, and then that $hn\ell \equiv hm \pmod{a}$ since $a$ divides $bh$. Now $h\ell \equiv hk \pmod{a}$ implies that $hn\ell \equiv hnk \pmod{a}$, and so $hnk \equiv hm \pmod{a}$, as we wanted to show.

Conversely, suppose that $v$ divides $w$, so that $hnk \equiv hm \pmod{a}$ by Lemma 2.3.2. Observe that $bh = N(m + nz)h = (m + nz)(m + n\overline{z})h = w(m + n\overline{z})$. If $v$ divides $w$, then $v$ divides $bh = bh + 0 \cdot z$ as an element of $D$. But then $0 \cdot k \equiv bh \pmod{a}$, again applying Lemma 2.3.2. That is, $a$ divides $bh$. Now $n\ell \equiv m \pmod{b}$ implies that $hn\ell \equiv hm \pmod{a}$, as we saw above, and so we have that $hn\ell \equiv hnk \pmod{ag}$. By the congruence cancellation property (Proposition 0.1.6), then $n\ell \equiv nk \pmod{a'}$, where $a' = ag/\gcd(ag, h)$. But we can argue as follows that $a'$ and $n$ can have no prime common divisor. If $p$ divides $a'$, we see that the exponent of $p$ in the prime factorization of $h$ must be strictly smaller than the exponent of $p$ in $a$. Since $a$ divides $bh$, it follows that $p$ must divide $b$. But we noted above that $b$ and $n$ have no prime common divisor.

So now Proposition 0.1.6 implies that $\ell \equiv k \pmod{a'}$, and then that $h\ell \equiv hk \pmod{a}$. □

**Example.** Let $D = D_{-20}$, so that $z = \sqrt{-5}$. The norm of an element $v = q + rz$ is $N(v) = q^2 + 5r^2$. Here $v = 1 + z$ can be written in ideal form as $[6 : 1]$, and Lemma 2.3.2 implies that $v$ divides $w = m + nz$ if and only if $m \equiv n \pmod{6}$. For instance, $v$ divides $w = 5 - 7z$, and we can use the method of the proof of Lemma 2.3.2 to show that $5 - 7z = (1 + z)(-5 - 2z)$. If $w$ is expressed as $h[b : \ell]$ in ideal form, then $v$ divides $w$ if and only if 6 divides $bh$ and $h\ell \equiv h \pmod{6}$. For example, since $N(5-7z) = 5^2+5\cdot(-7)^2 = 270$, and $k = 115$ satisfies $-7x \equiv 5 \pmod{270}$, we have that $w = 5-7z$ has ideal form $[270 : 115]$. With $270 = 6 \cdot 45$ and $115 \equiv 1 \pmod{6}$, we confirm that $v$ divides $w$. ◊

**Exercise 2.3.4.** In each part, find ideal forms for $v$ and $w$ in the given quadratic domain $D = D_\Delta$, and determine whether $v$ divides $w$ in $D$.

(a) $v = 1 + z$ and $w = 5 + 2z$ in $D_{-8}$.

(b) $v = 1 + z$ and $w = 5 - 2z$ in $D_{-8}$.

(c) $v = 5 + 3z$ and $w = 7 + 3z$ in $D_{12}$.

(d) $v = 1 + z$ and $w = 5 - z$ in $D_{-20}$.

(e) $v = 1 + z$ and $w = 5 + z$ in $D_{-20}$.

Theorem 2.3.3 establishes the following result as a consequence, characterizing units and associates in ideal form.

**Corollary 2.3.4.** *Let $D$ be a quadratic domain.*

(1) *An element $u$ of $D$ is a unit if and only if $u$ has ideal form $[1 : 0]$ or $[-1 : 0]$.*

(2) *If $v$ and $w$ are elements of $D$, written in ideal form as $g[a : k]$ and $h[b : \ell]$, respectively, then $v$ and $w$ are associates if and only if $g = h$, $b = \pm a$, and $\ell \equiv k \pmod{a}$.*

*Proof.* In every quadratic domain $D$, the norm of 1 is $N(1 + 0 \cdot z) = 1$. So 1 has ideal form $[1 : 0]$, since 0 satisfies $0 \cdot x \equiv 1 \pmod{1}$. Now $u$ is a unit of $D$ if and only if $u$ divides 1. If $u$ is written as $g[a : k]$ in ideal form, Theorem 2.3.3 implies that $ag$ divides 1. With $g$ positive, and $k$ defined modulo $a$, the only possibilities are $[1 : 0]$ or $[-1 : 0]$ as an ideal form for $u$. Conversely, if $u$ has ideal form $[1 : 0]$ or $[-1 : 0]$, then $u$ divides 1 by Theorem 2.3.3. This establishes statement (1).

Now suppose that $v$ and $w$ are expressed in ideal form as $g[a : k]$ and $h[b : \ell]$, respectively. Then Theorem 2.3.3 implies that $v$ and $w$ are associates if

and only if

(1) $g$ divides $h$ and $h$ divides $g$, so that $g = h$ since $g$ and $h$ are positive,

(2) $ag$ divides $bh$ and $bh$ divides $ag$, which then implies that $b = \pm a$,

(3) $h\ell \equiv hk \pmod{ag}$ and $g\ell \equiv gk \pmod{bh}$, which simplify in both cases to $\ell \equiv k \pmod{a}$.

This establishes statement (2) of Corollary 2.3.4. □

We noted in §2.2 that if $D = D_\Delta$ with $\Delta$ negative, then the norm of every nonzero element of $D$ is positive. So in that case, $u$ is a unit if and only if $u$ has ideal form $[1 : 0]$, and $v$ and $w$ are associates if and only if $v$ and $w$ can be expressed the same way in ideal form. If $\Delta$ is positive, then $D_\Delta$ may or may not have units with ideal form $[-1 : 0]$. In $D_8$, for instance, we have that $u = 1 + \sqrt{2}$ is a unit with $N(u) = -1$, so that $u$ has ideal form $[-1 : 0]$. In $D_{12}$, on the other hand, with $N(q + r\sqrt{3}) = q^2 - 3r^2$, we see as follows that there is no element $u$ with $N(u) = -1$. Since $q^2 - 3r^2 \equiv q^2 + r^2 \pmod 4$, while $-1 \equiv 3 \pmod 4$, there can be no solution of $q^2 - 3r^2 = -1$.

**Multiplication with Ideal Forms.** Multiplication of quadratic integers written in ideal form follows the same rules as we saw for Gaussian integers. We conclude this section with two results that often allow us to calculate products in practice. We begin by stating a lemma whose proof is identical to one we established for Gaussian integers.

**Lemma 2.3.5.** *Let $v$ and $w$ be primitive quadratic integers in some quadratic domain $D_\Delta$, having ideal forms $[a : k]$ and $[b : \ell]$, respectively. Suppose that $vw$ has ideal form $g[c : m]$. Then $g$ is a common divisor of $a$ and $b$.*

*Proof.* See the proof of Lemma 1.4.3. □

**Proposition 2.3.6.** *Let $v$ and $w$ be primitive quadratic integers in some quadratic domain $D_\Delta$, having ideal forms $[a : k]$ and $[b : \ell]$, respectively. If $\gcd(a, b) = 1$, then $vw$ has ideal form $[ab : m]$, where $m \equiv k \pmod{a}$ and $m \equiv \ell \pmod{b}$.*

*Proof.* By Lemma 2.3.5, we know that $vw$ is primitive, so that $vw$ has ideal form $[ab : m]$ for some $m$, since $N(vw) = ab$. Theorem 2.3.3 implies that $m \equiv k \pmod{a}$ and $m \equiv \ell \pmod{b}$, since $v$ and $w$ divide $vw$. □

**Exercise 2.3.5.** Find ideal forms for $v = 1 + 2z$ and $w = 1 + 3z$ in $D_{-8}$. Use Proposition 2.3.6 to find an ideal form for $vw$. Verify that your answer is correct by calculating $vw$ and its ideal form directly.

**Proposition 2.3.7.** *Let $D$ be the quadratic domain and let $\phi(x)$ be the principal polynomial, of some discriminant $\Delta$. Let $p$ be a prime for which $\phi(x) \equiv 0 \pmod{p}$ has two distinct solutions, say $k$ and $-k-\varepsilon$. Suppose that $v$ is an element of $D$ that can be written in ideal form as $v = [p : k]$. Then for every positive integer $e$, we can write $v^e$ as $[p^e : k_e]$, where $k_e$ satisfies $\phi(x) \equiv 0 \pmod{p^e}$ and $k_e \equiv k \pmod{p}$.*

*Proof.* To simplify matters, we prove this proposition for $e = 2$ only. (The inductive argument is similar for all $e > 2$.) Suppose that $v = q + rz$ has ideal form $[p : k]$ in the quadratic domain $D$ of discriminant $\Delta$, so that $N(v) = p$ and $rk \equiv q \pmod{p}$. Then write

$$v^2 = \left(q^2 - \frac{\varepsilon^2 - \Delta}{4} r^2\right) + (2qr + \varepsilon r^2)z$$

as $g[c : m]$ in ideal form. Lemma 2.3.5 implies that $g$ divides $p$, but if $g = p$, then $p$ divides $2qr + \varepsilon r^2 \equiv (2k + \varepsilon)r^2 \pmod{p}$. This is impossible, since $\gcd(q, r) = 1$, and $k$ and $-k - \varepsilon$ are not congruent modulo $p$. Thus $g = 1$, and $v^2 = [p^2 : m]$ for some $m$. It follows that $m$ must satisfy $\phi(x) \equiv 0 \pmod{p^2}$, and that $m \equiv k \pmod{p}$ since $v$ divides $v^2$. □

**Exercise 2.3.6.** Find an ideal form for $v = 1 + z$ in $D_{-8}$. Use Proposition 2.3.7 to find ideal forms for $v^2$ and $v^3$. Verify that your answers are correct by calculating these powers and their ideal forms directly.

Factorization in an arbitrary quadratic domain, using ideal form for elements, requires more caution than it does in the Gaussian integers, since in general there is no obvious *sufficient* condition for $g[a : k]$ to be an ideal form for a quadratic integer. We demonstrate this fact in §2.4, and introduce a notational definition to overcome this difficulty. We then consider factorization in an arbitrary quadratic domain in §2.5 and §2.6.

## 2.4 Ideal Numbers

In Proposition 2.3.1, we saw that if a quadratic integer $v$ in $D = D_\Delta$ has ideal form $g[a : k]$, then $k$ satisfies the congruence $\phi(x) \equiv 0 \pmod{a}$, where $\phi(x)$ is the principal polynomial of discriminant $\Delta$. That is, we have a necessary condition for $g[a : k]$ to be an ideal form for some $v$ in $D$. In the Gaussian integers, we found that this condition (when we restricted $a$ to be positive) is also sufficient to ensure that $g[a : k]$ is an ideal form. But this is not the case in all quadratic domains, as the following example demonstrates.

**Example.** Let $\Delta = \Delta(-5, 1) = -20$ and let $D = D_{-20}$. The norm of an element $v = q + rz$ in $D$ is $N(v) = q^2 + 5r^2$, with $\phi(x) = x^2 + 5$ the principal polynomial of

discriminant $\Delta$. Since $a = 3$ divides $\phi(1) = 6$, we have that $[3 : 1]$ is *potentially* an ideal form for a quadratic integer in $D$. But in fact this cannot occur, since the equation $q^2 + 5r^2 = 3$ has no integer solutions. No element $v$ in $D$ can have norm $N(v) = 3$, and thus $[3 : 1]$ is not an ideal form for a quadratic integer in $D_{-20}$. $\Diamond$

In this section, we introduce the following terminology for this situation, as an alternative way of saying that $g[a : k]$ *can be*, but is *not necessarily*, an ideal form for a quadratic integer in $D_\Delta$.

**Definition.** Let $\phi(x)$ be the principal polynomial of some discriminant $\Delta$, and suppose that $a$ and $k$ are integers for which $a$ divides $\phi(k)$. If $g$ is a positive integer, we will say that an expression of the form $g[a : k]$, or $[a : k]$ when $g = 1$, is an *ideal number* of discriminant $\Delta$. If $g[a : k]$ is an ideal form for some element $v$ of $D_\Delta$, we also say that $g[a : k]$ is a *principal ideal number*. We call $g$, $a$, and $k$ the *divisor*, the *subnorm*, and the *character* of $g[a : k]$, respectively.

We view the character of $g[a : k]$ as being defined only modulo $a$. That is, we say that $g[a : k] = g[a : \ell]$ if $k \equiv \ell \pmod{a}$. By Exercise 2.2.4, we know that $\phi(-k - \varepsilon) = \phi(k)$, where $\varepsilon = \varepsilon_\Delta$ is the basis index of $\Delta$. So if $g[a : k]$ is an ideal number of discriminant $\Delta$, then $g[a : -k - \varepsilon]$ is as well. We will refer to $g[a : -k - \varepsilon]$ as the *conjugate* of $g[a : k]$. (Exercise 2.3.1 shows that this terminology is consistent for principal ideal numbers.)

**Reduction of Ideal Numbers.** In the remainder of this section, we develop a method of testing whether an ideal number $g[a : k]$ of discriminant $\Delta$ is a principal ideal number, and of determining a quadratic integer $v$ for which $g[a : k]$ is an ideal form when that is the case. Results are easier to obtain, with the methods available at this point, when $\Delta$ is a *negative* discriminant. Our starting point, similar to a result we established for Gaussian integers, applies to arbitrary discriminant values, however.

**Proposition 2.4.1.** *Let $\phi(x)$ be the principal polynomial of some discriminant $\Delta$. Let $a$ and $k$ be integers for which $a$ divides $\phi(k)$, say with $\phi(k) = ac$. Suppose that $[c : -k-\varepsilon]$ is an ideal form for some quadratic integer $w$ in $D_\Delta$. Then $v = \frac{1}{c}(k+z)w$ is an element of $D_\Delta$, and $[a : k]$ is an ideal form for $v$. Therefore, $[a : k]$ is a principal ideal number if and only if $[c : -k - \varepsilon]$ is a principal ideal number.*

*Proof.* Note that $[a : k]$ and $[c : -k-\varepsilon]$ are both ideal numbers of discriminant $\Delta$. Suppose that $[c : -k - \varepsilon]$ is an ideal form for $w = s + tz$. Then $N(w) = c$ and $(-k - \varepsilon)t \equiv s \pmod{c}$ by definition. We find that

$$(k + z)(s + tz) = \left(ks - \frac{\varepsilon^2 - \Delta}{4}t\right) + (s + (k + \varepsilon)t)z,$$

with

$$ks - \frac{\varepsilon^2 - \Delta}{4}t \equiv k(-k-\varepsilon)t - \frac{\varepsilon^2-\Delta}{4}t \equiv -\phi(k)t \equiv 0 \pmod{c}$$

and

$$s + (k+\varepsilon)t \equiv (-k-\varepsilon)t + (k+\varepsilon)t \equiv 0 \pmod{c}.$$

So $q = \frac{1}{c}\left(ks - \frac{\varepsilon^2-\Delta}{4}t\right)$ and $r = \frac{1}{c}(s + (k+\varepsilon)t)$ are integers, and

$$v = \frac{1}{c}(k+z)(s+tz) = q + rz$$

is a quadratic integer. Now since $cv = (k+z)w$, we find that $c^2 \cdot N(v) = N(k+z) \cdot N(w) = ac \cdot c$, and thus $N(v) = a$. (Here we use the observation that $N(k+z) = \phi(k,1) = \phi(k)$.) Then note that

$$kr - q = \frac{1}{c}\left(ks + (k^2+\varepsilon k)t - ks + \frac{\varepsilon^2-\Delta}{4}t\right) = \frac{1}{c}\cdot\phi(k)t = at,$$

so that $kr \equiv q \pmod{a}$. Finally, since

$$q(-t) + rs = \frac{1}{c}\left(-kst + \frac{\varepsilon^2-\Delta}{4}t^2 + s^2 + (k+\varepsilon)st\right) = \frac{1}{c}\cdot N(s+tz) = 1,$$

we must have $\gcd(q,r) = 1$. Thus $v$ has ideal form $[a : k]$.

So we see that if $[c : -k-\varepsilon]$ is a principal ideal number, then $[a : k]$ is principal as well. The converse is also true, since $\phi(-k-\varepsilon) = ca$ and $-(-k-\varepsilon)-\varepsilon = k$. Thus we could replace $[a : k]$ by $[c : -k-\varepsilon]$ in the argument above, and obtain the result that if $[a : k]$ is principal, then $[c : -k-\varepsilon]$ is also principal. □

**Example.** Let $\Delta = -20$, so that $\phi(x) = x^2 + 5$, and consider $[67 : 14]$, an ideal number of discriminant $\Delta$ since $\phi(14) = 201 = 67 \cdot 3$. Here $\phi(-14) = \phi(14)$, so that $[3 : -14]$ is also an ideal number of discriminant $\Delta$, which we can rewrite as $[3 : 1]$. We noted in a previous example that $[3 : 1]$ is not a principal ideal number when $\Delta = -20$. It follows that $[67 : 14]$ is likewise not a principal ideal number. ◊

**Example.** Again with $\Delta = -20$, consider $[89 : 23]$, an ideal number since $\phi(23) = 534 = 89 \cdot 6$. Now $[6 : -23] = [6 : 1]$ is also an ideal number, and $\phi(1) = 6 = 6 \cdot 1$. Since $[1 : -1] = [1 : 0]$ is an ideal form for $w = 1$, Proposition 2.4.1 implies that $[6 : 1]$ is an ideal form for $v = \frac{1}{1}(1+z)w = 1+z$. But now, changing notation, since $w = 1+z$ has ideal form $[6 : 1] = [6 : -23]$, then $v = \frac{1}{6}(23+z)(1+z) = \frac{1}{6}(18+24z) = 3+4z$ is an element of $D_{-20}$ with ideal form $[89 : 23]$. ◊

The preceding examples illustrate an approach in which a given ideal number $[a : k]$ is replaced by ideal numbers with successively smaller subnorms. If

we eventually obtain a principal ideal number (in particular, $[1 : 0]$), then the original ideal number is principal, and we can construct a quadratic integer $v$ with ideal form $[a : k]$. If we obtain an ideal number that we know is not principal, then $[a : k]$ is also not a principal ideal number. In Theorem 2.4.3, we develop this idea into a *reduction algorithm* that applies to an arbitrary negative discriminant.

**Theorem 2.4.2.** *Let $\phi(x)$ be the principal polynomial of some negative discriminant $\Delta$, and let $u = u_\Delta = \left\lfloor \sqrt{-\Delta/3} \right\rfloor$. If $1 < a \le u$, and $k$ is a solution of $\phi(x) \equiv 0 \pmod{a}$, then $[a : k]$ is an ideal number that is not principal. On the other hand, if there is no integer $a$ with $1 < a \le u$ for which $\phi(x) \equiv 0 \pmod{a}$ has a solution, then every ideal number $[a : k]$ of discriminant $\Delta$ with $a > 0$ is a principal ideal number.*

We refer to $u_\Delta = \left\lfloor \sqrt{-\Delta/3} \right\rfloor$ as the *upper bound* of the negative discriminant $\Delta$. We define a similar upper bound for positive discriminants in §10.1.

*Proof.* Suppose first that $k$ is a solution of $\phi(x) \equiv 0 \pmod{a}$ for some $a$ with $1 < a \le u$. If $[a : k]$ were an ideal form for an element $v = q + rz$ in $D_\Delta$, then we would have

$$N(v) = q^2 + \varepsilon qr + \frac{\varepsilon^2 - \Delta}{4} r^2 = \frac{(2q + \varepsilon r)^2 - \Delta r^2}{4} = a.$$

This implies, since $2 \le a$ and $a^2 \le -\frac{\Delta}{3}$, that

$$-\Delta r^2 \le (2q + \varepsilon r)^2 - \Delta r^2 = 4a \le 2a^2 \le -\frac{2\Delta}{3}.$$

With $-\Delta > 0$ it follows that $r$ must equal 0. But then $q = \pm 1$ since $v$ is primitive, and we conclude that $a = 1$, contrary to assumption. So $[a : k]$ cannot be a principal ideal number.

Conversely, suppose that there is no integer $a$ with $1 < a \le u$ for which $\phi(x) \equiv 0 \pmod{a}$ has a solution, but that there is an ideal number $[a : k]$ of discriminant $\Delta$ with $a > 0$ that is not principal. There must be a smallest positive integer $a$ so that $[a : k]$ is an ideal number for some $k$, but not principal. Note that $a > 1$, since $[1 : 0]$ is the only distinct ideal number with subnorm 1, and we have seen that $[1 : 0]$ is an ideal form for $v = 1$. Furthermore, since the character of $[a : k]$ is defined only modulo $a$, we can assume that $-a < 2k + \varepsilon \le a$, that is, $\frac{-a-\varepsilon}{2} < k \le \frac{a-\varepsilon}{2}$. (This range of values for $k$ contains a representative of each congruence class modulo $a$.)

Now $\phi(k) = ac$ for some $c$. If $c$ is smaller than $a$, then $[c : -k - \varepsilon]$ is a principal ideal number by assumption. But then $[a : k]$ is also principal by Proposition 2.4.1. Therefore $c \ge a$, and then $\phi(k) = ac \ge a^2$. But on the other

hand,

$$\phi(k) = k^2 + \varepsilon k + \frac{\varepsilon^2 - \Delta}{4} = \frac{(2k+\varepsilon)^2 - \Delta}{4} \leq \frac{a^2 - \Delta}{4}.$$

So now $a^2 \leq \phi(k) \leq \frac{a^2-\Delta}{4}$, which on solving for $a$ implies that $a \leq u$. But this is contrary to our assumption, so in fact every ideal number of discriminant $\Delta$ must be a principal ideal number. □

**Example.** Notice that if $\Delta$ is a discriminant with $-12 < \Delta < 0$, then $u = \left\lfloor \sqrt{-\Delta/3} \right\rfloor = 1$. So in that case there is no $a$ with $1 < a \leq u$ for which $\phi(x) \equiv 0 \pmod{a}$ has a solution. Therefore, every ideal number $g[a : k]$ of discriminant $\Delta = -3, -4, -7, -8$, or $-11$, with $a$ positive, is principal. ♢

**Example.** If $\Delta = -19$, then $u_\Delta = 2$. Here $\phi(x) = x^2 + x + 5$ is odd for all $x$, so there is no solution of $\phi(x) \equiv 0 \pmod{2}$. We conclude that every ideal number $g[a : k]$ of discriminant $\Delta = -19$, with $a$ positive, is principal. ♢

**Example.** If $\Delta = -23$, then $u_\Delta = 2$, but $\phi(x) = x^2 + x + 6$ is even for all $x$. Since $\phi(x) \equiv 0 \pmod{2}$ has distinct solutions 0 and $-1$ (among other possible representatives), we can say that $[2 : 0]$ and $[2 : -1]$ are ideal numbers of discriminant $\Delta = -23$ that are not principal. ♢

When $g[a : k]$ is a principal ideal number of some discriminant $\Delta$, then $g[a : k]$ is an ideal form for some element $v$ in $D_\Delta$. We conclude this section with a method by which we can find such an element $v$, or determine that $g[a : k]$ is not in fact principal.

**Theorem 2.4.3.** *Let $\Delta$ be a negative discriminant, with basis element $z$ and basis index $\varepsilon$ defined as in equation (2.2.2). Let $\phi(x)$ be the principal polynomial of discriminant $\Delta$, and let $u$ be the upper bound of $\Delta$. Let $a > 1$ be an integer, and let $k$ be an integer with $\frac{-a-\varepsilon}{2} < k \leq \frac{a-\varepsilon}{2}$ for which $a$ divides $\phi(k)$. Define sequences $a_i$ and $k_i$ recursively for $i \geq 0$ as follows. Let $a_0 = a$ and $k_0 = k$, and for $i \geq 0$, let $a_{i+1} = \frac{1}{a_i} \cdot \phi(k_i)$ and select $k_{i+1}$ so that $k_{i+1} \equiv -k_i - \varepsilon \pmod{a_{i+1}}$ with $\frac{-a-\varepsilon}{2} < k_{i+1} \leq \frac{a-\varepsilon}{2}$. Then there is a smallest integer $n \geq 0$ so that $a_n \leq u$. If $a_n = 1$, then $[a : k]$ is an ideal form for a quadratic integer $v$ in $D_\Delta$ given by*

$$v = \frac{1}{a_1} \cdot (k_0 + z) \cdot \frac{1}{a_2} \cdot (k_1 + z) \cdots \frac{1}{a_n} \cdot (k_{n-1} + z). \tag{2.4.1}$$

*If $1 < a_n \leq u$, then $[a : k]$ is not a principal ideal number.*

*Proof.* In the proof of Theorem 2.4.2, we found that if $\phi(k) = ac$ with $\frac{-a-\varepsilon}{2} < k \leq \frac{a-\varepsilon}{2}$ and $a \leq c$, then $1 \leq a \leq u$. So we must have $a_n \leq u$ for some $n$, since

otherwise $a_i$ is a strictly decreasing infinite sequence of positive integers, which is impossible. If $1 < a_n \leq u$, then $[a_n : k_n]$ is not principal by Theorem 2.4.2, and repeated application of Proposition 2.4.1 shows that $[a : k]$ is not a principal ideal number. If $a_n = 1$, then Proposition 2.4.1 implies that $[a_{n-1} : k_{n-1}]$ is an ideal form for $v_{n-1} = \frac{1}{a_n} \cdot (k_{n-1} + z) \cdot 1$, and then $[a_{n-2} : k_{n-2}]$ is an ideal form for

$$v_{n-2} = \frac{1}{a_{n-1}} \cdot (k_{n-2} + z) \cdot v_{n-1} = \frac{1}{a_{n-1}} \cdot (k_{n-2} + z) \cdot \frac{1}{a_n} \cdot (k_{n-1} + z),$$

and so forth, eventually obtaining $[a : k]$ as an ideal form for $v$ as given in equation (2.4.1). □

**Example.** Let $\Delta = -79$, so that $z = \frac{-1+\sqrt{-79}}{2}$ and $\phi(x) = x^2 + x + 20$. We find that $[83 : 40]$ is an ideal number of discriminant $-79$ since $\phi(40) = 1660 = 83 \cdot 20$. Following the algorithm of Theorem 2.4.3, if $a_0 = 83$ and $k_0 = 40$, then $a_1 = \frac{1}{83} \cdot \phi(40) = 20$, and $k \equiv -40 - 1 \equiv -1 \pmod{20}$. Now we find that $\phi(-1) = 20 \cdot 1$, and conclude that $[83 : 40]$ is a principal ideal number. Specifically, $[83 : 40]$ is an ideal form for

$$v = \frac{1}{20} \cdot (40 + z) \cdot \frac{1}{1} \cdot (-1 + z) = \frac{1}{20} \cdot (-60 + 40z) = -3 + 2z,$$

here using the fact that $z^2 = -20 + z$ by equation (2.2.8). ◊

**Example.** Again let $\Delta = -79$, so that $\phi(x) = x^2 + x + 20$. We find that $-79 \equiv 1 \pmod{8}$, $\left(\frac{-79}{5}\right) = \left(\frac{1}{5}\right) = 1$, and $\left(\frac{-79}{11}\right) = \left(\frac{9}{11}\right) = 1$, and so $\phi(x) \equiv 0 \pmod{p}$ has two solutions each for $p = 2$, 5, and 11. Applying the Chinese Remainder Theorem, we find that there are eight ideal numbers of discriminant $-79$ having subnorm $110 = 2 \cdot 5 \cdot 11$, namely the following ideal numbers and their conjugates:

$$[110 : 9], \qquad [110 : 20], \qquad [110 : 34], \qquad [110 : 45].$$

Since $\phi(9) = 110 \cdot 1$, we immediately find that $[110 : 9]$ is an ideal form for $9 + z$. On the other hand, $\phi(20) = 440 = 110 \cdot 4$, so that $[110 : 20]$ is a principal ideal number if and only if $[4 : -21] = [4 : -1]$ is as well. But $4 < u_{-79} = 5$, so in fact $[110 : 20]$ is not an ideal form for any element of $D_{-79}$. We leave it to the reader to verify that the same is true for $[110 : 34]$ and $[110 : 45]$. ◊

**Exercise 2.4.1.** In each part, verify that $[a : k]$ is an ideal number of the given discriminant $\Delta$, and apply the algorithm of Theorem 2.4.3 to determine whether $[a : k]$ is a principal ideal number. If so, find an element $v$ of $D_\Delta$ having ideal form $[a : k]$.

(a) $[a : k] = [121 : 19]$, $\quad \Delta = -8$.

(b) $[a : k] = [111 : 23]$, $\Delta = -11$.

(c) $[a : k] = [94 : -10]$, $\Delta = -15$.

(d) $[a : k] = [94 : 37]$, $\Delta = -15$.

(e) $[a : k] = [123 : 47]$, $\Delta = -20$.

(f) $[a : k] = [129 : 52]$, $\Delta = -20$.

(g) $[a : k] = [246 : 15]$, $\Delta = -23$.

(h) $[a : k] = [246 : 56]$, $\Delta = -23$.

(i) $[a : k] = [246 : 66]$, $\Delta = -23$.

(j) $[a : k] = [246 : 107]$, $\Delta = -23$.

## 2.5 Quadratic Domains with Unique Factorization

We saw in Proposition 2.2.7 that if $D = D_\Delta$ is a quadratic domain, then every element that is neither zero nor a unit can be written as a product of irreducible elements of $D$. In the domain of Gaussian integers, $D_{-4} = \mathbb{Z}[i]$, we found that this factorization is unique and we used that fact to draw conclusions about representations of integers by $x^2 + y^2$. We now establish some other examples of quadratic domains with unique factorization, leading to similar arithmetic results. We first review some standard terminology.

**Definition.** A quadratic domain $D = D_\Delta$ is a *unique factorization domain* if every element $w$ that is neither zero nor a unit can be written uniquely, aside from order and unit multiples, as a product of irreducible elements of $D$. That is, if $w = u_1 \cdot u_2 \cdots u_k$ and $w = v_1 \cdot v_2 \cdots v_\ell$ with each $u_i$ and $v_i$ irreducible, then $k = \ell$, and we can rearrange the factors so that $u_i$ is an associate of $v_i$ for $1 \le i \le k$.

**Definition.** Let $w$ be an element of a quadratic domain $D$ that is neither zero nor a unit. We say that $w$ is *prime* in $D$ if whenever $w$ divides a product $uv$ of elements of $D$, then $w$ divides $u$ or $w$ divides $v$ (or both).

**Exercise 2.5.1.** Show that every prime element $w$ of a quadratic domain is irreducible. (Hint: Note that if $w = uv$, then $w$ divides $uv$.)

The converse of the claim of Exercise 2.5.1 is not always true. In fact, the following two exercises show that for quadratic domains, this property is equivalent to unique irreducible factorization.

**Exercise 2.5.2.** Let $D$ be a quadratic domain. Show that if every irreducible element of $D$ is prime, then $D$ is a unique factorization domain. (Hint: Use the approach of Exercise 1.2.10.)

**Exercise 2.5.3.** Let $D$ be a quadratic domain. Show that if $D$ is a unique factorization domain, then every irreducible element of $D$ is prime. (Hint: Let $w$ be irreducible and suppose that $w$ divides $uv$. Show that if $w$ divides neither $u$ nor $v$, then $uv$ has two distinct irreducible factorizations.)

In this section, we connect unique factorization to a property that we saw in §2.4 holds for some discriminants $\Delta$.

**Definition.** Let $D$ be the quadratic domain and $\phi(x)$ the principal polynomial of some discriminant $\Delta$. We say that $D$ is a *principal ideal number domain* if it has the following property: for every pair of integers $a$ and $k$ for which $a$ divides $\phi(k)$, either $[a : k]$ or $[-a : k]$ (or both) is a principal ideal number, that is, an ideal form for some element of $D$.

Note that when $\Delta$ is negative, then $[a : k]$ can be a principal ideal number only when $a$ is positive. Our definition allows us to consider positive discriminants as well. We will see in §3.2 that for quadratic domains this definition is equivalent to the more standard one of a *principal ideal domain*.

**Classification of Irreducible Elements.** When $D = D_\Delta$ is a principal ideal number domain, we can show that every irreducible element of $D$ is prime, and thus that $D$ is a unique factorization domain. We begin by classifying all irreducible elements of $D$ in ideal form as follows.

**Proposition 2.5.1.** *Let $D$ be the quadratic domain and $\phi(x)$ the principal polynomial of some discriminant $\Delta$, and suppose that $D$ is a principal ideal number domain. Let $p$ be a rational prime. Then the following statements are true.*

(1) *If $\phi(x) \equiv 0 \pmod{p}$ has no solutions, then $p$ is irreducible in $D$.*

(2) *If $\phi(x) \equiv 0 \pmod{p}$ has two distinct solutions, $k$ and $-k-\varepsilon$, then $[p : k]$ and $[p : -k-\varepsilon]$, or $[-p : k]$ and $[-p : -k-\varepsilon]$, are ideal forms for distinct irreducible elements $w$ and $\overline{w}$ of $D$ for which $w \cdot \overline{w} = p$.*

(3) *If $\phi(x) \equiv 0 \pmod{p}$ has a unique solution $k$, then $[p : k]$ or $[-p : k]$ is an ideal form for an irreducible element $w$ of $D$ for which $w^2$ is an associate of $p$.*

*Every irreducible element of $D$ can be expressed in one of these ways.*

**Example.** Let $\Delta = -8$, so that $\phi(x) = x^2 + 2$ and $z = \sqrt{-2}$ in $D = D_{-8}$. We saw in §2.4 that every ideal number of discriminant $-8$ is principal. If $p = 2$, then

$\phi(x) \equiv 0 \pmod{p}$ has just one solution—we find that $[2 : 0]$ is an ideal form for $w = z$, and $w^2 = -2$ is an associate of $p = 2$. If $p$ is an odd prime, then $\phi(x) \equiv 0 \pmod{p}$ has solutions if and only if $\left(\frac{-8}{p}\right) = \left(\frac{-2}{p}\right) = 1$. Using results from §0.2,

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \text{ or } 3 \pmod 8, \\ -1, & \text{if } p \equiv 5 \text{ or } 7 \pmod 8. \end{cases}$$

For instance, $x^2 + 2 \equiv 0 \pmod{43}$ has solutions $k = 16$ and $-k = -16$. So $[43 : 16]$ and $[43 : -16]$ are ideal forms for irreducible elements $w$ and $\overline{w}$ of $D$. Applying the reduction algorithm of Theorem 2.4.3, we can let $w = 5 + 3z$ and $\overline{w} = 5 - 3z$. On the other hand, 47 is irreducible in $D$. ◊

*Proof.* Let $p$ be a rational prime and note that $N(p) = p^2$ in $D$. If $\phi(x) \equiv 0 \pmod{p}$ has no solutions, then $D$ has no elements of norm $p$, and we conclude that $p$ is irreducible in $D$ by Proposition 2.2.6. On the other hand, if $\phi(k) \equiv 0 \pmod{p}$, then $\phi(-k - \varepsilon) \equiv 0 \pmod{p}$ as well. If $D_\Delta$ is a principal ideal number domain, then there are conjugate elements $w$ and $\overline{w}$ in $D$ having ideal forms $[p : k]$ and $[p : -k - \varepsilon]$, or $[-p : k]$ and $[-p : -k - \varepsilon]$, respectively. Here $N(w) = w \cdot \overline{w} = p = N(\overline{w})$, so $w$ and $\overline{w}$ are both irreducible in $D$, again by Proposition 2.2.6. If $k \equiv -k - \varepsilon \pmod{p}$, which is the case if and only if $\phi(x) \equiv 0 \pmod{p}$ has just one solution, then $w$ and $\overline{w}$ are associate elements, and $w^2$ is an associate of $w \cdot \overline{w} = p$.

Now suppose that $w$ is an irreducible element of $D$, written as $g[a : k]$ in ideal form. Then either $g = 1$ or $a = \pm 1$ since otherwise $w$ is written as a product of elements of $D$, neither of which is a unit. If $a = \pm 1$, then $w$ is an associate of a positive rational integer. That integer must be prime, since if $w$ factors in $\mathbb{Z}$ it also has a nontrivial factorization in $D$. If $w = p$, we find that $\phi(x) \equiv 0 \pmod{p}$ cannot have a solution—if $k$ were such a solution, then $[p : k]$ or $[-p : k]$ would be an ideal form for an element of $D$ that divides $p$, as noted above, but is neither a unit nor an associate of $p$.

On the other hand, suppose that $g = 1$. Here $a \neq \pm 1$ since $w$ is not a unit, so $a$ must have a prime divisor, say $a = pq$ with $p$ prime. Now $k$ satisfies $\phi(x) \equiv 0 \pmod{a}$ by Proposition 2.3.1, so must satisfy $\phi(x) \equiv 0 \pmod{p}$. We conclude that $[p : k]$ is an ideal form for an element $v$ of $D$ that divides $w$, by Theorem 2.3.3. If $w$ is irreducible in $D$, we must have that $v$ is an associate of $w$, and so $q = 1$. So the only irreducible elements of $D$ are as given in statements (1)–(3). □

**Theorem 2.5.2.** *If $D = D_\Delta$ is a principal ideal number domain, then $D$ is a unique factorization domain.*

*Proof.* It suffices to show that every irreducible element of $D = D_\Delta$, as categorized in Proposition 2.5.1, is prime. Suppose first that $w$ has ideal form $[\pm p : k]$

for some rational prime $p$, and that $w$ divides some product

$$uv = (q + rz)(s + tz) = \left(qs - \frac{\varepsilon^2 - \Delta}{4}rt\right) + (qt + rs + \varepsilon rt)\, z = m + nz$$

in $D$ (here using equation (2.2.8)). By Lemma 2.3.2, this occurs if and only if $nk \equiv m \pmod{p}$. But we find that

$$\begin{aligned} nk - m &= (qtk + rsk + \varepsilon rtk) - \left(qs - \frac{\varepsilon^2 - \Delta}{4}rt\right) \\ &= (-rtk^2 + qtk + rsk - qs) + \left(k^2 + \varepsilon k + \frac{\varepsilon^2 - \Delta}{4}\right) rt \\ &= -(rk - q)(tk - s) + \phi(k)rt. \end{aligned}$$

We conclude that $p$ divides $(rk - q)(tk - s)$ since $p$ divides $\phi(k)$ by Proposition 2.3.1. With $p$ a rational prime, then either $rk \equiv q \pmod{p}$ or $tk \equiv s \pmod{p}$. But then $w$ divides either $u = q+rz$ or $v = s+tz$, again by Lemma 2.3.2. Thus $w$ is a prime element of $D$.

Now suppose that a rational prime $p$ is irreducible in $D$, and that $p$ divides a product $uv$ in $D$. We may assume that $u$ and $v$ are primitive, say with ideal forms $[a : k]$ and $[b : \ell]$, respectively, and that $uv$ has ideal form $g[c : m]$. Applying Theorem 2.3.3, then $p$, which has ideal form $p[1 : 0]$, divides $g$. But Lemma 2.3.5 shows that $g$ is a common divisor of $a$ and $b$. Since $k$ is a solution of $\phi(x) \equiv 0 \pmod{a}$, and thus of $\phi(x) \equiv 0 \pmod{p}$, this contradicts the assumption that $p$ is irreducible in $D$. So in fact $p$ must be prime in $D$, and every irreducible element of $D$ is prime. □

**Consequences of Unique Factorization.** We conclude this section with some general statements and examples that illustrate the importance of unique irreducible factorization in a quadratic domain, when that property occurs. We begin with some standard terminology related to the possibilities noted in Proposition 2.5.1. (Here we use the Kronecker symbol, defined as in §0.3, when $p = 2$.)

**Definition.** Let $D = D_\Delta$ be a principal ideal number domain, and let $p$ be a rational prime.

(1) If $p$ is irreducible in $D$, we say that $p$ is *inert* in $D$. This case occurs if $\left(\frac{\Delta}{p}\right) = -1$.

(2) If $p$ is a product of distinct irreducible elements of $D$, we say that $p$ *splits* in $D$. This case occurs if $\left(\frac{\Delta}{p}\right) = 1$.

(3) If $p$ is an associate of the square of an irreducible element in $D$, we say that $p$ is *ramified* in $D$. This case occurs if $\left(\frac{\Delta}{p}\right) = 0$.

The term "ramified" is a reference to branching, or in this case to branches coming together, with the two factors of $p$ that exist when $p$ splits being the same for a ramified prime.

If $D_\Delta$ is a principal ideal number domain, we can connect the factorization of a rational integer $a$ to representations of $a$ by a particular function of two variables, namely the principal form $\phi(x, y)$ of discriminant $\Delta$, defined as in equation (2.2.6). We say that $\phi$ *represents* an integer $a$ if $\phi(q, r) = a$ for some integers $q$ and $r$, and that $\phi$ *properly represents* $a$ if $\phi(q, r) = a$ with $\gcd(q, r) = 1$.

**Theorem 2.5.3.** *Let $\Delta$ be an integer for which $D = D_\Delta$ is a principal ideal number domain, and let $\phi(x, y)$ be the principal form of discriminant $\Delta$. If $a$ is a positive integer, then $a$ is properly represented by $\phi(x, y)$ if and only if $a$ is not divisible by any prime $p$ that is inert in $D$ nor by the square of any prime $p$ that is ramified in $D$.*

*Proof.* Recall that if $v = q + rz$ in $D$, then $N(v) = \phi(q, r)$. In this case, $\phi$ represents $a$ if and only if $a = v \cdot \overline{v}$, and this representation is proper if and only if $v$ is *primitive*, that is, not divisible by any rational prime. Assuming that $D$ is a principal ideal number domain, and so a unique factorization domain, then the irreducible factorizations of $a$ and of $v \cdot \overline{v}$ must be the same, and if $u$ is an irreducible factor of $v$, then $\overline{u}$ is a factor of $\overline{v}$. Let

$$a = q_1 \cdots q_j \cdot p_1^{e_1} \cdot p_2^{e_2} \cdots p_\ell^{e_\ell},$$

with each $q_i$ a distinct ramified prime, so that $q_i$ is (an associate of) $w_i^2$ for some irreducible $w_i$ in $D$, and with each $p_i$ a prime that splits as $p_i = v_i \cdot \overline{v_i}$ in $D$. Then we find that $a = v \cdot \overline{v}$, where $v = w_1 \cdots w_j \cdot v_1^{e_1} \cdot v_2^{e_2} \cdots v_\ell^{e_\ell}$. Here the uniqueness of irreducible factorization shows that $v$ is primitive. (For example, $v$ cannot be divisible by $p_1 = v_1 \cdot \overline{v_1}$, since $\overline{v_1}$ is not part of this factorization.) So $a$ has a proper representation by $\phi(x, y)$ in this case. On the other hand, if $a$ is divisible by the square of a ramified prime, say $q_1^2$, then in any product $a = v \cdot \overline{v}$, we must have $v$ and $\overline{v}$ divisible by $w_1^2 = q_1$, so that $v$ is not primitive. Likewise, if $a$ is divisible by an inert prime $p$ and $a = v \cdot \overline{v}$, then $p = \overline{p}$ must divide both $v$ and $\overline{v}$. □

We note an application of this theorem as a corollary of Theorem 2.5.3, with other examples appearing as exercises.

**Corollary 2.5.4.** *Let $\phi(x, y) = x^2 + xy + 2y^2$, the principal form of discriminant $\Delta = -7$. Then a positive integer $a$ is properly represented by $\phi$ if and only if $a$ is not divisible by* 49 *or any prime $p \equiv 3, 5, 6 \pmod 7$. The same values of $a$ are properly represented by $x^2 + 7y^2$ if and only if we have the additional condition that $a$ is odd or divisible by* 8.

*Proof.* We saw in §2.4 that every ideal number $[a : k]$, with $a$ positive, of discriminant $\Delta = -7$ is principal. So $D = D_{-7}$ is a unique factorization domain by

Theorem 2.5.2. The only ramified prime in $D$ is $p = 7$. By Exercise 0.2.7, we have $\left(\frac{-7}{p}\right) = \left(\frac{p}{7}\right)$ for every odd prime $p \neq 7$, since $7 \equiv 3 \pmod 4$. Thus $p$ splits in $D$ if $p \equiv 1, 2, \text{ or } 4 \pmod 7$ (since $-7 \equiv 1 \pmod 8$, this includes $p = 2$), while $p$ is inert in $D$ if $p \equiv 3, 5, \text{ or } 6 \pmod 7$. The first claim of this corollary is now a direct application of Theorem 2.5.3.

To establish the second claim, it will suffice to show that if $a$ is odd, then $a$ is properly represented by $x^2 + xy + 2y^2$ if and only if $a$ is properly represented by $x^2 + 7y^2$, while if $a$ is even, then $a$ is properly represented by $x^2 + xy + 2y^2$ if and only if $4a$ is properly represented by $x^2 + 7y^2$.

Suppose first that $a = q^2 + qr + 2r^2$ with $\gcd(q, r) = 1$. If $r$ is even, so that $q$ is odd, then $a$ is odd. On the other hand, if $r$ is odd, we find that $a$ is even, independent of the parity of $q$. Now notice that $4a = 4q^2 + 4qr + 8r^2 = (2q + r)^2 + 7r^2$. If $r$ is odd, we find that $\gcd(2q + r, r) = 1$, and we have a proper representation of $4a$ by $x^2 + 7y^2$. On the other hand, if $r$ is even, then $a = \left(q + \frac{r}{2}\right)^2 + 7\left(\frac{r}{2}\right)^2$, and we have a proper representation of $a$ by $x^2 + 7y^2$.

Now suppose that $a = q^2 + 7r^2$ with $\gcd(q, r) = 1$. If $q$ and $r$ have opposite parity, then $a$ is odd, while if $q$ and $r$ are both odd, so that $q^2 \equiv r^2 \equiv 1 \pmod 8$, then 8 divides $a$. Note that

$$(q - r)^2 + (q - r) \cdot 2r + (2r)^2 = q^2 - 2qr + r^2 + 2qr - 2r^2 + 8r^2 = q^2 + 7r^2.$$

Here $\gcd(q - r, 2r) = 1$ if $q - r$ is odd, while $\gcd(q - r, 2r) = 2$ if $q - r$ is even. So if $q$ and $r$ have opposite parity, the pair $(q - r, 2r)$ gives us a proper representation of $m$ by $x^2 + xy + 2y^2$. On the other hand, if $q$ and $r$ are both odd, $\left(\frac{q-r}{2}, r\right)$ is a proper representation of $\frac{m}{4}$ by $x^2 + xy + 2y^2$. □

**Exercise 2.5.4.** Show that a positive integer $a$ is properly represented by $x^2 + 2y^2$ if and only if $a$ is not divisible by 4 or by any prime congruent to 5 or 7 modulo 8.

**Exercise 2.5.5.** Show that a positive integer $a$ is properly represented by $x^2 + xy + y^2$ if and only if $a$ is not divisible by 9 or any prime $p \equiv 2 \pmod 3$.

**Exercise 2.5.6.** Let $\phi(x, y) = x^2 + xy + y^2$. Show that if $\phi(q, r) = a$, then we also have $\phi(-r, q + r) = a$ and $\phi(-q - r, q) = a$.

**Exercise 2.5.7.** Show that every positive integer $a$ that is properly represented by $\phi(x, y) = x^2 + xy + y^2$ is also properly represented by $x^2 + 3y^2$. (Hint: Show that if $\phi(q, r) = a$ with $r$ even, then $\left(q + \frac{r}{2}\right)^2 + 3\left(\frac{r}{2}\right)^2 = a$. Use Exercise 2.5.6 to explain why we can assume that $r$ is even.)

## 2.6 Quadratic Domains without Unique Factorization

In §2.5, we saw that if $\Delta$ is a discriminant for which $D = D_\Delta$ is a principal ideal number domain, then $D$ is a unique factorization domain. But we know from §2.4 that there are examples of ideal numbers of certain discriminants that are not principal. When this occurs, the following condition implies that $D$ is not a unique factorization domain.

**Proposition 2.6.1.** *Let $\Delta$ be a discriminant. Suppose that there is a rational prime $p$ and an integer $k$ so that $[p : k]$ is an ideal number of discriminant $\Delta$, but neither $[p : k]$ nor $[-p : k]$ is a principal ideal number. Then $p$ is an irreducible element of $D = D_\Delta$, but is not prime in $D$. Therefore, $D$ is not a unique factorization domain.*

*Proof.* Assume that $\phi(x) \equiv 0 \pmod{p}$ has a solution $k$, where $\phi(x)$ is the principal polynomial of discriminant $\Delta$. Note that $[\pm p : k]$ is an ideal form for some $w$ in $D$ if and only if $[\pm p : -k-\varepsilon]$ is an ideal form for $\overline{w}$. Since $\phi(x) \equiv 0 \pmod{p}$ has at most two solutions, it follows that if neither $[p : k]$ nor $[-p : k]$ is an ideal form for an element of $D$, then $D$ has no elements of norm $p$. With $N(p) = p^2$, then $p$ is irreducible in $D$ by Proposition 2.2.6.

But now note that $\phi(k) = N(k + z) = (k + z)(k + \overline{z})$ in $D$. Here $p$ divides this product, since it is given that $p$ divides $\phi(k)$. But $p$ divides neither $k + z$ nor $k + \overline{z}$, since both of those elements are primitive in $D$. Thus $p$ is not prime in $D$, and we conclude as in Exercise 2.5.3 that $D$ cannot be a unique factorization domain. □

We can use the method of this proof to construct examples of irreducible factorization in $D_\Delta$ that are not unique, as we illustrate below.

**Example.** Let $D$ be the quadratic domain of discriminant $\Delta = -20$, so that $z = \sqrt{-5}$, the norm of a typical element of $D$ is $N(q+rz) = q^2+5r^2$, and the principal polynomial of discriminant $-20$ is $\phi(x) = x^2 + 5$. Since $p = 3$ divides $\phi(1) = 6$, we have that $[3 : 1]$ is an ideal number of discriminant $-20$. But we have seen that $[3 : 1]$ is not principal since there is no element $q + rz$ in $D$ for which $N(q + rz) = 3$. So Proposition 2.6.1 shows that $p = 3$ is irreducible, but not prime, in $D$. Specifically, $p$ divides $\phi(1) = N(1 + z) = (1 + z)(1 + \overline{z}) = 6$, but divides neither $1 + z$ nor $1 + \overline{z} = 1 - z$. In fact, all factors in the equation

$$2 \cdot 3 = (1 + z)(1 - z)$$

are irreducible in $D$, by Proposition 2.2.6, since there are no rational integers $q$ and $r$ for which $q^2 + 5r^2$ equals 2 or 3. The only units in $D = D_{-20}$ are $\pm 1$, by Proposition 2.2.5, so no two of these factors are associates. Thus we have two essentially different irreducible factorizations of the same element. ◊

In quadratic domains with unique factorization, we saw that every irreducible element is obtained as a factor of some rational prime. This example illustrates that the same is not generally true in a quadratic domain without unique factorization. Here $v = 1 + z$ is irreducible in $D = D_{-20}$, but $v$ does not divide a rational prime, since $N(v) = 6$ does not divide $N(p) = p^2$ for any prime $p$ in $\mathbb{Z}$.

When $\Delta$ is negative, it is quite rare for the quadratic domain $D = D_\Delta$ to have the unique factorization property. In fact, it is known that $D$ is a unique factorization domain if and only if $\Delta$ is one of the following: $-3, -4, -7, -8, -11, -19, -43, -67$, or $-163$. This fact was conjectured by Gauss—the first accepted proofs were given independently by Baker and Stark in 1966. When $\Delta$ is positive, there are many more examples of quadratic domains with unique factorization. But even then, it is not known whether there are infinitely many such cases.

**Exercise 2.6.1.** For each value of $\Delta$ below, find an ideal number of the form $[p : k]$ with $p$ prime that is not a principal ideal number. In each case, use the method of Proposition 2.6.1 to construct two distinct irreducible factorizations of some element of $D_\Delta$.

(a) $\Delta = -24$.

(b) $\Delta = -40$.

(c) $\Delta = -52$.

**Factorization with Ideal Numbers.** The preceding claim indicates that there are many examples of quadratic domains that lack the property of unique irreducible factorization. In the remainder of this section, we will illustrate how we might be able to attain uniqueness by introducing additional potential factors to the elements of our domain. We begin with an example, which we previously encountered in the Preface, where we can describe these additional factors concretely as quadratic integers.

**Example.** Let $D$ and $D'$ be the quadratic domains of discriminant $\Delta = \Delta(-7, 1) = -7$ and $\Delta' = \Delta(-7, 2) = -28$, respectively. In this case, $D'$ is a subdomain of the complete quadratic domain $D$. (To simplify notation in this example, we will write the typical element of $D'$ as $q + r\sqrt{-7}$ with $q$ and $r$ integers, while $D = \{q + rz \mid q, r \in \mathbb{Z}\}$ with $z = \frac{1+\sqrt{-7}}{2}$.) We find that $D'$ is not a unique factorization domain. For instance, we can factor 8 in $D'$ in the following distinct ways:

$$(1 + \sqrt{-7})(1 - \sqrt{-7}) = 8 = 2 \cdot 2 \cdot 2. \tag{2.6.1}$$

Here we know that $w = 1 + \sqrt{-7}$ is irreducible in $D'$ because if $w = uv$ with neither $u$ nor $v$ a unit in $D'$, we are led to the conclusion that $x^2 + 7y^2 = 2$ has a

solution, which is impossible. Each other factor is shown to be irreducible in $D'$ in a similar way.

But if we consider equation (2.6.1) in the larger domain $D$, we see that each term factors further. Specifically, $2 = z(1-z)$, while $1+\sqrt{-7} = 2z = z^2(1-z)$ and $1-\sqrt{-7} = 2-2z = z(1-z)^2$. So equation (2.6.1) merely presents different arrangements of the same irreducible factors in $D$:

$$(1+\sqrt{-7})(1-\sqrt{-7}) = z^2(1-z)\cdot z(1-z)^2 = z(1-z)\cdot z(1-z)\cdot z(1-z) = 2\cdot 2\cdot 2.$$

In this case, $D$ is a unique factorization domain, and other examples of distinct irreducible factorization in $D'$ can be resolved in a similar way with elements of the larger domain $D$. ◊

However, a complete quadratic domain $D$ might itself fail to be a unique factorization domain. To conclude Chapter 2, we illustrate how *ideal numbers*, in particular, ideal numbers that are not principal, can be viewed as the additional objects that appear to restore unique factorization in an arbitrary quadratic domain $D_\Delta$. (The concept of ideal numbers is superseded by definitions and results that we introduce in Chapter 3. We will view the remainder of this section as motivation for that more precise development, and thus will not provide proofs of our claims.)

To illustrate the idea, we look more closely at an example in which we have seen different irreducible factorizations of the same element.

**Example.** Let $D = D_{-20}$, so that $z = \sqrt{-5}$ and $\phi(x) = x^2 + 5$. Ideal numbers of discriminant $\Delta = -20$ have the form $[a : k]$ (or more generally $g[a : k]$), where $k$ satisfies $\phi(x) \equiv 0 \pmod{a}$. For any particular $a$, we can assume that $-\frac{a}{2} < k \leq \frac{a}{2}$. Notice that to determine *all* ideal numbers $[a : k]$ for $a$ smaller than some arbitrary upper bound $u$, we might begin then by calculating $\phi(x)$ for $-\frac{u}{2} < x \leq \frac{u}{2}$. The fact that $\phi(-x) = \phi(x)$ reduces our computations. For instance, to find all primitive ideal numbers with subnorm $a \leq 50$, as in Table 2.1, it suffices to calculate $\phi(x)$ for $0 \leq x \leq 25$.

We have seen that not every $[a : k]$ is actually the ideal form of an element of $D$, that is, not every ideal number is principal. But the reduction algorithm of Theorem 2.4.3 shows that each ideal number reduces to $[1 : 0]$ or $[2 : 1]$. An ideal number that reduces to $[1 : 0]$ corresponds to an element of $D$, or more precisely to all associates of that element. An ideal number that reduces to $[2 : 1]$ might be regarded as a new type of (vaguely defined) number, not in $D$. In Table 2.1, we list all primitive ideal numbers $[a : k]$ with $a \leq 50$ that reduce to $[1 : 0]$ in the two left columns, together with an element $q + rz$ having $[a : k]$ as its ideal form, and all $[a : k]$ that reduce to $[2 : 1]$ in the two columns at right.

Suppose that ideal numbers can be multiplied and factored by the same rules that we saw hold for ideal forms of Gaussian integers. (We will confirm, using

Table 2.1. Ideal Numbers of Discriminant $\Delta = -20$

| | | | | | |
|---|---|---|---|---|---|
| $[1 : 0]$ | $= 1$ | $[29 : 13]$ | $= 3 - 2z$ | $[2 : 1]$ | $[27 : 7]$ |
| $[5 : 0]$ | $= z$ | $[29 : -13]$ | $= 3 + 2z$ | $[3 : 1]$ | $[27 : -7]$ |
| $[6 : 1]$ | $= 1 + z$ | $[30 : 5]$ | $= 5 + z$ | $[3 : -1]$ | $[35 : 10]$ |
| $[6 : -1]$ | $= 1 - z$ | $[30 : -5]$ | $= 5 - z$ | $[7 : 3]$ | $[35 : -10]$ |
| $[9 : 2]$ | $= 2 + z$ | $[41 : 6]$ | $= 6 + z$ | $[7 : -3]$ | $[42 : 11]$ |
| $[9 : -2]$ | $= 2 - z$ | $[41 : -6]$ | $= 6 - z$ | $[10 : 5]$ | $[42 : -11]$ |
| $[14 : 3]$ | $= 3 + z$ | $[45 : 20]$ | $= 5 - 2z$ | $[15 : 5]$ | $[42 : 17]$ |
| $[14 : -3]$ | $= 3 - z$ | $[45 : -20]$ | $= 5 + 2z$ | $[15 : -5]$ | $[42 : -17]$ |
| $[21 : 4]$ | $= 4 + z$ | $[46 : 15]$ | $= 1 - 3z$ | $[18 : 7]$ | $[43 : 9]$ |
| $[21 : -4]$ | $= 4 - z$ | $[46 : -15]$ | $= 1 + 3z$ | $[18 : -7]$ | $[43 : -9]$ |
| $[21 : 10]$ | $= 1 - 2z$ | $[49 : 17]$ | $= 2 + 3z$ | $[23 : 8]$ | $[47 : 18]$ |
| $[21 : -10]$ | $= 1 + 2z$ | $[49 : -17]$ | $= 2 - 3z$ | $[23 : -8]$ | $[47 : -18]$ |

a more precise definition, that this assumption is correct in §3.4.) For instance, $[3 : 1] \cdot [7 : 3] = [21 : 10]$ since 10 is the unique solution of $x \equiv 1 \pmod 3$ and $x \equiv 3 \pmod 7$ modulo 21. Similarly, $[3 : -1] \cdot [3 : -1] = [9 : 2]$ since $k = 2$ is the unique solution of $x^2 + 5 \equiv 0 \pmod 9$ congruent to $-1$ modulo 3. On the other hand, $[3 : 1] \cdot [3 : -1] = 3[1 : 0]$. For factorization, we have $[21 : -4] = [3 : -4] \cdot [7 : -4] = [3 : -1] \cdot [7 : 3]$ for example. Note that an ideal number $[p : k]$ with $p$ prime cannot be factored further (aside from using $[1 : 0]$, which corresponds to a unit of $D$, as one of the factors). It will be reasonable to regard such an ideal number as *irreducible*.

Now we can see that every ideal number can be written as a product of irreducible ideal numbers, and we claim that this product is unique, aside from order. Furthermore, we assert that different irreducible factorizations of elements of $D = D_{-20}$ can be understood as different groupings of these ideal numbers. For instance, we saw in a previous example that $2 \cdot 3 = 6 = (1 + z)(1 - z)$ in $D$, with each factor irreducible as an element of $D$. But using ideal number factorization, we have that

$$\begin{aligned}(1 + z)(1 - z) &= [6 : 1] \cdot [6 : -1] = ([2 : 1] \cdot [3 : 1]) \cdot ([2 : 1] \cdot [3 : -1]) \\ &= ([2 : 1] \cdot [2 : 1]) \cdot ([3 : 1] \cdot [3 : -1]) = 2[1 : 0] \cdot 3[1 : 0] = 2 \cdot 3.\end{aligned}$$

(Here we use the fact that $[2 : 1] = [2 : -1]$ is its own conjugate. Note also that we are blurring the distinction between elements of $D$ and their ideal forms, which are unique only up to associates of elements of $D$.)

**Exercise 2.6.2.** Verify that each $[a : k]$ below is an ideal number in $D_{-20}$. Use the reduction algorithm of Theorem 2.4.3 to find an element $v$ having ideal form $[a : k]$, or show that there is no such element. Write each element as a product of irreducible ideal numbers of discriminant $-20$.

(a) $[87 : -16]$.

(b) $[161 : 31]$.

(c) $[161 : -38]$.

(d) $[203 : -74]$.

(e) $[270 : 115]$.

As an example requiring only primitive elements of $D$, one can verify that

$$(1 + 3z)(1 - 2z) = 31 + z = (3 + z)(7 - 2z),$$

with each factor irreducible as an *element* of $D$. (For instance, $N(7 - 2z) = 7^2 + 5(-2)^2 = 69$. If we could write $7 - 2z = uv$ in $D$ with neither $u$ nor $v$ a unit, then one of those elements would have norm 3, which we have already noted does not occur.) But if we regard these terms as ideal numbers, we find that each one factors further:

$$(1+3z)(1-2z) = [46 : -15] \cdot [21 : 10] = ([2 : 1] \cdot [23 : 8]) \cdot ([3 : 1] \cdot [7 : 3])$$
$$= ([2 : 1] \cdot [7 : 3]) \cdot ([3 : 1] \cdot [23 : 8]) = [14 : 3] \cdot [69 : 31] = (3+z)(7-2z).$$

Again, we find that the irreducible ideal number factorizations are identical, aside from order. ♢

**Exercise 2.6.3.** Verify that the following pairs of products are equal in the given quadratic domain $D = D_\Delta$, and that each of the factors is irreducible in $D$. Find an ideal form for each of the terms, and find the factorization of each of those terms into irreducible ideal numbers of discriminant $\Delta$.

(a) $(3 + 2z)(2 + z) = (4 - z)(-3 + z)$ in $D_{-24}$, where $z = \sqrt{-6}$.

(b) $(5 + z)(8 + z) = (-3 + z)(4 - 3z)$ in $D_{-52}$, where $z = \sqrt{-13}$.

(c) $(3 + 2z)(2 - z) = (4 + z)(5 - z)$ in $D_{-56}$, where $z = \sqrt{-14}$.

(d) $(3 + 2z)(7 + z) = (-5 + z)(3 - 4z)$ in $D_{-23}$, where $z = \frac{1+\sqrt{-23}}{2}$.

In the next chapter, we will make these rather vague notions more precise, with the introduction of *ideals* as a replacement for ideal numbers. But we will find that the calculations introduced here carry over to that new setting in an identical way. We will then begin to consider how these irreducible ideal number factorizations apply to representations of integers by the principal form of discriminant $\Delta = -20$, or by related expressions.

## Quadratic Domains—Review

In this chapter, we introduced a general setting for our study of quadratic number theory, namely domains of quadratic integers, of which the domain of Gaussian integers is a special case. Important concepts of divisibility, such as units and irreducible elements, carry over from $\mathbb{Z}[i]$ to these quadratic domains. We again introduced a notation of *ideal form* for each element of a quadratic domain, and developed criteria for divisibility using this notation. But we also found that, unlike in the domain of Gaussian integers, there are many quadratic domains that lack the unique factorization property for irreducible elements. We connected unique factorization to a property of ideal forms for elements, and we introduced the concept of *ideal numbers* as a possible method of resolving examples of distinct irreducible factorizations of elements of a quadratic domain. We summarize the main results of Chapter 2 as follows.

(1) A complex number $\upsilon$ is called a *quadratic number* if $f(\upsilon) = 0$ for some nonzero quadratic polynomial $f(x)$ having integer coefficients. If $\upsilon$ is not rational, then $f(x) = ax^2+bx+c$ is uniquely determined by $\upsilon$, under the assumption that $\gcd(a, b, c) = 1$ and $a > 0$. We call $f(x)$ the *minimum polynomial* of $\upsilon$, and its discriminant, $\Delta = b^2 - 4ac$, is called the *discriminant* of $\upsilon$.

(2) A quadratic number $\upsilon$ is called a *quadratic integer* if its minimum polynomial is *monic*, $f(x) = x^2 + bx + c$.

(3) If $d \neq 1$ is a squarefree integer and $\gamma$ is a positive integer, we define a corresponding *discriminant*, $\Delta = \Delta(d, \gamma)$ (see equation (2.2.1)). Then $D = D_\Delta = \{q + rz \mid q, r \in \mathbb{Z}\}$ is the *quadratic domain* of discriminant $\Delta$. (Here $z$ is a particular quadratic integer defined in terms of $d$ and $\gamma$ (see (2.2.2) and (2.2.3)).) This set is an integral domain, consisting of all quadratic integers whose discriminant is a square multiple of $\Delta$. If $\gamma = 1$, then $D$ is the set of all quadratic integers in the field $\mathbb{Q}(\sqrt{d})$, and is called a *complete* quadratic domain. If $\gamma > 1$, then $D$ is a subdomain of its corresponding complete quadratic domain, and is called a *quadratic subdomain*.

(4) To each element $\upsilon \neq 0$ in $D_\Delta$, we associate an *ideal form* $g[a : k]$. For $g[a : k]$ to be an ideal form of an element $\upsilon$, it is necessary that $k$ satisfies the quadratic congruence $\phi(x) \equiv 0 \pmod{a}$, where $\phi(x)$ is the *principal polynomial* of discriminant $\Delta$ (defined in (2.2.7)). This condition is not always sufficient, but we define each eligible expression $g[a : k]$ to be an *ideal number* of discriminant $\Delta$. We define $g[a : k]$ to be a *principal ideal number* if it is an ideal form for some quadratic integer in $D_\Delta$.

(5) We can describe divisibility, multiplication, and factorization for elements in a quadratic domain using ideal forms. When every ideal number is principal, we can describe all irreducible elements precisely, and have uniqueness of irreducible factorization, which we can apply to representations of integers by corresponding quadratic expressions.

(6) When there are ideal numbers of a particular discriminant $\Delta$ that are not principal, we can find essentially distinct irreducible factorizations of some elements in the quadratic domain $D_\Delta$. In this situation, ideal numbers that are not principal appear to restore uniqueness to these irreducible factorizations.

In Chapter 3, we will make the concept of ideal numbers more exact, but we will continue with the "numerical" notation introduced for these discriminants. In later chapters, we will begin to see how the unique factorization that this concept provides can be applied to arithmetic questions about integers.

# 3

# Ideals of Quadratic Domains

Using ideal form notation, and with the benefit of considerable hindsight, we have arrived at a position similar to that introduced by Kummer in the mid-nineteenth century. We have seen that a quadratic domain may fail to have unique factorization into irreducible elements. But evidence suggests that *ideal numbers* are additional factors that help us attain a form of unique factorization in an arbitrary quadratic domain. In Chapter 2, we left many details of ideal numbers unclear, simply assuming that these expressions follow the same rules for multiplication and factorization as do ideal forms for actual quadratic integers. Our goal in this chapter is to put this viewpoint on firmer ground.

The terminology of ideal numbers is due to Kummer, who applied the idea in broader settings involving algebraic integers (particularly in *cyclotomic* fields, defined in terms of $n$-th roots of unity). Dedekind clarified this concept by defining an ideal number, renamed as an *ideal*, as a certain type of subset of a ring or integral domain. This development, described in Dedekind's 1877 work *Theory of Algebraic Integers*, quickly became essential in the advancement of modern algebra. (See Appendix C for more details on ideals of arbitrary rings.)

In this chapter, we adopt Dedekind's standard definition of ideals in full, but will emphasize a more "numerical" interpretation of ideals than is common in most accounts of abstract algebra or algebraic number theory. We will see in particular that in a *quadratic* domain $D$, every nontrivial ideal can be expressed using the notation that we introduced for quadratic integers, and then for ideal numbers. We will establish precisely, for ideals, the rules for multiplication and irreducible factorization that we saw hold for Gaussian integers in ideal form, and that we assumed to hold for ideal numbers. As our main result, we will prove the

uniqueness of prime ideal factorization in every *complete* quadratic domain, and for what we will define as complete ideals in an arbitrary quadratic domain.

## 3.1 Ideals and Ideal Numbers

Throughout this section, let $D = D_\Delta = \{q + rz \mid q, r \in \mathbb{Z}\}$ be the quadratic domain of some discriminant $\Delta$, with $z = z_\Delta$ the basis element as defined in equation (2.2.2).

**Definition.** Let $D$ be a quadratic domain. A nonempty subset $A$ of $D$ is called an *ideal* of $D$ if the following statements are true.

(1) If $\upsilon$ and $w$ are elements of $A$, then $\upsilon - w$ is an element of $A$.

(2) If $\upsilon$ is in $A$ and $x$ is in $D$, then $\upsilon x$ is an element of $A$.

Since $A$ is nonempty, $0 = \upsilon - \upsilon$ is always in $A$. Note that for every $\upsilon$ and $w$ in $A$, then $0 - w = -w$ and $\upsilon - (-w) = \upsilon + w$ are elements of $A$. In particular, an ideal is always closed under addition. The following exercise provides a general example of an ideal in a quadratic domain.

**Exercise 3.1.1.** If $\upsilon$ and $w$ are elements of a quadratic domain $D$, show that $\langle \upsilon, w \rangle = \{\upsilon x + wy \mid x, y \in D\}$ is an ideal of $D$.

**Definition.** Elements of $\langle \upsilon, w \rangle$ are called *combinations* of $\upsilon$ and $w$. Note as a special case that $\langle \upsilon, 0 \rangle = \{\upsilon x + 0 \cdot y \mid x, y \in D\} = \{\upsilon x \mid x \in D\}$ is an ideal of $D$. We will also denote $\langle \upsilon, 0 \rangle$ as $\langle \upsilon \rangle$, and refer to $\langle \upsilon \rangle$ as the *principal ideal* of $D$ generated by $\upsilon$. The sets $\langle 0 \rangle = \{0 \cdot x \mid x \in D\} = \{0\}$ and $\langle 1 \rangle = \{1 \cdot x \mid x \in D\} = D$ are ideals of every quadratic domain $D$. If $A$ is an ideal of $D$, we say that $A$ is *proper* if $A \neq D$, and that $A$ is *nontrivial* if $A \neq \{0\}$.

**Exercise 3.1.2.** Let $\upsilon$ be an element and $A$ an ideal of a quadratic domain $D$. Show that the set $\upsilon A = \{\upsilon x \mid x \in A\}$ is an ideal of $D$, and that $\upsilon A$ is a subset of the principal ideal $\langle \upsilon \rangle$. Show that if $A$ and $B$ are ideals of $D$ and $\upsilon \neq 0$, then $A = B$ if and only if $\upsilon A = \upsilon B$.

**Exercise 3.1.3.** Let $\upsilon$ be an element and $B$ an ideal of a quadratic domain $D$. Show that the set $A = \{x \in D \mid \upsilon x \in B\}$ is an ideal of $D$. Show in this case that if $B$ is a subset of the principal ideal $\langle \upsilon \rangle$, then $B = \upsilon A$.

In some cases, we can use a pair of elements in $D$ to define an ideal of $D$ in a different way, as we will see after we introduce the following terminology.

**Definition.** If $S = \{\upsilon_1, \ldots, \upsilon_t\}$ is a finite subset of a quadratic domain $D$, then an element of the form $m_1\upsilon_1 + \cdots + m_t\upsilon_t$ with each $m_i$ in $\mathbb{Z}$ is called a *$\mathbb{Z}$-combination*

of $S$. The set of all $\mathbb{Z}$-combinations of $S$ is called the $\mathbb{Z}$-*span* of $S$. If $A$ is an ideal of $D$, and $S$ is a subset of $A$, we say that $S$ is a $\mathbb{Z}$-*basis* for $A$ if every element of $A$ can be written uniquely as a $\mathbb{Z}$-combination of $S$.

**Exercise 3.1.4.** Show that the $\mathbb{Z}$-span of a finite subset $S$ of a quadratic domain $D$ is closed under subtraction. Show that the $\mathbb{Z}$-span of $S = \{3, 1+i\}$ is not an ideal of $D_{-4} = \mathbb{Z}[i]$.

As illustrated in Exercise 3.1.4, the $\mathbb{Z}$-span of a subset of $D$ is not always an ideal of $D$. The following proposition provides a criterion that ensures that the $\mathbb{Z}$-span of a particular type of subset of $D$ is an ideal, and connects ideals of $D$ to the ideal numbers defined in Chapter 2.

**Proposition 3.1.1.** *Let $D = D_\Delta = \{q + rz \mid q, r \in \mathbb{Z}\}$ be a quadratic domain, and let $\phi(x)$ be the principal polynomial of discriminant $\Delta$. Let $a$ and $k$ be rational integers, and let $A$ be the $\mathbb{Z}$-span of the subset $S = \{a, k+z\}$ of $D$. Then $A$ is an ideal of $D$ if and only if $a$ divides $\phi(k)$.*

*Proof.* Let $A$ be the $\mathbb{Z}$-span of $S = \{a, k+z\}$, that is,

$$A = \{m(a) + n(k+z) \mid m, n \in \mathbb{Z}\}.$$

Exercise 3.1.4 shows that $A$ is closed under subtraction. So to show that $A$ is an ideal of $D$, it suffices to establish that $a(s+tz)$ and $(k+z)(s+tz)$ are elements of $A$ for every $s+tz$ in $D$. Now $a(s+tz) = (s-tk)a + at(k+z)$ is a $\mathbb{Z}$-combination of $S$ in every case. Direct calculation, using the product formula in (2.2.8) and the definition of $\phi(k)$ in (2.2.7), shows that

$$\begin{aligned}(k+z)(s+tz) &= \left(ks - \frac{\varepsilon^2 - \Delta}{4} \cdot t\right) + (s + kt + \varepsilon t)z \\ &= (ks + \varepsilon kt + k^2 t - \phi(k) \cdot t) + (s + kt + \varepsilon t)z \\ &= -\phi(k) \cdot t + (s + kt + \varepsilon t)(k+z). \quad (3.1.1)\end{aligned}$$

In particular, if $s = k + \varepsilon$ and $t = -1$, then $(k+z)(s+tz) = \phi(k)$, a rational integer. If $\phi(k) = ac$ for some integer $c$, then equation (3.1.1) implies that $(k+z)(s+tz) = (-ct)a + (s+kt+\varepsilon t)(k+z)$ is a $\mathbb{Z}$-combination of $S$. Conversely, if $\phi(k) = m(a) + n(k+z)$ for some $m$ and $n$ in $\mathbb{Z}$, then $n = 0$ and so $a$ divides $\phi(k)$. Thus $A$ is an ideal of $D$ if and only if $a$ divides $\phi(k)$. □

**Example.** Let $\Delta = \Delta(-5, 1) = -20$, so that $z = \sqrt{-5}$ and $\phi(x) = x^2 + 5$. Since 18 divides $\phi(7) = 54$, the $\mathbb{Z}$-span $A$ of $S = \{18, 7+z\}$ is an ideal of $D_{-20}$. Here $A = \{(18m + 7n) + nz \mid m, n \in \mathbb{Z}\} = \{q + rz \mid q \equiv 7r \pmod{18}\}$. ♢

If $A$ is an ideal of a quadratic domain $D$ and $g$ is a positive rational integer, then Exercise 3.1.2 shows that $B = gA = \{gx \mid x \in A\}$ is also an ideal of $D$.

We now introduce a notation for the ideals defined in Proposition 3.1.1 and these related ideals.

**Definition.** Let $D$ be the quadratic domain and $\phi(x)$ the principal polynomial of some discriminant $\Delta$. If $a$ and $k$ are integers for which $a$ divides $\phi(k)$, we will denote the ideal $A$ of $\mathbb{Z}$-combinations of the set $S = \{a, k+z\}$ as $A = [a : k]_\Delta$, or as $A = [a : k]$ if $\Delta$ is clear from the context. If $B = gA$ for some positive rational integer $g$, then we write $B = g[a : k]_\Delta = g[a : k]$. We say that $A$ and $B$ are written in *ideal number* notation, or as *ideal numbers*, in this case.

As in the preceding example, if $A = [a : k]$ for some integer $a$ dividing $\phi(k)$, then $A = \{q + rz \mid q \equiv kr \pmod{a}\}$. The following exercise shows that $[a : k] = [-a : k]$, and that if $\ell \equiv k \pmod{a}$, then $[a : k] = [a : \ell]$.

**Exercise 3.1.5.** Let $D = \{q + rz \mid q, r \in \mathbb{Z}\}$ be a quadratic domain, and let $a$, $k$, and $\ell$ be integers with $a$ positive. Show that the $\mathbb{Z}$-spans of $S = \{a, k+z\}$ and $T = \{-a, k+z\}$ are equal. Show that the $\mathbb{Z}$-spans of $S = \{a, k+z\}$ and $T = \{a, \ell+z\}$ are equal if $\ell \equiv k \pmod{a}$.

**Classification of Ideals of a Quadratic Domain.** A quadratic domain $D = D_\Delta$ contains an ideal $g[a : k]$ under precisely the same conditions in which $g[a : k]$ is an ideal number of discriminant $\Delta$. In the remainder of this section, we will show that every nontrivial ideal $A$ of $D$ has this form. Thus nontrivial ideals of $D_\Delta$ are identical to ideal numbers of discriminant $\Delta$.

**Proposition 3.1.2.** *Let $B$ be a nontrivial ideal of a quadratic domain $D$. Then there is a smallest positive rational integer $g$ so that $B$ contains an element $m + gz$ for some $m$ in $\mathbb{Z}$. In this case, there is an ideal $A$ of $D$ for which $B = gA$.*

*Proof.* If $B$ is nontrivial, then $B$ contains an element $v = q + rz$ with $q$ and $r$ not both zero, as well as $-v$, $vz$, and $-vz$ by closure properties of an ideal. If $r \neq 0$, then the coefficient of $z$ in either $v$ or $-v$ is positive. If $r = 0$, then $q \neq 0$, and the coefficient of $z$ in either $vz = qz$ or $-vz = -qz$ is positive. Thus $B$ contains an element with a positive coefficient of $z$, and we can select $g$ to be the smallest such positive integer, with $m + gz$ an element of $B$.

Now let $s + tz$ be an element of $B$, and write $t = gq + r$ with $0 \leq r < g$. Then we find that $(s + tz) - q(m + gz) = (s - qm) + rz$ is an element of $B$ by closure properties. We must conclude that $r = 0$, and so $g$ divides $t$, to avoid contradicting the definition of $g$. But $(s + tz)(-\varepsilon + z)$, in which the coefficient of $z$ is $s$, is likewise in $B$, and the same argument shows that $g$ divides $s$. So $g$ divides each element of $B$, and $B$ is a subset of the principal ideal $\langle g \rangle$. By Exercise 3.1.3, then $B = gA$, where $A = \{x \in D \mid gx \in B\}$ is an ideal of $D$. □

**Definition.** If $B$ is a nontrivial ideal of a quadratic domain $D$, and $g$ is the smallest positive coefficient of $z$ in an element of $B$, as in Proposition 3.1.2, we call $g$ the *divisor* of $B$. If $g = 1$, we say that $B$ is a *primitive* ideal of $D$.

**Exercise 3.1.6.** Show that if $g$ is the divisor of an ideal $B$ of a quadratic domain $D$, and $B = gA$ as in Proposition 3.1.2, then $A$ is primitive.

**Proposition 3.1.3.** *Let $A$ be a primitive ideal of a quadratic domain $D$. Then there is a smallest positive rational integer $a$ in $A$. In this case, $m$ is a rational integer in $A$ if and only if $a$ divides $m$.*

*Proof.* If $A$ is a nontrivial ideal of $D$, then $A$ contains a nonzero element $v$ of $D$. Now $\overline{v}$ is an element of $D$, so that $N(v) = v\overline{v}$ is a nonzero rational integer contained in $A$, as is $-N(v)$, by the closure properties of an ideal. Thus $A$ contains a positive rational integer, and must have a smallest such element, which we label $a$. If $m = aq$ for some $q$ in $\mathbb{Z}$, then $m$ is in $A$ since $q$ is in $D$. Conversely, if $m$ is a rational integer in $A$, we can write $m = aq + r$ with $0 \leq r < a$. But then $r = m - aq$ is an element of $A$ also, and we must have $r = 0$, so that $a$ divides $m$, to avoid contradicting the definition of $a$. □

**Proposition 3.1.4.** *Let $A$ be a primitive ideal of a quadratic domain $D$, and let $a$ be the smallest positive rational integer in $A$. Then there is a rational integer $k$, which is unique modulo $a$, so that $A$ contains $k + z$.*

*Proof.* If $A$ is primitive, then the divisor of $A$ is 1, and $A$ contains an element $k + z$ by definition. If $\ell + z$ is also in $A$, then $(\ell + z) - (k + z) = \ell - k$ is a rational integer in $A$. Proposition 3.1.3 shows that $a$ divides $\ell - k$, that is, $k$ is uniquely determined modulo $a$. □

**Definition.** Let $B$ be a nontrivial ideal of a quadratic domain $D$ with divisor $g$, and let $A$ be the primitive ideal of $D$ for which $B = gA$. If $a$ is the smallest positive rational integer in $A$, we say that $a$ is the *subnorm* of $B$. If $k + z$ is an element of $A$, we define the *character* of $B$ to be the congruence class of $k$ modulo $a$. We define the *norm* of $B$ to be $N(B) = g^2 a$.

**Theorem 3.1.5.** *Let $B$ be a nontrivial ideal of a quadratic domain $D$, with divisor $g$, subnorm $a$, and character $k$. Then $B$ is the same as the ideal written as $g[a : k]$ in ideal number notation.*

*Proof.* Let $B = gA$, where $A = \{x \in D \mid gx \in B\}$, as in Proposition 3.1.2. Then, by definition, $a$ is the smallest positive rational integer in $A$, and $k + z$ is an element of $A$. Every $\mathbb{Z}$-combination of $S = \{a, k + z\}$ is an element of $A$ by closure properties. Conversely, if $v = s + tz$ is an element of $A$, then $v - t(k + z) =$

$s - tk$ is a rational integer in $A$. It follows that $s - tk = ar$ for some integer $r$ by Proposition 3.1.3. Thus $v = s + tz = r(a) + t(k + z)$ is a $\mathbb{Z}$-combination of $S$. Therefore $A = [a : k]$ and $B = gA = g[a : k]$ by definition. □

**Exercise 3.1.7.** Let $B$ be a nontrivial ideal of a quadratic domain $D$, with divisor $g$, subnorm $a$, and character $k$. Show that the set $S = \{ga, g(k + z)\}$ is a $\mathbb{Z}$-basis for $B$.

An implication of Proposition 3.1.1 and Theorem 3.1.5 is that the number of *primitive* ideals of a quadratic domain $D_\Delta$ having norm $a$ is the same as the number of solutions of $\phi(x) \equiv 0 \pmod{a}$, where $\phi(x)$ is the principal polynomial of discriminant $\Delta$. It follows that there are only finitely many ideals with a particular norm in a fixed quadratic domain, and these can be compiled by the same process we developed for solving a quadratic congruence. We illustrate this claim with an example to conclude this section.

**Example.** Let $\Delta = \Delta(79, 1) = 316$, so that $z = \sqrt{79}$ and $\phi(x) = x^2 - 79$. Suppose that we want to find all ideals of norm 45 in $D = D_\Delta$. Since $\left(\frac{79}{3}\right) = 1$ and $\left(\frac{79}{5}\right) = 1$, we know that $\phi(x) \equiv 0 \pmod 3$ and $\phi(x) \equiv 0 \pmod 5$ both have two solutions, as does $\phi(x) \equiv 0 \pmod 9$. So $x^2 \equiv 79 \pmod{45}$ has four solutions, which we find by applying the Chinese Remainder Theorem to $x \equiv s \pmod 9$ and $x \equiv t \pmod 5$, where $s = \pm 4$ and $t = \pm 2$. We obtain $x = \pm 13$ and $x = \pm 22$ in minimal absolute value. Since $45 = 3^2 \cdot 5$, an ideal $A = 3[5 : k]$ also has norm 45 if $\phi(k) \equiv 0 \pmod 5$. We conclude that

$$[45 : 13], \quad [45 : -13], \quad [45 : 22], \quad [45 : -22], \quad 3[5 : 2], \quad 3[5 : -2]$$

are the ideals of $D$ with norm 45. ◊

**Exercise 3.1.8.** Let $\Delta = \Delta(31, 1) = 124$. Find all ideals $A$ of norm 75 in the quadratic domain $D_\Delta$, writing each as an ideal number $g[a : k]$.

**Exercise 3.1.9.** For each pair of integers $a$ and $\Delta$ below, find all ideals $A$ of $D = D_\Delta$ with $N(A) = a$.

(a) $a = 2, \Delta = -7$.

(b) $a = 70, \Delta = -31$.

(c) $a = 100, \Delta = 41$.

**Exercise 3.1.10.** Let $A$ be an ideal of a quadratic domain $D$, and for $v$ and $w$ in $D$, say that $v \equiv w \pmod A$ if and only if $v - w$ is an element of $A$. Show that this *congruence* relation is an equivalence relation on $D$. If $A$ has divisor $g$ and

subnorm $a$, show that every element of $D$ is congruent modulo $A$ to precisely one element $q + rz$ with $0 \leq q < ga$ and $0 \leq r < g$. (Thus $N(A)$ is the same as the number of distinct equivalence classes of elements of $D$ under congruence modulo $A$. This is sometimes taken as the definition of the norm of an ideal.)

## 3.2 Writing Ideals as Ideal Numbers

In this section, we compile some general statements on expressing an ideal $A$ of a quadratic domain $D = D_\Delta$ as an ideal number in practice. Results from §3.1 show that $A = g[a : k]$ if $g$ is the smallest positive coefficient of $z$ in an element of $A$, with $gk + gz$ a particular example of such an element, and $ga$ is the smallest positive rational integer in $A$. In specific examples, we may write $A$ as an ideal number by finding these elements, as in the following important example.

**Proposition 3.2.1.** *Let $D$ be a quadratic domain. As an ideal of itself, $D$ can be expressed as $[1 : 0]$. If $g$ is a positive rational integer, then $\langle g \rangle = g[1 : 0]$. If $A$ is an ideal of $D$, then $N(A) = 1$ if and only if $A = D$.*

*Proof.* The ideal $D$ contains 1 and $z = 0 + z$, which must be the smallest positive rational integer and an element with smallest positive coefficient of $z$, respectively. So $D = [1 : 0]$. If $B = \langle g \rangle$, then $A = \{\upsilon \in D \mid g\upsilon \in B\} = D$, and so $B = gD = g[1 : 0]$. Since $D = [1 : 0]$, then $N(D) = 1$ by definition. Conversely, if the norm of an ideal $A$ equals 1, then $g = 1$ is the divisor of $A$, and $a = 1$ must be the smallest positive rational integer in $A$. But in that case $\langle 1 \rangle = D$ is a subset of $A$, so that $A = D$. □

**Principal Ideals.** We see in this subsection how every principal ideal of a quadratic domain can be expressed in the form $g[a : k]$ in practice. We begin with an example approached directly, before establishing a general formula.

**Example.** Let $D = D_{28}$, so that $z = \sqrt{7}$, and consider the principal ideal $A = \langle 5 - 3z \rangle$ of $D$. The typical element of $A$ has the form

$$(5 - 3z)(s + tz) = (5s - 21t) + (5t - 3s)z,$$

with $s$ and $t$ integers. Such an element is in $\mathbb{Z}$ if and only if $3s = 5t$. Since $\gcd(3, 5) = 1$, this implies that 3 divides $t$, say that $t = 3q$ and then $s = 5q$ for some $q$ in $\mathbb{Z}$. Now $5s - 21t = 25q - 63q = -38q$, and $a = 38$ is the smallest positive integer of this form. Similarly, $5t - 3s = 1$ when, for example, $s = 3$ and $t = 2$, and in that case, $5s - 21t = -27$. So $-27 + z$ is in $A$, and we can write $A = [38 : -27] = [38 : 11] = [-38 : 11]$, among other possibilities. ◊

Notice that $N(5 - 3z) = 5^2 - 7(-3)^2 = -38$, and $-3k \equiv 5 \pmod{38}$ has $k = 11$ as a solution. So $[-38 : 11]$ is also an ideal form for $\upsilon = 5 - 3z$ as an

element of $D$. Our next result shows that the same is true for every principal ideal of a quadratic domain.

**Theorem 3.2.2.** *Let $\upsilon$ be a nonzero element of a quadratic domain $D$, and suppose that $g[a : k]$ is an ideal form for $\upsilon$. Then the principal ideal of $D$ generated by $\upsilon$ can also be written as $\langle\upsilon\rangle = g[a : k]$. Thus $N(\langle\upsilon\rangle) = |N(\upsilon)|$ for every element $\upsilon$ of a quadratic domain $D$.*

A proof of Theorem 3.2.2 could generalize the calculations of the preceding example. Instead, we invoke criteria for divisibility using ideal forms, which we compiled in §2.3, as follows.

*Proof.* By definition, an element $w = m+nz$ of $D$ is in $\langle\upsilon\rangle$ if and only if $\upsilon$ divides $w$ in $D$. Assume first that $\upsilon = q+rz$ is primitive, so that $N(q+rz) = a$ and $rk \equiv q \pmod{a}$. Lemma 2.3.2 implies that $\upsilon$ divides $w$ if and only if $nk \equiv m \pmod{a}$. In particular, $\upsilon$ divides $k + z$, and $\upsilon$ divides a rational integer $m = m + 0z$ if and only if $m \equiv 0 \pmod{a}$. Thus $\langle\upsilon\rangle$ can be expressed as $[a : k]$. More generally, if $\upsilon = g(q + rz)$ with $g$ positive, then $\langle\upsilon\rangle$ is a subset of $\langle g\rangle$, and we find that $\langle\upsilon\rangle = g[a : k]$ with $a$ and $k$ as above. Here $a$ might be negative, but the norm of $\langle\upsilon\rangle$ is $g^2 \cdot |a| = |N(\upsilon)|$ in every case. □

**Example.** Let $\upsilon = 12 - 21z = 3(4 - 7z)$ in $D = D_{-43}$. Here

$$N(4 - 7z) = 4^2 + 4(-7) + 11(-7)^2 = 527,$$

and $k = 150$ satisfies $-7x \equiv 4 \pmod{527}$. Thus $\langle\upsilon\rangle = 3[527 : 150]$. ♢

**Exercise 3.2.1.** For each of the following principal ideals $A$ of the given quadratic domain $D$, write $A$ as an ideal number, $A = g[a : k]$.

(a) $A = \langle 1 + 3z\rangle$ in $D = D_{13}$.

(b) $A = \langle 1 + 3z\rangle$ in $D = D_{28}$.

(c) $A = \langle 5 - 3z\rangle$ in $D = D_{37}$.

(d) $A = \langle 12 - 9z\rangle$ in $D = D_{-67}$.

(e) $A = \langle 13 + 5z\rangle$ in $D = D_{-68}$.

**Definition.** A quadratic domain $D$ is called a *principal ideal domain* if every ideal of $D$ is a principal ideal.

The following exercise shows that $D$ is a principal ideal domain if and only if $D$ is a principal ideal number domain, a term we introduced in §2.5.

**Exercise 3.2.2.** Let $D$ be the quadratic domain and $\phi(x)$ be the principal polynomial of discriminant $\Delta$. Show that $D$ is a principal ideal domain if and only if for every pair of integers $a$ and $k$ for which $a$ divides $\phi(k)$, either $[a : k]$ or $[-a : k]$ is an ideal form for some element of $D$.

**Ideals Consisting of Combinations.** If $A = \langle v, w\rangle$ is an ideal made up of combinations of a pair of elements, we can take two approaches to expressing $A$ in the form $g[a : k]$. We illustrate a direct approach in the following example.

**Example.** Let $\Delta = -20$, so that $z = \sqrt{-5}$. Consider the ideal $A = \langle 3, 1 + 2z\rangle$ in $D = D_{-20}$. The typical element of $A$ has the form

$$3(q + rz) + (1 + 2z)(s + tz) = (3q + s - 10t) + (3r + 2s + t)z,$$

where $q$, $r$, $s$, and $t$ are integers. If $3r + 2s + t = 0$, so that $t = -3r - 2s$, then $3q + s - 10t = 3q + 30r + 21s$. Every integer of this form is divisible by 3. Since $3 = 3(1) + (1 + 2z)(0)$ is in $A$, then $a = 3$ must be the smallest positive rational integer in $A$. Now if $q = 3$, $r = 0$, $s = 0$, and $t = 1$, we find that $-1 + z$ is in $A$. We can write $A = [3 : -1]$. ◊

Theorem 3.2.3 allows an alternative approach to writing an ideal $\langle v, w\rangle$ as an ideal number, based on the following definition and preliminary statements.

**Definition.** If $A$ and $B$ are ideals of a quadratic domain $D$, we define the *sum* of $A$ and $B$ to be $A + B = \{a + b \mid a \in A \text{ and } b \in B\}$.

**Exercise 3.2.3.** If $A$ and $B$ are ideals of a quadratic domain $D$, show that $A + B$ is also an ideal of $D$. Show that $A + B$ contains both $A$ and $B$ as subsets. Show that if $C$ is an ideal of $D$ containing both $A$ and $B$ as subsets, then $A + B$ is also a subset of $C$.

**Theorem 3.2.3.** *Let $A = g[a : k]$ and $B = h[b : \ell]$ be ideals of a quadratic domain $D$, with $\gcd(g, h) = 1$. Then $A + B = [c : m]$, where*

$$c = \gcd(ga, hb, gh(\ell - k)),$$

*and $x = m$ satisfies the pair of congruences*

$$gx \equiv gk \pmod{c} \quad \text{and} \quad hx \equiv h\ell \pmod{c}. \tag{3.2.1}$$

Note that if $\gcd(g, h) = d$, then $gA + hB = d(\frac{g}{d}A + \frac{h}{d}B)$. So we can assume that $\gcd(g, h) = 1$ in practice. If $\gcd(g, h) = 1$, then Exercise 0.1.11 shows that the pair of congruences in (3.2.1) has a unique solution modulo $c$ if and only if $c$ divides $g \cdot h\ell - h \cdot gk = gh(\ell - k)$. This must be the case given the definition of $c$.

*Proof.* The typical element of $A + B$ has the form

$$g[q(a) + r(k + z)] + h[s(b) + t(\ell + z)] = (gaq + gkr + hbs + h\ell t) + (gr + ht)z,$$

where $q$, $r$, $s$, and $t$ are integers. Suppose that $gr + ht = 0$. Since $\gcd(g, h) = 1$, it follows that $g$ divides $t$, say that $t = gu$ for some rational integer $u$, and then that $r = -hu$. In that case,

$$gaq + gkr + hbs + h\ell t = (ga)q + (hb)s + (gh(\ell - k))u.$$

The smallest positive rational integer that can be expressed in this form, so as an element of $A + B$, is $c = \gcd(ga, hb, gh(\ell - k))$.

Since $\gcd(g, h) = 1$, we can also select $r$ and $t$ so that $gr + ht = 1$. In that case, $A + B$ contains $m + z$, where $m = gaq + gkr + hbs + h\ell t$. On substituting $1 - ht$ for $gr$, we have that

$$gm = ga(gq) + hb(gs) + gh(\ell - k)t + gk \equiv gk \pmod{c},$$

since $c$ divides $ga$, $hb$, and $gh(\ell - k)$. On substituting $1 - gr$ for $ht$, we find in a similar way that $hm \equiv h\ell \pmod{c}$. □

By the following result, we can apply Theorem 3.2.3 to an ideal consisting of combinations, expressing the result as an ideal number.

**Exercise 3.2.4.** If $v$ and $w$ are elements of a quadratic domain $D$, show that $\langle v, w\rangle = \langle v\rangle + \langle w\rangle$.

**Example.** Let $A = \langle 3, 1 + 2z\rangle$ in $D = D_{-20}$, as in the preceding example. By Theorem 3.2.2, we find that $\langle 3\rangle = 3[1 : 0]$ and $\langle 1 + 2z\rangle = [21 : -10]$. (Here $N(1 + 2z) = 1^2 + 5 \cdot 2^2 = 21$, and $2x \equiv 1 \pmod{21}$ has $x = -10$ as a solution.) So $A = \langle 3\rangle + \langle 1 + 2z\rangle = [c : m]$, where $c = \gcd(3, 21, -30) = 3$ and $m$ satisfies $3m \equiv 0 \pmod 3$ and $m \equiv -10 \pmod 3$. The second congruence implies that $m \equiv -1 \pmod 3$ and so $A = [3 : -1]$, as we saw previously. ◊

**Exercise 3.2.5.** For each of the following ideals $A$ of the given quadratic domain $D$, write $A$ as an ideal number, $A = g[a : k]$.

(a) $A = \langle 12, 5 + z\rangle$ in $D = D_{13}$.

(b) $A = \langle 7, 3 - 2z\rangle$ in $D = D_{-40}$.

(c) $A = \langle 14, 6 + 2z\rangle$ in $D = D_8$.

**Conjugates of Ideals.** We conclude this section with the following definition that will be important in later calculations.

**Definition.** Let $A$ be an ideal of a quadratic domain $D = D_\Delta$. We define the *conjugate* of $A$ to be the set of conjugates (as defined in $D$) of all elements of $A$, that is, $\overline{A} = \{\overline{v} \mid v \in A\}$.

**Exercise 3.2.6.** Show that if $A$ is an ideal of a quadratic domain $D$, then $\overline{A}$ is also an ideal of $D$.

**Exercise 3.2.7.** Show that if $A = \langle v \rangle$ is a principal ideal of a quadratic domain $D$, then $\overline{A} = \langle \overline{v} \rangle$.

**Proposition 3.2.4.** *Let $A = g[a : k]$ be an ideal of a quadratic domain $D = D_\Delta$. Then its conjugate ideal can be written as $\overline{A} = g[a : -k - \varepsilon]$, where $\varepsilon$ is the basis index of discriminant $\Delta$.*

*Proof.* Let $z = \frac{\varepsilon+\sqrt{\Delta}}{2}$ in $D$, so that $\overline{z} = \frac{\varepsilon-\sqrt{\Delta}}{2} = \varepsilon - z$. The typical element of $A$ has the form $mg(a) + ng(k+z)$ for some integers $m$ and $n$. Thus we find that the typical element of $\overline{A}$ is

$$mg(a) + ng(k + \overline{z}) = mg(a) - ng((-k - \varepsilon) + z).$$

The result follows, since $-n$ varies over all integers as $n$ does. □

## 3.3 Prime Ideals of Quadratic Domains

We have seen in the preceding two sections that every nontrivial ideal $A$ of a quadratic domain can be written as an ideal number, $A = g[a : k]$, in theory and in practice. Our goal in the remainder of Chapter 3 is to introduce arithmetic concepts, such as irreducible factorization, on these ideals, applied particularly in ideal number notation. We will define an operation of multiplication on ideals in §3.4, which allows for consideration of divisibility with ideals. But even before defining multiplication, we can make sense of our "irreducible" elements, which we call *prime ideals*, in terms of ideal containment. We will follow that approach in this section.

**Criteria for Ideal Containment.** The following proposition and its consequences provide useful tests for when one ideal of a quadratic domain is a subset of another, or when two ideals are equal.

**Proposition 3.3.1.** *Let $A = g[a : k]$ and $B = h[b : \ell]$ be nontrivial ideals of a quadratic domain $D$. Then $B$ is a subset of $A$ if and only if*

$$g \text{ divides } h, \quad ag \text{ divides } bh, \quad \text{and} \quad h\ell \equiv hk \pmod{ag}.$$

The reader might recognize the similarity between Proposition 3.3.1 and the criteria for $g[a : k]$ to divide $h[b : \ell]$ in Theorem 1.3.2 for Gaussian integers written in ideal form and in Theorem 2.3.3 for more general quadratic integers. We will see later that in many situations these two relations are interchangeable. But for now, we again emphasize that we have not yet defined an operation of multiplication or a relation of divisibility on ideals.

*Proof.* We show that $g$ divides $h$, $ag$ divides $bh$, and $h\ell \equiv hk \pmod{ag}$ if and only if $bh$ and $h\ell + hz$ are $\mathbb{Z}$-combinations of the set $S = \{ag, gk + gz\}$, so that $B$ is a subset of $A$. Suppose first that $h = gr$, $bh = ags$, and $h\ell - hk = agt$ for some integers $r$, $s$, and $t$. Then we find that $bh = s(ag) + 0(gk + gz)$ and $h\ell + hz = t(ag) + r(gk + gz)$ are $\mathbb{Z}$-combinations of $S$.

Conversely, let $bh = q(ag) + r(gk + gz)$ and $h\ell + hz = s(ag) + t(gk + gz)$ for some integers $q$, $r$, $s$, and $t$. Comparing coefficients of $z$ in these equations shows that $r = 0$ and $h = tg$. It follows that $g$ divides $h$ and $ag$ divides $bh$. The second equation then also implies that $h\ell = ags + tgk = ags + hk$ so that $h\ell \equiv hk \pmod{ag}$. □

**Exercise 3.3.1.** Let $D = D_{-4} = \mathbb{Z}[i]$. Verify that each of the following is an ideal of $D$: $A = [5 : 2]$, $\overline{A} = [5 : -2]$, $B = 5[1 : 0]$, and $C = [65 : 8]$. In each part below, indicate which statement is correct for the given ideals.

(a) $A \subseteq B$ or $B \subseteq A$, or neither.

(b) $\overline{A} \subseteq B$ or $B \subseteq \overline{A}$, or neither.

(c) $A \subseteq C$ or $C \subseteq A$, or neither.

(d) $\overline{A} \subseteq C$ or $C \subseteq \overline{A}$, or neither.

The following exercises provide useful consequences of Proposition 3.3.1.

**Exercise 3.3.2.** Let $A = g[a : k]$ and $B = h[b : \ell]$ be ideals of a quadratic domain $D$. Show that $A = B$ if and only if $g = h$, $a = \pm b$, and $k \equiv \ell \pmod{a}$.

**Exercise 3.3.3.** Show that if $A$ and $B$ are ideals of a quadratic domain $D$ and $B$ is a subset of $A$, then $N(A)$ divides $N(B)$.

**Exercise 3.3.4.** Show that if $A$ and $B$ are ideals of a quadratic domain $D$ with $B$ a subset of $A$ and $N(A) = N(B)$, then $A = B$.

**Definition and Classification of Prime Ideals.** We now define prime ideals in terms of subset containment.

**Definition.** Let $P$ be a proper ideal of a quadratic domain $D$. We say that $P$ is a *prime* ideal of $D$ if there is no proper ideal $Q$ of $D$ that properly contains $P$. That is, $P$ is prime if when $Q$ is an ideal with $P \subseteq Q \subseteq D$, then either $Q = P$ or $Q = D$.

Here we follow the original definition of prime ideals given by Dedekind (see §12 in *Theory of Algebraic Integers*). In more modern terminology, an ideal given by this definition is called *maximal*, while a prime ideal is one with the

property of Proposition 3.3.2 below. It is always the case that a maximal ideal is prime, by the same argument as in the proof of this proposition, but the converse is typically not true. However, for quadratic domains, and for the domains of algebraic integers studied by Dedekind, the two terms are interchangeable for *nontrivial* ideals. (We demonstrate that this is the case in Appendix C.)

**Proposition 3.3.2.** *Let $P$ be a prime ideal of a quadratic domain $D$. Suppose that $v$ and $w$ are elements of $D$ for which $vw$ is in $P$. Then either $v$ is in $P$ or $w$ is in $P$.*

*Proof.* Let $P$ be a prime ideal of $D$, and suppose that $vw$ is an element of $P$ for some $v$ and $w$ in $D$, but that $v$ is not in $P$. Then consider the set $Q = P + \langle v \rangle = \{u+vx \mid u \in P \text{ and } x \in D\}$, an ideal of $D$ containing $P$ by Exercise 3.2.3. Note that $Q$ contains $0 + v(1) = v$, which is not in $P$, so that $Q$ *properly* contains $P$. If $P$ is prime, then $Q$ must equal $D$. In particular, since 1 is in $D$, we have $1 = u + vx$ for some $u$ in $P$ and $x$ in $D$. But now notice that $w = (1)w = (u+vx)w = uw+(vw)x$. Since $u$ is in $P$, and $vw$ is in $P$ by assumption, we conclude that $w$ is in $P$ by the closure properties of an ideal. So $P$ must contain at least one of the elements $v$ or $w$. □

We can describe all prime ideals of a quadratic domain using the following propositions.

**Proposition 3.3.3.** *Let $P$ be a prime ideal of a quadratic domain $D$. Then $P$ contains a unique rational prime number $p$. The norm of $P$ is either $p$ or $p^2$, with $P = \langle p \rangle$ in the latter case.*

*Proof.* Let $P$ be a prime ideal of $D$, and let $a$ be the smallest positive rational integer in $P$. We know that $a \neq 1$ since $P \neq D$. If $a = bc$ with $1 < b, c < a$, then either $b$ or $c$ is in $P$ by Proposition 3.3.2. Either possibility contradicts the definition of $a$. So $a = p$ must be a prime number. Since $a$ divides every rational integer in $P$, this prime number is unique.

Now if $P = g[b : k]$ in ideal number notation with $b$ positive, then $gb$ is the smallest positive rational integer in $P$, that is, $gb = p$. So either $g = 1$ and $b = p$, or $g = p$ and $b = 1$, in which case $P = p[1 : k] = p[1 : 0] = \langle p \rangle$ by Proposition 3.2.1. In the first case, $N(P) = p$. In the second case, $N(P) = p^2 \cdot 1 = p^2$. □

**Proposition 3.3.4.** *Let $D$ be a quadratic domain and let $p$ be a rational prime. If $P$ is an ideal of $D$ with $N(P) = p$, then $P$ is a prime ideal of $D$. The ideal $\langle p \rangle$ is a prime ideal of $D$ if and only if $D$ contains no ideals of norm $p$.*

*Proof.* Let $P$ be an ideal of $D$. Suppose that either $N(P) = p$ or that $N(P) = p^2$ and $D$ contains no ideals of norm $p$. Let $Q$ be an ideal of $D$ with $P \subseteq Q$, so

that $N(Q)$ divides $N(P)$ by Exercise 3.3.3. By our assumptions, we conclude that either $N(Q) = 1$, in which case $Q = D$, or $N(Q) = N(P)$. Since $P \subseteq Q$, the latter possibility implies that $Q = P$, by Exercise 3.3.4. So $P$ is a prime ideal of $D$.

For the converse of the final statement, note that if $P$ is an ideal with $N(P) = p$, then $P$ is primitive, so that $p$ is an element of $P$. But then $\langle p \rangle \subseteq P \subseteq D$, with both containments proper since $N(\langle p \rangle) = p^2$, $N(P) = p$, and $N(D) = 1$. So when $D$ contains an ideal of norm $p$, the ideal $\langle p \rangle$ cannot be prime. □

With these propositions, our task is to categorize the ideals of a quadratic domain with prime norm, which we do in the following theorem. The reader may find it interesting to compare the statement of Theorem 3.3.5 to that of Proposition 2.5.1, which similarly classifies the irreducible elements in a quadratic domain with the unique factorization property. We emphasize, however, that the following result holds in *every* quadratic domain.

**Theorem 3.3.5.** *Let $D$ be the quadratic domain with discriminant $\Delta$, and let $p$ be a rational prime. Then the following statements are true.*

(1) *If $\left(\frac{\Delta}{p}\right) = -1$, then $D$ has no ideals of norm $p$.*

(2) *If $\left(\frac{\Delta}{p}\right) = 1$, then $D$ has exactly two ideals of norm $p$. These ideals are conjugates of each other.*

(3) *If $\left(\frac{\Delta}{p}\right) = 0$, then $D$ has exactly one ideal of norm $p$.*

*Proof.* An ideal of prime norm $p$ must be primitive, so the number of such ideals is the number of solutions of $\phi(x) \equiv 0 \pmod{p}$, where $\phi(x)$ is the principal polynomial of discriminant $\Delta$. The number of solutions of this quadratic congruence is determined by $\Delta$, as in the three cases above. (See Theorem 0.3.4.) Furthermore, if $k$ is a solution of $\phi(x) \equiv 0 \pmod{p}$, then $-k - \varepsilon$ is as well, so when $\phi(x)$ has two distinct roots modulo $p$, the corresponding ideals are conjugates. □

We again adopt the following standard terminology.

**Definition.** Let $D$ be a quadratic domain and let $p$ be a rational prime.

(1) If $D$ has no ideals of norm $p$, we say that $p$ is *inert* in $D$.

(2) If $D$ has two ideals of norm $p$, we say that $p$ *splits* in $D$.

(3) If $D$ has exactly one ideal of norm $p$, we say that $p$ is *ramified* in $D$.

**Example.** Let $\Delta = 92$ and $p = 7$. Here $\left(\frac{92}{7}\right) = \left(\frac{1}{7}\right) = 1$, with $\phi(x) = x^2 - 23 \equiv 0 \pmod{7}$ having solutions $k = 3$ and $k = -3$. There are two ideals of norm 7

in $D_{92}$, and thus exactly two prime ideals of $D$ containing 7: $P = [7 : 3]$ and $\overline{P} = [7 : -3]$. ◊

**Exercise 3.3.5.** In each part, find all ideals of the given norm $p$ in $D_\Delta$ or explain why there are such ideals.

(a) $p = 23$ in $D_{-7}$.

(b) $p = 2$ in $D_{-23}$.

(c) $p = 5$ in $D_{29}$.

(d) $p = 2$ in $D_{-47}$.

(e) $p = 3$ in $D_{-47}$.

(f) $p = 17$ in $D_{-47}$.

(g) $p = 23$ in $D_{-47}$.

(h) $p = 11$ in $D_{-60}$.

## 3.4 Multiplication of Ideals

In §3.3, we defined prime ideals of quadratic domains in terms of set containment. We now introduce an operation of multiplication on the set of ideals of a quadratic domain, and will see in §3.5 that, in some cases, prime ideals can be regarded as irreducible factors under multiplication.

**Definition.** Let $A$ and $B$ be ideals of a quadratic domain $D$. We define the *product* of $A$ and $B$ to be the set of all finite sums of products of an element from $A$ with an element from $B$, that is,

$$AB = \{v_1w_1 + v_2w_2 + \cdots + v_nw_n \mid v_i \in A \text{ and } w_i \in B\}.$$

**Exercise 3.4.1.** Show that if $A$ and $B$ are ideals of a quadratic domain $D$, then $AB$ is also an ideal of $D$, contained in both $A$ and $B$.

**Exercise 3.4.2.** Let $A$, $B$, and $C$ be ideals of a quadratic domain $D$.

(a) Show that $AB = BA$.

(b) Show that $(AB)C = A(BC)$.

(c) Show that $AD = A$.

(d) Show that $\overline{A} \cdot \overline{B} = \overline{AB}$.

(e) Show that if $v$ and $w$ are elements of $D$, then $\langle v \rangle \langle w \rangle = \langle vw \rangle$.

The operation of ideal multiplication allows a corresponding definition of divisibility for ideals.

**Definition.** Let $A$ and $B$ be ideals of a quadratic domain $D$. We say that $B$ *divides* $A$ if there is some ideal $C$ of $D$ for which $A = BC$.

Since $BC$ is an ideal contained in $B$, a necessary condition for $B$ to divide $A$ is that $B$ contains $A$ as a subset. We will see in Corollary 3.4.3 that in some cases this condition is also sufficient.

**The Index of an Ideal.** Our goal, which we will attain in full in §3.6, is to derive a formula for products of ideals of a quadratic domain $D$ as ideal numbers. As a preliminary step in the remainder of this section, we describe several techniques of ideal multiplication, which will often be sufficient in practice. We begin by introducing the following terminology.

**Definition.** Let $D$ be the quadratic domain of some discriminant $\Delta$, and let $\phi(x) = x^2 + \varepsilon x + \frac{\varepsilon^2 - \Delta}{4}$ be the corresponding principal polynomial. If $A = g[a : k]$ is a nontrivial ideal of $D$, let $\phi(k) = ac$ and let $\phi'(k) = 2k + \varepsilon = b$, and define the *index* of $A$ to be $\gamma(A) = \gcd(a, b, c)$.

Note that $c$ is a rational integer, since if $A = g[a : k]$, then $a$ must divide $\phi(k)$. The values of $b$ and $c$ depend on the particular representative that we use for the character $k$ of $A$, but the following exercise shows that $\gamma(A)$ is independent of that selection.

**Exercise 3.4.3.** Let $A = g[a : k]$ be an ideal of a quadratic domain $D_\Delta$, and let $\ell$ be congruent to $k$ modulo $a$. Let $\phi(x)$ be the principal polynomial of discriminant $\Delta$, and let $ac = \phi(k)$, $b = \phi'(k)$, $ac_0 = \phi(\ell)$, and $b_0 = \phi'(\ell)$. Show that $\gcd(a, b, c) = \gcd(a, b_0, c_0)$, so that the index of $A$ is well-defined.

**Example.** Let $\Delta = \Delta(-3, 2) = -12$, so that $\phi(x) = x^2 + 2x + 4$, and let $D = D_{-12}$. Here $\phi(0) = 4$ and $\phi'(0) = 2$, and so $A = [2 : 0]$ and $B = [4 : 0]$ are ideals of $D$. We find that $\gamma(A) = \gcd(2, 2, 2) = 2$ and $\gamma(B) = \gcd(4, 2, 1) = 1$. ◊

The following proposition shows that there are strong restrictions on the index of an ideal of a quadratic domain $D_\Delta$.

**Proposition 3.4.1.** *Let $A = g[a : k]$ be an ideal of the quadratic domain $D$ with discriminant $\Delta$. If $\gamma = \gamma(A)$, then $\Delta = \gamma^2 \Delta_0$ with $\Delta_0 \equiv 0$ or $1 \pmod 4$.*

*Proof.* Let $\phi(k) = ac$ and $\phi'(k) = b$, where $\phi(x)$ is the principal polynomial of discriminant $\Delta$. If $\gcd(a, b, c) = \gamma$, we can write $a = \gamma a_0$, $b = \gamma b_0$, $c = \gamma c_0$ with

$a_0$, $b_0$, and $c_0$ integers. If $\Delta$ is the discriminant of $D$, then

$$ac = \phi(k) = k^2 + \varepsilon k + \frac{\varepsilon^2 - \Delta}{4} = \frac{(2k+\varepsilon)^2 - \Delta}{4} = \frac{b^2 - \Delta}{4}.$$

But then $b^2 - 4ac = \Delta = \gamma^2\Delta_0$ with $\Delta_0 = b_0^2 - 4a_0c_0 \equiv 0$ or $1 \pmod 4$. □

Proposition 3.4.1 implies that if $\Delta = \Delta(d, \gamma)$, as defined in (2.2.1), and $A$ is a nontrivial ideal of $D_\Delta$, then $\gamma(A)$ divides $\gamma$. That is, the index of an ideal of $D_\Delta$ divides the index of $\Delta$. In particular, if $\Delta = \Delta(d, 1)$, then every ideal $A$ of $D_\Delta$ has index 1. Recall that we say $\Delta$ is a primitive discriminant and that $D_\Delta$ is a complete quadratic domain in this case.

Our next theorem proves to be fundamental in establishing results about norms of ideals, which we apply to ideal multiplication.

**Theorem 3.4.2.** *Let $A$ be an ideal of a quadratic domain $D = D_\Delta$, and let $\overline{A}$ be its conjugate. If the index of $A$ is $\gamma(A) = 1$, then $A\overline{A}$ is the principal ideal of $D$ generated by $N(A)$.*

*Proof.* We may assume that $A$ is a primitive ideal, since $gA \cdot \overline{gA} = g^2 A\overline{A}$ and $N(gA) = g^2N(A)$. So let $A = [a : k]$ be an ideal of $D$. If $w = k + z$ and $\phi(x)$ is the principal polynomial of discriminant $\Delta$, then we can let

$$ac = \phi(k) = w \cdot \overline{w} \quad \text{and} \quad b = \phi'(k) = w + \overline{w}. \tag{3.4.1}$$

We are given that $\gamma(A) = \gcd(a, b, c) = 1$, so there are integers $\ell$, $m$, and $n$ with $a\ell + bm + cn = 1$.

Now the typical product of an element of $A$ with an element of $\overline{A}$ can be written as

$$\begin{aligned}(qa + rw)(sa + t\overline{w}) &= qsa^2 + rsaw + qta\overline{w} + rtw\overline{w} \\ &= a(aqs + rsw + qt\overline{w} + rtc) \end{aligned} \tag{3.4.2}$$

for some integers $q$, $r$, $s$, and $t$. This product is an element of $\langle a\rangle$, as is every finite sum of such products, and so $A\overline{A} \subseteq \langle a\rangle = \langle N(A)\rangle$.

To show the reverse inclusion, note first that $N(v) = v\overline{v}$ is an element of $A\overline{A}$ for all $v$ in $A$. If $v = qa + rw$, then as a special case of equation (3.4.2), and using the expressions in (3.4.1), we have

$$\begin{aligned}N(v) = (qa + rw)(qa + r\overline{w}) &= q^2a^2 + qra(w + \overline{w}) + r^2w\overline{w} \\ &= a(aq^2 + bqr + cr^2). \end{aligned} \tag{3.4.3}$$

Now we find that

$$\begin{aligned}&(\ell - m)N(a) + mN(a + w) + (n - m)N(w) \\ &\quad = (\ell - m)a^2 + ma(a + b + c) + (n - m)ac = a(a\ell + bm + cn) = a.\end{aligned}$$

Thus $a$ is a $\mathbb{Z}$-combination of elements of $A\overline{A}$, so that $\langle a\rangle \subseteq A\overline{A}$. Therefore $A\overline{A} = \langle a\rangle = \langle N(A)\rangle$ when $\gamma(A) = 1$. □

We note two useful consequences of Theorem 3.4.2.

**Corollary 3.4.3.** *Let $A$ and $B$ be ideals of a quadratic domain $D$. If $A$ is a subset of $B$ and the index of $B$ is $\gamma(B) = 1$, then there is an ideal $C$ of $D$ for which $A = BC$.*

*Proof.* If $A$ is a subset of $B$, then $A\overline{B}$ is a subset of $B\overline{B}$, which equals $\langle N(B)\rangle$ when $\gamma(B) = 1$. Thus $A\overline{B} = N(B)\cdot C$ for some ideal $C$ of $D$ (see Exercise 3.1.3). Similarly, $A\overline{B}\cdot B = N(B)\cdot C\cdot B$, so that $N(B)\cdot A = N(B)\cdot BC$. Since $N(B)\neq 0$, it follows that $A = BC$ (see Exercise 3.1.2). □

Corollary 3.4.3 shows that when $B$ is an ideal of index 1, then $B$ divides an ideal $A$ if and only if $B$ contains $A$.

**Corollary 3.4.4.** *Let $A$, $B$, and $C$ be ideals of a quadratic domain $D$. If $AC = BC$ and $\gamma(C) = 1$, then $A = B$.*

*Proof.* If $AC = BC$, then $AC\overline{C} = BC\overline{C}$, so that $N(C)\cdot A = N(C)\cdot B$ by Theorem 3.4.2. Since $N(C)\neq 0$, then $A = B$. □

**Ideal Multiplication in Complete Quadratic Domains.** To conclude §3.4, we describe some practical methods of multiplying ideals expressed as ideal numbers. We restrict our attention to primitive ideals, since if $A$ and $B$ are ideals of $D$, then $(gA)(hB) = (gh)(AB)$. For convenience, we will also assume that $D = D_\Delta$ is a complete quadratic domain, so that $\gamma(A) = 1$ for all ideals $A$ of $D$. If $A$ is written as $[a : k]$ in $D$, then Theorem 3.4.2 can be rephrased as follows:

$$[a : k]\cdot[a : -k-\varepsilon] = \langle a\rangle = a[1 : 0]. \tag{3.4.4}$$

(Here we use Proposition 3.2.4, with $\varepsilon = \varepsilon_\Delta$, in the expression for $\overline{A}$ as an ideal number.) We also have the following important consequence of Theorem 3.4.2.

**Corollary 3.4.5.** *Let $A$ and $B$ be nontrivial ideals of a complete quadratic domain $D$. Then $N(AB) = N(A)\cdot N(B)$.*

*Proof.* Using Theorem 3.4.2 and properties of ideal multiplication from Exercise 3.4.2,

$$\langle N(AB)\rangle = AB\cdot\overline{AB} = A\overline{A}\cdot B\overline{B} = \langle N(A)\rangle\langle N(B)\rangle = \langle N(A)\cdot N(B)\rangle.$$

We conclude that $N(AB) = N(A)\cdot N(B)$ since the norm of a nontrivial ideal is a positive rational integer. □

We can establish two special cases of a formula for ideal multiplication in a complete quadratic domain, identical to results we proved for ideal forms of quadratic integers, and assumed to be true for all ideal numbers in §2.6.

**Theorem 3.4.6.** *Let $A = [a : k]$ and $B = [b : \ell]$ be primitive ideals of a complete quadratic domain $D$. If $\gcd(a, b) = 1$, then $AB = [ab : m]$, where $m \equiv k \pmod{a}$ and $m \equiv \ell \pmod{b}$.*

*Proof.* The ideal $AB$ contains products such as $a(\ell + z) = a\ell + az$ and $(k+z)b = bk + bz$. The divisor of $AB$ is thus a common divisor of $a$ and $b$, and so $AB$ is primitive if $\gcd(a, b) = 1$. Since $D$ is a complete quadratic domain, we have that $N(AB) = N(A) \cdot N(B) = ab$. Thus $AB = [ab : m]$ for some integer $m$. But now $m + z$ is an element of $AB$, which is a subset of $A$, and it follows that $m \equiv k \pmod{a}$. Likewise, $m \equiv \ell \pmod{b}$ since $AB \subseteq B$. □

**Example.** The principal polynomial of the complete quadratic domain $D$ of discriminant $-7$ is $\phi(x) = x^2 + x + 2$. We find that $D$ has two ideals of norm 11 since $\left(\frac{-7}{11}\right) = 1$, namely $A = [11 : 4]$ and $\overline{A} = [11 : -5]$, and two ideals of norm 29, which we can write as $B = [29 : 7]$ and $\overline{B} = [29 : -8]$. We then compute four ideals of $D$ with norm $319 = 11 \cdot 29$,

$$AB = [319 : -51], \quad A\overline{B} = [319 : -95], \quad \overline{A}B = [319 : 94], \quad \overline{AB} = [319 : 50],$$

by solving $m \equiv k \pmod{11}$ and $m \equiv \ell \pmod{29}$ for all choices of $k$ and $\ell$. ◊

**Theorem 3.4.7.** *Let $p$ be a rational prime, and suppose that $P = [p : k]$ is an ideal of a complete quadratic domain $D$ for which $P \neq \overline{P}$. Then for all integers $e \geq 1$, there is some $k_e \equiv k \pmod{p}$ so that $P^e = [p^e : k_e]$.*

*Proof.* We proceed by induction on $e$. The claim of Theorem 3.4.7 is true when $e = 1$, so suppose that $P^e = [p^e : k_e]$ with $k_e \equiv k \pmod{p}$ for some $e \geq 1$. Now $P^{e+1} = P \cdot P^e$ contains the product $p(k_e + z) = pk_e + pz$. If $g$ is the divisor of $P^{e+1}$, then $g$ divides $p$, so that $g = 1$ or $g = p$. But if $g = p$, then $p$ would also divide the coefficient of $z$ in $(k + z)(k_e + z)$, which is $k + k_e + \varepsilon$. This would imply that $k \equiv k_e \equiv -k - \varepsilon \pmod{p}$, but then $P = [p : k] = [p : -k - \varepsilon] = \overline{P}$, contrary to assumption. So we conclude that $g = 1$ and $P^{e+1}$ is primitive. Now $N(P^{e+1}) = N(P) \cdot N(P^e) = p^{e+1}$ by Corollary 3.4.5, and so $P^{e+1} = [p^{e+1} : k_{e+1}]$ for some integer $k_{e+1}$. But $k_{e+1} + z$ is an element of $P^{e+1}$, which is a subset of $P$, and it follows that $k_{e+1} \equiv k \pmod{p}$. The result follows for all $e \geq 1$ by induction. □

**Example.** The principal polynomial of discriminant $\Delta = -31$ is $\phi(x) = x^2 + x + 8$. Since 7 divides $\phi(2) = 14 = \phi(-3)$, then $P = [7 : 2]$ and $\overline{P} = [7 : -3]$ are

distinct ideals of $D$, and so Theorem 3.4.7 applies to powers of $P$. We illustrate the application of this theorem by calculating $P^4$.

Since $\phi(x) = x^2 + x + 8$, then $\phi'(x) = 2x + 1$, and $\phi'(2) = 5$. If $k_e$ is a solution of $\phi(x) \equiv 0 \pmod{7^e}$ congruent to 2 modulo 7, then $k_{e+1} = k_e + 7^e t$ satisfies $\phi(x) \equiv 0 \pmod{7^{e+1}}$ if and only if

$$5t \equiv -\frac{\phi(k_e)}{7^e} \pmod 7.$$

(1) When $e = 1$, then $5t \equiv -\frac{\phi(2)}{7} \equiv -2 \pmod 7$ has solution $t = 1$, so that $k_2 = 2 + 7(1) = 9$ satisfies $\phi(x) \equiv 0 \pmod{7^2}$. This shows that $P^2 = [49 : 9]$.

(2) When $e = 2$, then $5t \equiv -\frac{\phi(9)}{7^2} \equiv -2 \pmod 7$ again has solution $t = 1$, so that $k_3 = 9 + 7^2(1) = 58$ satisfies $\phi(x) \equiv 0 \pmod{7^3}$. Thus $P^3 = [343 : 58]$.

(3) When $e = 3$, then $5t \equiv -\frac{\phi(58)}{7^3} \equiv -10 \pmod 7$ has solution $t = -2$, so that $k_4 = 58 + 7^3(-2) = -628$ satisfies $\phi(x) \equiv 0 \pmod{7^4}$. We conclude that $P^4 = [2401 : -628]$. ◊

**Exercise 3.4.4.** Let $D = D_{61}$. Show that $A = [3 : 0]$ and $B = [5 : 0]$ are ideals of $D$. Use the methods of Theorems 3.4.6 and 3.4.7 to calculate the following ideals as ideal numbers.

(a) $AB$.

(b) $A^2$.

(c) $B^2$.

(d) $A\overline{B}$

(e) $A^2B$.

(f) $A^3$.

(g) $A^3B^2$.

Theorems 3.4.2, 3.4.6, and 3.4.7, together with properties of prime ideal factorization that we will introduce in the next section, are generally sufficient for ideal multiplication in a complete quadratic domain.

## 3.5 Prime Ideal Factorization

We have seen that in an arbitrary quadratic domain, every nonzero element that is not a unit can be written as a product of irreducible elements, although the factors are not always unique. In §3.3, we claimed that prime ideals can be regarded as irreducible elements in a collection of ideals of a quadratic domain. However,

the following example illustrates that not every ideal of a quadratic domain can be expressed as a product of prime ideals, uniquely or otherwise. We will then define a particular type of ideal that allows us to sidestep this difficulty, and will arrive at our main result for Chapter 3, a unique factorization theorem for ideal multiplication.

**Example.** Let $D = D_\Delta$, where $\Delta = \Delta(-3, 2) = -12$. The principal polynomial of discriminant $\Delta$ is $\phi(x) = x^2 + 2x + 4$, hence $A = [4 : 0]$ is an ideal of $D$. If $A$ is written as a product of prime ideals of $D$, then each of those prime ideals must contain $A$. But all rational integers in a prime ideal are multiples of a single rational prime, so with 4 in $A$, we see that any such prime ideal $P$ must contain 2. Since $p = 2$ divides $\Delta$, there is only one prime ideal of $D$ containing 2, namely $P = [2 : 0]$. However, we show as follows that $P^2 \subseteq A \subseteq P$, with both containments proper. If $z = z_\Delta = 1 + \sqrt{-3}$, then

$$P = \{m(2) + n(z) \mid m, n \in \mathbb{Z}\} \quad \text{and} \quad A = \{m(4) + n(z) \mid m, n \in \mathbb{Z}\}.$$

Thus $A \subseteq P$, with 2 an element of $P$ not in $A$, so that $A \neq P$. On the other hand, with $z^2 = -4 + 2z$, the typical product of two elements of $P$ is

$$(2q + rz)(2s + tz) = 4(qs - rt) + 2(qt + rs + rt)z.$$

In the sum of any finite number of such products, the coefficient of $z$ is even while the constant coefficient is divisible by 4. Therefore we see that $P^2 \subseteq A$, but that $z$ is an element of $A$ not in $P^2$, so that $A \neq P^2$. But now with $P^e \subseteq P^2$ when $e > 2$, it follows that $A$ cannot equal $P^e$ for any positive integer $e$, and so cannot be expressed as a product of prime ideals of $D$. ◊

**Definition.** Let $D$ be the quadratic domain of discriminant $\Delta = \Delta(d, \gamma)$ for some squarefree $d \neq 1$ and positive integer $\gamma$. We will say that an ideal $A$ of $D$ is a *complete* ideal if $\gcd(N(A), \gamma) = 1$.

If $\Delta = \Delta(d, 1)$ is a *primitive* discriminant, then every nontrivial ideal of $D$ has this property. In other words, every nontrivial ideal of a complete quadratic domain is complete. Furthermore, if $\gcd(N(A), \gamma) = 1$ and $A$ is contained in an ideal $B$, then $N(B)$ divides $N(A)$ and so $\gcd(N(B), \gamma) = 1$. That is, if $A \subseteq B$ are ideals of $D$ and $A$ is complete, then $B$ is also complete. Finally, note that if $A$ is a complete ideal of $D$, then $\gamma(A) = 1$, as the index of an ideal $A$ is a common divisor of $N(A)$ and the index of $\Delta$. (The converse of this statement is not generally true, however. If $A = [4 : 0]$ in $D_{-12}$ as in the preceding example, then $\phi(0) = 4 \cdot 1$ and $\phi'(0) = 2$, so that $\gamma(A) = \gcd(4, 2, 1) = 1$, but $\gcd(N(A), \gamma_{-12}) = \gcd(4, 2) = 2$.)

**Theorem 3.5.1.** *Every proper complete ideal of a quadratic domain $D$ can be written as a product of prime ideals of $D$.*

*Proof.* Let $A$ be a proper complete ideal of a quadratic domain $D$. To show that $A$ can be written in some way as a product of prime ideals, suppose instead that $N(A)$ is as small as possible among all *complete* ideals of $D$ that cannot be expressed in that form. Then $A$ is not prime, as we regard a prime ideal as a product of prime ideals with only one term. Thus, by definition, there is a proper ideal $B$ of $D$ that properly contains $A$. As noted above, $B$ is also complete, so that $\gamma(B) = 1$, and thus Corollary 3.4.3 applies. There is an ideal $C$ of $D$ with $A = BC$, and $C$ is complete since $A \subseteq C$. Now since each ideal has index 1, Theorem 3.4.2 implies that

$$\langle N(A)\rangle = A\overline{A} = BC \cdot \overline{BC} = B\overline{B} \cdot C\overline{C} = \langle N(B)\rangle \langle N(C)\rangle = \langle N(B) \cdot N(C)\rangle,$$

from which it follows that $N(A) = N(B) \cdot N(C)$. With neither $B$ nor $C$ equal to $D$, then $1 < N(B), N(C) < N(A)$. But now by assumption, both $B$ and $C$, and therefore $A = BC$, can be written as products of prime ideals. □

To prove the uniqueness of this prime ideal factorization, we require the following lemma.

**Lemma 3.5.2.** *Let $P$ be a proper complete ideal of a quadratic domain $D$. Then $P$ is a prime ideal of $D$ if and only if the following statement is true: if $A$ and $B$ are ideals of $D$ for which $AB$ is a subset of $P$, then either $A$ is a subset of $P$ or $B$ is a subset of $P$.*

*Proof.* Suppose first that $P$ is a prime ideal of $D$, and let $A$ and $B$ be ideals of $D$ for which $AB \subseteq P$. If $A$ is not a subset of $P$, then there is some element $v$ of $A$ that is not in $P$. If $w$ is any element of $B$, then $vw$ is an element of $AB$, so must be in $P$. But now since $v$ is not in $P$, we must conclude that $w$ is in $P$ by Proposition 3.3.2. Since this is true for an arbitrary element $w$ of $B$, we conclude that $B$ is a subset of $P$.

Conversely, suppose that $P$ is a proper complete ideal of $D$ with the property that $AB \subseteq P$ implies $A \subseteq P$ or $B \subseteq P$ when $A$ and $B$ are ideals of $D$. To show that $P$ is a prime ideal of $D$, suppose that $Q$ is an ideal of $D$ with $P \subseteq Q \subseteq D$. Then $Q$ is complete, and Corollary 3.4.3 shows that $P = QC$ for some ideal $C$ of $D$. Since $QC \subseteq P$, then either $Q \subseteq P$ or $C \subseteq P$. If $Q \subseteq P$, we immediately conclude that $Q = P$. On the other hand, if $C \subseteq P$, then $P = QC \subseteq PQ$. But since $PQ \subseteq P$ is always true, we have that $PQ = P = PD$, and conclude that $Q = D$ by Corollary 3.4.4. So there is no proper ideal $Q$ of $D$ that properly contains $P$, and $P$ is a prime ideal of $D$ by definition. □

**Theorem 3.5.3.** *Let $A$ be a proper complete ideal of a quadratic domain $D$. Then $A$ can be written uniquely, aside from the order of the factors, as a product of prime ideals of $D$.*

*Proof.* By Theorem 3.5.1, it remains only to show the uniqueness of the prime ideal factorization of $A$. Suppose that $A = P_1P_2 \cdots P_k = Q_1Q_2 \cdots Q_\ell$ with each $P_i$ and $Q_j$ prime. Each of these factors is also a complete ideal. We can assume that $P_i \neq Q_j$ for all $1 \leq i \leq k$ and $1 \leq j \leq \ell$, since otherwise we could cancel the common factor from both sides of the equation by Corollary 3.4.4. Notice that $P_1$ contains $A = Q_1Q_2 \cdots Q_\ell$. By Lemma 3.5.2, it follows that $P_1$ contains $Q_1$ or that $P_1$ contains $Q_2 \cdots Q_\ell$. Continuing in this way, $P_1$ must contain $Q_j$ for some $j$ with $1 \leq j \leq \ell$. Rearranging terms if necessary, we may assume that $P_1$ contains $Q_1$. But $Q_1$ is a prime ideal of $D$, so $Q_1 \subseteq P_1$ implies that either $P_1 = Q_1$ or $P_1 = D$. By definition, the prime ideal $P_1$ is a proper ideal of $D$, so we must conclude that $P_1 = Q_1$. This contradicts our assumption, so we must conclude that the two expressions for $A$ as products of prime ideals are the same, aside from rearrangements of the terms. □

**Factoring Ideals.** Prime ideal decomposition of a complete ideal of a quadratic domain is straightforward in practice, as our next theorem demonstrates.

**Theorem 3.5.4.** *Let $D$ be a quadratic domain with discriminant $\Delta$, and let $A = [a : k]$ be a primitive complete ideal of $D$. If $a = bc$ for rational integers $b$ and $c$, then $A = BC$, where $B = [b : k]$ and $C = [c : k]$.*

*Proof.* Let $\phi(x)$ be the principal polynomial of discriminant $\Delta$. If $A = [a : k]$ is a complete ideal of $D$, then $a = bc$ divides $\phi(k)$, and it follows that $B = [b : k]$ and $C = [c : k]$ are also ideals of $D$, and both contain $A$ by Proposition 3.3.1. Since each ideal is complete, we find that $N(BC) = N(B) \cdot N(C) = bc = a = N(A)$, as in the proof of Theorem 3.5.1. If we can show that $BC$ is a subset of $A$, then it follows that $A = BC$ by Exercise 3.3.4. But if $qb + r(k + z)$ is in $B$ and $sc + t(k + z)$ is in $C$ (for some integers $q$, $r$, $s$, and $t$), then their product,

$$(qb + r(k + z))(sc + t(k + z)) = qs \cdot a + (qbt + rsc + rt(k + z)) \cdot (k + z),$$

is an element of $A$ by closure properties of an ideal. Thus $BC \subseteq A$, and so $A = BC$. □

The factorization method of Theorem 3.5.4 might fail when $A$ is not complete. For instance, $[4 : 0]$ is not equal to $[2 : 0] \cdot [2 : 0]$ in $D_{-12}$, as we noted in a previous example. However, Theorem 3.5.4 applies to every ideal of a complete quadratic domain.

**Example.** Let $D$ be the complete quadratic domain with discriminant $\Delta = \Delta(-5, 1) = -20$, so that $\phi(x) = x^2 + 5$. Since $a = 282$ divides $\phi(29) = 846$, we find that $A = [282 : 29]$ is an ideal of $D$. With $282 = 2 \cdot 3 \cdot 47$, Theorem 3.5.4 implies that

$$A = [2 : 29] \cdot [3 : 29] \cdot [47 : 29] = [2 : 1] \cdot [3 : -1] \cdot [47 : -18],$$

among other possible representations. Each factor is a prime ideal, since the norm of each is a rational prime. ◊

**Exercise 3.5.1.** In each part, verify that $A$ is an ideal of the quadratic domain $D$ with the given primitive discriminant $\Delta$, and find the prime ideal factorization of $A$ in $D$.

(a) $A = [615 : 35]$, with $\Delta = -20$.

(b) $A = [775 : 39]$, with $\Delta = 41$.

(c) $A = [220 : 29]$, with $\Delta = -39$.

More generally, if $A$ is a complete ideal of $D = D_\Delta$ and $\gcd(g, \gamma_\Delta) = 1$, then $B = gA = \langle g \rangle A$ is also a complete ideal of $D$. If a prime number $p$ divides $g$, then $\langle p \rangle$ is a factor of $\langle g \rangle$. That ideal may be prime or may factor further, according to Theorem 3.3.5.

**Example.** In §3.1, we found that there are six ideals of $D = D_{316}$ having norm 45:

$$[45 : 13], \quad [45 : -13], \quad [45 : 22], \quad [45 : -22], \quad 3[5 : 2], \quad 3[5 : -2].$$

Here $316 = \Delta(79, 1)$, so all ideals are complete, and we can apply Theorem 3.5.4 to find the prime factorizations of these ideals. With $\phi(x) = x^2 - 79$, we find that $P = [3 : 1]$, $\overline{P} = [3 : -1]$, $Q = [5 : 2]$, and $\overline{Q} = [5 : -2]$ are prime ideals of $D$. Then:

(1) $[45 : 13] = [3 : 1] \cdot [3 : 1] \cdot [5 : -2] = P^2 \cdot \overline{Q}$,

(2) $[45 : -13] = [3 : -1] \cdot [3 : -1] \cdot [5 : 2] = \overline{P}^2 \cdot Q$,

(3) $[45 : 22] = [3 : 1] \cdot [3 : 1] \cdot [5 : 2] = P^2 \cdot Q$,

(4) $[45 : -22] = [3 : -1] \cdot [3 : -1] \cdot [5 : -2] = \overline{P}^2 \cdot \overline{Q}$,

(5) $3[5 : 2] = P \cdot \overline{P} \cdot Q$,

(6) $3[5 : -2] = P \cdot \overline{P} \cdot \overline{Q}$.

(We use the fact that $P \cdot \overline{P} = \langle 3 \rangle$ in the final two calculations.) Notice that these six products represent all possible ways of multiplying two of the prime ideals of norm 3 with one prime ideal of norm 5. ◊

**Exercise 3.5.2.** For each ideal $A$ of norm 75 in $D = D_{124}$ (found in Exercise 3.1.8), find the factorization of $A$ into prime ideals of $D$.

**Exercise 3.5.3.** In each part, write the ideal $A$ as an ideal number, and find the prime ideal factorization of $A$ in the given quadratic domain $D_\Delta$. (In each part, $z$ is the basis element of discriminant $\Delta$.)

(a) $A = \langle 4 - 6z \rangle$ in $D_{40}$.

(b) $A = \langle 4 + 3z \rangle$ in $D_{-11}$.

(c) $A = \langle 6 + 12z \rangle$ in $D_{-68}$.

(d) $A = \langle -2 + 3z \rangle$ in $D_{-23}$.

(e) $A = \langle 23 + 3z \rangle$ in $D_{220}$.

**Example.** Let $A = 7[133 : 22]$, an ideal of $D = D_{-12}$ since $\phi(22) = 22^2 + 2 \cdot 22 + 4 = 532 = 133 \cdot 4$. Here $N(A) = 7^2 \cdot 133 = 6517$ is relatively prime to $\gamma_{-12} = 2$, so $A$ can be written as a product of prime ideals. We have $\left(\frac{-12}{7}\right) = \left(\frac{2}{7}\right) = 1$, which means that $\langle 7 \rangle = 7[1 : 0]$ factors as a product of two prime ideals of $D$—we find that $\langle 7 \rangle = [7 : 1] \cdot [7 : -3]$. Now with $133 = 7 \cdot 19$,

$$7[133 : 22] = [7 : 1] \cdot [7 : -3] \cdot [7 : 22] \cdot [19 : 22] = [7 : 1]^2 \cdot [7 : -3] \cdot [19 : 3]$$

is the prime ideal factorization of $A$. ◊

**Exercise 3.5.4.** Let $D$ be the quadratic domain of discriminant $\Delta = \Delta(-11, 5) = -275$. Find the prime ideal factorization of each of the following ideals of $D$, or explain why it is impossible to do so.

(a) $[25 : 0]$.

(b) $[27 : 1]$.

(c) $[99 : 3]$.

Our next example illustrates how we might calculate a product of ideals in a complete quadratic domain by first applying Theorem 3.5.4 to write both ideals as products of prime ideals.

**Example.** Let $A = [42 : 17]$ and $B = [138 : -61]$ in the complete quadratic domain $D = D_{-20}$. Using Theorem 3.5.4, we find that

$$A = [2 : 1] \cdot [3 : -1] \cdot [7 : 3] \quad \text{and} \quad B = [2 : 1] \cdot [3 : -1] \cdot [23 : 8].$$

Thus

$$AB = [2 : 1]^2 \cdot [3 : -1]^2 \cdot [7 : 3] \cdot [23 : 8].$$

Theorem 3.4.7 does not apply to $[2 : 1]^2$, since $P = [2 : 1] = [2 : -1] = \overline{P}$. Instead, we have that $[2 : 1]^2 = P\overline{P} = \langle 2 \rangle$ by Theorem 3.4.2. On the other hand,

Theorem 3.4.7 implies that $[3 : -1]^2 = [9 : k]$, where $k \equiv -1 \pmod 3$ and 9 divides $\phi(k) = k^2 + 5$. We find that $[3 : -1]^2 = [9 : 2]$. Finally, two applications of Theorem 3.4.6 show that $[9 : 2] \cdot [7 : 3] \cdot [23 : 8]$ equals $[1449 : k]$, where

$$k \equiv 2 \pmod 9, \quad k \equiv 3 \pmod 7, \quad \text{and} \quad k \equiv 8 \pmod{23}.$$

Applying the Chinese Remainder Theorem, we find that $k \equiv 353 \pmod{1449}$, and we conclude that $AB = 2[1449 : 353]$. ◊

We conclude this section with two examples that demonstrate how prime ideal factorization can resolve the different irreducible factorizations that occur in many examples of quadratic domains. (We had noted this, more informally, using ideal numbers in §2.6.)

**Example.** Let $D = D_{-20}$, with $z = \sqrt{-5}$. In §2.5, we saw that $6 = 2 \cdot 3 = (1 + z)(1 - z)$, with each factor in the two products irreducible in $D$, and no two of them associates. We can similarly express $\langle 6 \rangle$ as two different products of principal ideals: $\langle 6 \rangle = \langle 2 \rangle \langle 3 \rangle = \langle 1 + z \rangle \langle 1 - z \rangle$. With $D$ a complete quadratic domain, we can decompose all ideals into prime factors. Here we find that $\langle 2 \rangle = P^2$ and $\langle 3 \rangle = Q\overline{Q}$, where $P = [2 : 1]$ and $Q = [3 : 1]$ are prime ideals. By Theorems 3.2.2 and 3.5.4, we also find that

$$\langle 1 + z \rangle = [6 : 1] = [2 : 1] \cdot [3 : 1] = PQ$$

and

$$\langle 1 - z \rangle = [6 : -1] = [2 : 1] \cdot [3 : -1] = P\overline{Q}.$$

Therefore the different factorizations of $\langle 6 \rangle$ into *principal* ideals are simply different groupings of the *unique* factorization of $\langle 6 \rangle$ into prime ideals of $D$:

$$\langle 6 \rangle = \langle 2 \rangle \langle 3 \rangle = (P^2)(Q\overline{Q}) = (PQ)(P\overline{Q}) = \langle 1 + z \rangle \langle 1 - z \rangle .$$

Note that $P$, $Q$, and $\overline{Q}$ are not principal ideals, since $D$ contains no elements of norm 2 or 3. ◊

**Example.** Let $D$ be the quadratic domain with discriminant $\Delta = -164 = \Delta(-41, 1)$, so that $z = \sqrt{-41}$. In $D$, we can write $45 = 3 \cdot 3 \cdot 5 = (2 + z)(2 - z)$. Here $\langle 3 \rangle = P\overline{P}$ and $\langle 5 \rangle = Q\overline{Q}$, where $P = [3 : 1]$ and $Q = [5 : 2]$. Theorem 3.2.2 implies that $\langle 2 + z \rangle = [45 : 2] = [3 : 2]^2[5 : 2] = \overline{P^2}Q$ and, likewise, $\langle 2 - z \rangle = P^2\overline{Q}$. Thus

$$\langle 3 \rangle \langle 3 \rangle \langle 5 \rangle = P\overline{P} \cdot P\overline{P} \cdot Q\overline{Q} = \overline{P^2}Q \cdot P^2\overline{Q} = \langle 2 + z \rangle \langle 2 - z \rangle$$

represent different arrangements of the unique prime ideal factorization of $\langle 45 \rangle$ as $P^2\overline{P^2}Q\overline{Q}$. ◊

**Exercise 3.5.5.** For each rational integer $a$, find the prime ideal factorization of $\langle a \rangle$ in the given quadratic domain $D = D_\Delta$. Find all ways of writing $a$ as a product of irreducible elements in $D$, and use the prime ideal factorization to explain any distinct factorizations that exist.

(a) $a = 49$ in $D_{-40}$.

(b) $a = 16$ in $D_{-15}$.

(c) $a = 85$ in $D_{-84}$.

(d) $a = 12$ in $D_{-23}$.

(e) $a = 130$ in $D_{-120}$.

(f) $a = 42$ in $D_{-132}$.

(g) $a = 150$ in $D_{-35}$.

The preceding examples illustrate that we can use ideals to factor elements that are irreducible but not prime in a quadratic domain $D$. Roughly speaking, principal ideals of $D$ correspond to elements of $D$—actually to sets of elements that are associates of each other—while ideals that are not principal might be viewed as the "ideal numbers" required in some cases to obtain unique factorization.

## 3.6 A Formula for Ideal Multiplication

To conclude Chapter 3, we derive a formula for the product of two primitive ideals, written as ideal numbers, which holds in an arbitrary quadratic domain. We will state our main result first, and illustrate the calculation with several examples, before presenting a proof, which depends on some technical preliminaries.

**Theorem 3.6.1.** *Let $A = [a : k]$ and $B = [b : \ell]$ be primitive ideals of the quadratic domain $D$ of discriminant $\Delta$, with $\gamma = \gcd(\gamma(A), \gamma(B))$. Let $\phi(x)$ be the principal polynomial of discriminant $\Delta$, and let $t = k + \ell + \phi'(0)$. Then $AB$ can be written as $g[c : m]$, where $g = \gcd(a, b, t)$, $c = ab\gamma/g^2$, and $m$ satisfies the following congruences:*

$$\frac{a}{g} \cdot m \equiv \frac{a}{g} \cdot \ell \pmod{c}, \tag{3.6.1}$$

$$\frac{b}{g} \cdot m \equiv \frac{b}{g} \cdot k \pmod{c}, \tag{3.6.2}$$

$$\frac{t}{g} \cdot m \equiv \frac{1}{g}(k\ell - \phi(0)) \pmod{c}. \tag{3.6.3}$$

Note that $\phi(0)$ and $\phi'(0)$ are the constant coefficient and linear coefficient of $\phi(x)$, respectively. If the congruences in (3.6.1), (3.6.2), and (3.6.3) have a solution (which we will see must be the case in the proof of Theorem 3.6.1), then that solution is unique modulo $c$, since $\gcd\left(\frac{a}{g}, \frac{b}{g}, \frac{t}{g}\right) = 1$. (This follows by the same argument as in Exercise 0.1.11.) Congruences (3.6.1) and (3.6.2) simplify to

$$m \equiv \ell \pmod{b\gamma/g} \quad \text{and} \quad m \equiv k \pmod{a\gamma/g}, \tag{3.6.4}$$

respectively, by the congruence cancellation property (Proposition 0.1.6). The following exercise ensures that the right-hand side of congruence (3.6.3) is an integer.

**Exercise 3.6.1.** Show that if $t = k + \ell + \phi'(0)$, then $k\ell - \phi(0) = kt - \phi(k)$. Show that then $g = \gcd(a, b, t)$ must divide $k\ell - \phi(0)$.

In practice, it is not always necessary to consider all three congruences to determine $m$ modulo $c$. We illustrate this with several examples, the first three of which confirm calculations by other means in §3.4 and §3.5.

**Example.** Let $A = [11 : 4]$ and $B = [29 : 7]$ in $D = D_{-7}$, a complete quadratic domain, so that $\gamma(A) = \gamma(B) = \gamma = 1$. Since $\gcd(11, 29) = 1$, then $g = 1$ and $c = 11 \cdot 29 = 319$. The congruences of (3.6.4) are $m \equiv 7 \pmod{29}$ and $m \equiv 4 \pmod{11}$, which we find have a unique solution modulo 319, namely $m = -51$, the same calculation as in an example following Theorem 3.4.6. Here it was unnecessary to calculate $t$ in the notation of Theorem 3.6.1. But with $\phi(x) = x^2 + x + 2$, we find that $t = 4 + 7 + 1 = 12$ and $k\ell - \phi(0) = 4 \cdot 7 - 2 = 26$. We can verify that $m = -51$ also satisfies the congruence $12m \equiv 26 \pmod{319}$. In any event, $AB = [319 : -51]$. ◊

**Example.** Let $P = [7 : 2]$ in the complete quadratic domain $D = D_{-31}$, with $\phi(x) = x^2 + x + 8$. To calculate $P^2$ by Theorem 3.6.1, let $a = 7 = b$ and $k = 2 = \ell$. Here $t = 2 + 2 + 1 = 5$, and so $g = \gcd(7, 7, 5) = 1$ and $c = 49$. The congruences in (3.6.1) and (3.6.2) both become $7m \equiv 14 \pmod{49}$, not sufficient to calculate $m$ modulo 49. But $k\ell - \phi(0) = 2 \cdot 2 - 8 = -4$, and $5m \equiv -4 \pmod{49}$ has the unique solution $m \equiv 9 \pmod{49}$. So $P^2 = [49 : 9]$, as we found in an example following Theorem 3.4.7. ◊

**Exercise 3.6.2.** If $P$ and $D$ are as in the preceding example, use Theorem 3.6.1 to calculate $P^4$ directly as $P^2 \cdot P^2$.

**Example.** Let $A = [42 : 17]$ and $B = [138 : -61]$ in $D = D_{-20}$, with $\phi(x) = x^2 + 5$. Here $t = -44$ and $g = \gcd(42, 138, -44) = 2$, so that $c = (42 \cdot 138)/2^2 = 1449$ in the notation of Theorem 3.6.1. Congruences (3.6.1) and (3.6.2) reduce to

$m \equiv -61 \pmod{69}$ and $m \equiv 17 \pmod{21}$, not sufficient to calculate $m$ modulo 1449 since $\gcd(69, 21) = 3$. On the other hand, congruence (3.6.3) is

$$-22m \equiv \tfrac{1}{2}(17(-61) - 5) \equiv -521 \pmod{1449},$$

with a unique solution $m = 353$. Thus $AB = 2[1449 : 353]$. We saw this calculation by a different approach in §3.5. ◊

**Example.** Let $A = [2 : 0]$ in $D = D_{-12}$, so that $\phi(x) = x^2 + 2x + 4$. To calculate $A^2$ by Theorem 3.6.1, we let $a = 2 = b$ and $k = 0 = \ell$. With $\phi(0) = 4 = 2 \cdot 2$ and $\phi'(0) = 2$, we find that $\gamma(A) = \gcd(2, 2, 2) = 2$. In the notation of Theorem 3.6.1, then $\gamma = \gcd(2, 2) = 2$. We have that $t = 0+0+2 = 2$, hence $g = \gcd(a, b, t) = 2$ and $c = (2 \cdot 2 \cdot 2)/2^2 = 2$. So $A^2 = 2[2 : m]$ for some $m$. Any of the congruences (3.6.1), (3.6.2), or (3.6.3) is sufficient to conclude that $m \equiv 0 \pmod{2}$. Thus $A^2 = 2[2 : 0]$, a calculation we confirm below. ◊

In each example thus far, congruence (3.6.3) is sufficient to determine $m$ modulo $c$. This is not always the case, as our final example illustrates.

**Example.** Let $\Delta = \Delta(-21, 1) = -84$, so that $\phi(x) = x^2 + 21$. We find that $A = [3 : 0]$ and $B = [7 : 0]$ are ideals of $D = D_\Delta$. Here $\gamma = 1$ and $t = 0+0+0 = 0$, implying that $g = \gcd(3, 7, 0) = 1$. Thus $c = (3 \cdot 7 \cdot 1)/1^2 = 21$, and $AB = [21 : m]$ for some $m$. In this example, congruence (3.6.3) is $0 \cdot m \equiv -21 \pmod{21}$, which gives us no information about $m$. But from (3.6.4), we find that $m \equiv 0 \pmod{7}$ and $m \equiv 0 \pmod{3}$, and we conclude that $m \equiv 0 \pmod{21}$. Therefore $AB = [21 : 0]$. ◊

**Exercise 3.6.3.** In each part, verify that $A$ and $B$ are ideals of the given quadratic domain $D_\Delta$, and use Theorem 3.6.1 to calculate $AB$.

(a) $A = [6 : 1]$ and $B = [14 : 3]$ in $D_{-20}$.

(b) $A = [6 : 1]$ and $B = [21 : 4]$ in $D_{-20}$.

(c) $A = [6 : 1]$ and $B = [21 : -4]$ in $D_{-20}$.

(d) $A = [36 : 14]$ and $B = [142 : 20]$ in $D_{-23}$.

(e) $A = [36 : 14]$ and $B = [142 : -21]$ in $D_{-23}$.

**Exercise 3.6.4.** Let $D$ be the quadratic domain of discriminant $\Delta = \Delta(-5, 3) = -180$. Use Theorem 3.6.1 to calculate each of the following products of ideals of $D$.

(a) $[3 : 0] \cdot [3 : 0]$.

(b) $[9 : 0] \cdot [3 : 0]$.

(c) $[9 : 3] \cdot [3 : 0]$.

(d) $[9 : 0] \cdot [9 : 3]$.

(e) $[9 : 0] \cdot [9 : 0]$.

(f) $[9 : 3] \cdot [9 : 3]$.

(g) $[9 : -3] \cdot [9 : 3]$.

(h) $[27 : 3] \cdot [9 : 3]$.

**Exercise 3.6.5.** Let $D$ be the quadratic domain of discriminant $\Delta = \Delta(-11, 5) = -275$. Use Theorem 3.6.1 to calculate each of the following products of ideals of $D$.

(a) $[5 : 0] \cdot [25 : 0]$.

(b) $[5 : 0] \cdot [25 : 5]$.

(c) $[25 : 0] \cdot [25 : 0]$.

(d) $[25 : 0] \cdot [25 : 5]$.

(e) $[25 : 0] \cdot [25 : 10]$.

(f) $[25 : 5] \cdot [25 : 5]$.

(g) $[25 : 5] \cdot [25 : 10]$.

(h) $[25 : 10] \cdot [25 : 10]$.

**Complete Quadratic Domains and Subdomains.** To prove Theorem 3.6.1, we establish a connection between ideals of a complete quadratic domain and ideals of one of its subdomains with the following proposition.

**Proposition 3.6.2.** *Let $\Delta = \Delta(d, \gamma)$ be a discriminant, and for some fixed positive integer $g$, let $\Delta_1 = g^2\Delta = \Delta(d, g\gamma)$. Let $D$ and $D_1$ be the quadratic domains of discriminant $\Delta$ and $\Delta_1$, respectively. If $A$ is an ideal of $D$, written as $A = h[a : k]$, then $A_1 = \{gv \mid v \in A\}$ is an ideal of $D_1$, which equals $h[ga : gk]_{\Delta_1}$ in ideal number notation. In this case, $\gamma(A_1) = g \cdot \gamma(A)$. Conversely, if $A_1$ is an ideal of $D_1$ with $\gamma(A_1)$ divisible by $g$, then there is an ideal $A$ of $D$ so that $A_1 = \{gv \mid v \in A\}$.*

Some observations are in order before we prove Proposition 3.6.2. Note that $A_1 = \{gv \mid v \in A\}$ is the same as the set $gA$. This means that $gA$ can be regarded both as an ideal of $D$ and as an ideal of $D_1$. (To avoid confusion, we will write this set only as $gA$ when viewing it as an ideal of $D$ and only as $A_1$ when viewing it as an ideal of $D_1$.) The main claim of Proposition 3.6.2 can be expressed as the following equation in ideal number notation:

$$g \cdot h[a : k]_\Delta = h[ga : gk]_{g^2\Delta}. \tag{3.6.5}$$

Certain properties of this ideal might differ depending on how it is viewed. For instance, equation (3.6.5) implies that $N(gA) = g^2 \cdot N(A) = g^2h^2a$ while $N(A_1) = h^2ga$. (In Exercise 3.1.10, we saw that the norm of an ideal $A$ of $D$ is the number of equivalence classes of elements of $D$ under the relation of congruence modulo $A$. Thus $N(A)$ depends both on the ideal and the domain that contains it.) We note other distinctions between $gA$ and $A_1$ in examples below. The following result is needed in the proof of Proposition 3.6.2.

**Exercise 3.6.6.** Let $D = D_\Delta$ be a quadratic domain and let $D_1 = D_{\Delta_1}$ be a subdomain of $D$, where $\Delta_1 = g^2\Delta$ for some positive integer $g$. Show that if $A$ is an ideal of $D$, then $A_1 = A \cap D_1$ is an ideal of $D_1$.

*Proof of Proposition* 3.6.2. Let $z = z_\Delta$ and $\varepsilon = \varepsilon_\Delta$ be the basis element and basis index respectively of discriminant $\Delta$, with $z_1 = z_{\Delta_1}$ and $\varepsilon_1 = \varepsilon_{\Delta_1}$ the corresponding values for $\Delta_1 = g^2\Delta$. In the proof of Proposition 2.2.4, we saw that $z_1 = gz$ and $\varepsilon_1 = g\varepsilon$. So if $v = m + nz$ is an element of $D$, then $gv = gm + gnz = gm + nz_1$ is an element of $D_1$. Since $gA$ is an ideal of $D$, then $gA \cap D_1$ is an ideal of $D_1$ by Exercise 3.6.6. But here we see that $gA = \{gv \mid v \in A\}$ is a subset of $D_1$. Thus $gA = A_1$ is an ideal of $D_1$.

Let $A = h[a : k] = \{m(ha) + n(hk + hz) \mid m, n \in \mathbb{Z}\}$ be an ideal of $D$. Then

$$\begin{aligned} A_1 &= \{m(gha) + n(ghk + ghz) \mid m, n \in \mathbb{Z}\} \\ &= \{m(h(ga)) + n(h(gk + z_1)) \mid m, n \in \mathbb{Z}\}, \end{aligned}$$

which implies that $A_1 = h[ga : gk]$ when viewed as an ideal number of discriminant $\Delta_1$.

Let $\phi(x)$ and $\phi_1(x)$ be the principal polynomials of discriminant $\Delta$ and $\Delta_1$ respectively. If $\phi(k) = ac$ and $\phi'(k) = b$, then by Proposition 2.2.4, we have that $\phi_1(gk) = g^2\phi(k) = (ga)(gc)$ and $\phi_1'(gk) = g\phi'(k) = gb$. So the index of $A_1$, as an ideal of $D_1$, is

$$\gamma(A_1) = \gcd(ga, gb, gc) = g \cdot \gcd(a, b, c) = g \cdot \gamma(A).$$

Conversely, let $A_1 = h[a_1 : k_1]$ be an ideal of $D_1$ for which $g$ divides $\gamma(A_1)$. So if $\phi_1(k_1) = a_1c_1$ and $\phi_1'(k_1) = b_1$, then we can write $a_1 = ga$, $b_1 = gb$, and $c_1 = gc$ for some integers $a$, $b$, and $c$. Recall from the proof of Proposition 3.4.1 that $b^2 - 4ac = \Delta$, the discriminant of $D$, and so $b_1^2 - 4a_1c_1 = \Delta_1$. Now we see that

$$k_1 = \frac{b_1 - \varepsilon_1}{2} = \frac{gb - g\varepsilon}{2} = g \cdot \frac{b - \varepsilon}{2} = gk$$

for some integer $k$, since $b$ and $\varepsilon$ both have the same parity as $\Delta = b^2 - 4ac$. We find that $A = h[a : k]$ is an ideal of $D$, and that $A_1 = gA$ as above. □

**Example.** Let $D = D_{-3}$, so that $\phi(x) = x^2 + x + 1$ and $z = \frac{1+\sqrt{-3}}{2}$. If $A = D = [1 : 0]$ and $g = 2$, then $2A$ can be written as

$$2[1 : 0] = \{2m(1) + 2n(z) \mid m, n \in \mathbb{Z}\} = \left\{2m + n(1 + \sqrt{-3}) \mid m, n \in \mathbb{Z}\right\}.$$

On the other hand, if $D_1 = D_{-12}$, with $\phi_1(x) = x^2 + 2x + 4$ and $z_1 = 1 + \sqrt{-3}$, then $A_1$ equals

$$[2 : 0] = \{m(2) + n(z_1) \mid m, n \in \mathbb{Z}\} = \left\{2m + n(1 + \sqrt{-3}) \mid m, n \in \mathbb{Z}\right\}.$$

These ideals contain exactly the same elements. ◊

To generalize this example, if $\Delta_1 = g^2\Delta$ for some discriminant $\Delta$, then $[g : 0]$ is an ideal of $D_1 = D_{\Delta_1}$, equal to $\langle g \rangle = g[1 : 0]$ as an ideal of $D = D_\Delta$. We use this ideal in the following extension of Theorem 3.4.2.

**Theorem 3.6.3.** *Let $\Delta_1 = g^2\Delta$, where $g$ is a positive integer and $\Delta$ is a discriminant. Let $A_1$ be an ideal of $D_1 = D_{\Delta_1}$ with $\gamma(A_1) = g$ and let $\overline{A_1}$ be its conjugate. Then $A_1\overline{A_1} = N(A_1)B$, where $B = [g : 0]$ in $D_1$.*

*Proof.* If $\gamma(A_1) = g$, then $A_1 = \{gv \mid v \in A\} = gA$ for some ideal $A$ of $D = D_\Delta$ with $\gamma(A) = 1$, as in Proposition 3.6.2. We saw that if $A_1 = h[a_1 : k_1]$, then $a_1 = ga$ and $k_1 = gk$ for some integers $a$ and $k$, and $A = h[a : k]$. So then $N(A_1) = h^2a_1 = g(h^2a) = gN(A)$. But now by Theorem 3.4.2, and using equation (3.6.5), we find that

$$A_1\overline{A_1} = gA \cdot \overline{gA} = g^2 \langle N(A) \rangle = g^2N(A)[1 : 0]_\Delta = gN(A)[g : 0]_{\Delta_1} = N(A_1)B,$$

where $B = [g : 0]$ is an ideal of $D_1$. □

**Corollary 3.6.4.** *If $A$ is a nontrivial principal ideal of a quadratic domain $D$, then $\gamma(A) = 1$.*

*Proof.* Let $A = \langle v \rangle$ with $v \neq 0$. If $\gamma(A) = g$, then $A\overline{A} = N(A)[g : 0]$ by Theorem 3.6.3. But we also have

$$A\overline{A} = \langle v\overline{v} \rangle = \langle N(v) \rangle = \langle N(A) \rangle = N(A)[1 : 0],$$

since we saw in Theorem 3.2.2 that $N(A) = |N(v))|$. With $N(A) \neq 0$, it follows that $[g : 0] = [1 : 0]$, and so $g = 1$. □

**Example.** We saw that $A = [2 : 0]$ is an ideal of $D_{-12}$ with $\gamma(A) = 2$. Note that since $\varepsilon_{-12} = 2$, then $\overline{A} = [2 : -2] = [2 : 0] = A$. Theorem 3.6.3 shows that $A\overline{A} = N(A)[2 : 0] = 2[2 : 0]$, that is, $A^2 = 2A$. This confirms a previous example assuming the formula in Theorem 3.6.1. Corollary 3.6.4 shows that $A$ cannot be a principal ideal of $D_{-12}$. But in $D_{-3}$, $A = 2[1 : 0] = \langle 2 \rangle$. (This

illustrates that the property of $A$ being principal in $D$ depends not only on the ideal $A$ but on the domain $D$ to which it belongs.) ◊

The following lemma and theorem help us extend Theorem 3.6.3 to a general multiplication formula.

**Lemma 3.6.5.** *Let $D$ be the quadratic domain with discriminant $\Delta = \Delta(d, \gamma)$. Let $g_1$ and $g_2$ be positive divisors of $\gamma$. Then $A = [g_1 : 0]$ and $B = [g_2 : 0]$ are ideals of $D$, and $AB = g[m : 0]$, where $g = \gcd(g_1, g_2)$ and $m = \operatorname{lcm}(g_1, g_2)$.*

*Proof.* Let $\phi(x) = x^2 + \varepsilon x + \frac{\varepsilon^2 - \Delta}{4}$, the principal polynomial of discriminant $\Delta$, and note that $\gamma$ divides $\varepsilon = \varepsilon_\Delta$ by the definition in (2.2.2). Here $\{g_1, z\}$ and $\{g_2, z\}$ are $\mathbb{Z}$-bases for $A = [g_1 : 0]$ and $B = [g_2 : 0]$, respectively, so every element in $AB$ is a $\mathbb{Z}$-combination of $\{g_1g_2, g_1z, g_2z, z^2\}$, where $z^2 = -\frac{\varepsilon^2 - \Delta}{4} + \varepsilon z$. Since $g_1$ and $g_2$ are divisors of $\gamma$, which divides $\varepsilon$ as noted, we find that $g = \gcd(g_1, g_2)$ is the smallest positive integer coefficient of $z$ in any such combination. So $AB = gC$ for some ideal $C$ of $D$. Furthermore, since $g_1g_2$ divides $\gamma^2$, which divides $\frac{\varepsilon^2 - \Delta}{4}$, the smallest positive rational integer in $AB$ is $g_1g_2 = g \cdot \operatorname{lcm}(g_1, g_2)$. Finally, if $g = g_1s + g_2t$ for some integers $s$ and $t$, then $s(g_1z) + t(g_2z) = gz = g(0 + z)$ is in $AB$. Therefore $C$ can be written as $[m : 0]$. □

**Theorem 3.6.6.** *Let $D$ be the quadratic domain with discriminant $\Delta$, and let $A$ and $B$ be ideals of $D$. Then*

$$N(AB) = N(A) \cdot N(B) \cdot \gcd(\gamma(A), \gamma(B)) \quad \textit{and} \quad \gamma(AB) = \operatorname{lcm}(\gamma(A), \gamma(B)).$$

*Proof.* Let $g_1 = \gamma(A)$, $g_2 = \gamma(B)$, with $g = \gcd(g_1, g_2)$ and $m = \operatorname{lcm}(g_1, g_2)$. We have that

$$A\overline{A} \cdot B\overline{B} = N(A)[g_1 : 0] \cdot N(B)[g_2 : 0] = (N(A) \cdot N(B) \cdot g)[m : 0]$$

by Theorem 3.6.3 and Lemma 3.6.5, while

$$AB \cdot \overline{AB} = N(AB)[\gamma(AB) : 0]$$

by Theorem 3.6.3. But these two are equal by properties of conjugate ideals. We conclude that $N(AB) = N(A) \cdot N(B) \cdot g$ and $\gamma(AB) = m$. □

We are now ready to prove our main result.

*Proof of Theorem* 3.6.1. We are given that $\{a, k + z\}$ and $\{b, \ell + z\}$ are $\mathbb{Z}$-bases for $A$ and $B$, respectively, so each element of $AB$ can be expressed as a $\mathbb{Z}$-combination of

$$ab, \quad a\ell + az, \quad bk + bz, \quad \text{and} \quad \left(k\ell - \frac{\varepsilon^2 - \Delta}{4}\right) + (k + \ell + \varepsilon)z.$$

We can rewrite the final expression as $(k\ell - \phi(0)) + tz$, where $t = k + \ell + \phi'(0)$. Thus we see that the smallest positive integer coefficient of $z$ in an element of $AB$ is $g = \gcd(a, b, t)$, and so $AB = gC$, where $C = [c : m]$ for some integers $c$ and $m$. We find that

$$g^2 c = N(gC) = N(AB) = N(A) \cdot N(B) \cdot \gamma = ab\gamma$$

by Theorem 3.6.6. Since $\frac{a}{g}\ell + \frac{a}{g}z$, $\frac{b}{g}k + \frac{b}{g}z$, and $\frac{1}{g}(k\ell - \phi(0)) + \frac{t}{g}z$ are elements of $C = [c : m]$, hence are $\mathbb{Z}$-combinations of $c$ and $m + z$, then $m$ must satisfy congruences (3.6.1), (3.6.2), and (3.6.3). As noted previously, the solution of this system of congruences is unique modulo $c$. □

## Ideals of Quadratic Domains—Review

If $D = D_\Delta$ is a quadratic domain, then a nonempty subset $A$ is called an *ideal* of $D$ if $A$ is closed under subtraction and if $vx$ is in $A$ for every $v$ in $A$ and $x$ in $D$. In this chapter, we classified all ideals in a typical quadratic domain, and showed that they are essentially the same as what we previously defined as *ideal numbers* of discriminant $\Delta$. Thus we can describe precisely the properties of multiplication and irreducible factorization with these objects that we assumed in Chapter 2. We summarize our main results as follows.

(1) If $\phi(x)$ is the principal polynomial of discriminant $\Delta$, and $a$ and $k$ are integers, then the set $A = \{ma + n(k + z) \mid m, n \in \mathbb{Z}\}$, where $z = z_\Delta$, is an ideal of $D_\Delta$ if and only if $a$ divides $\phi(k)$. We denote this ideal as $A = [a : k]$. If $g$ is a positive integer, then $B = gA$ is also an ideal, written as $B = g[a : k]$.

(2) Every nontrivial ideal $B$ of a quadratic domain $D$ can be written as $B = g[a : k]$ for some integers $a$, $k$, and $g$. In practice, we can determine this *ideal number* expression for $B$ by identifying an element $gk + gz$ in $B$ with $g > 0$ as small as possible, and the smallest positive rational integer $ga$ in $B$.

(3) If $v$ is an element of a quadratic domain $D$, then $\langle v \rangle = \{vx \mid x \in D\}$ is an ideal of $D$, called the *principal ideal* of $D$ generated by $v$. If $v$ has ideal form $g[a : k]$ (as defined in Chapter 2), then $\langle v \rangle$ can also be written as $g[a : k]$.

(4) The ideal $\langle v, w \rangle = \{vx + wy \mid x, y \in D\}$ of combinations of a pair of elements can also be expressed as an ideal number, using an ideal number formula for a sum of ideals (Theorem 3.2.3) and noting that $\langle v, w \rangle = \langle v \rangle + \langle w \rangle$.

(5) *Prime ideals*, which play the part of irreducible ideal numbers, are defined in terms of set containment (as what are also called *maximal* ideals). These take the form $[p : k]$, where $p$ is a rational prime and $k$ satisfies $\phi(x) \equiv 0 \pmod{p}$, or $\langle p \rangle = p[1 : 0]$ when $\phi(x) \equiv 0 \pmod{p}$ has no solutions.

(6) There is an operation of multiplication on ideals of a quadratic domain $D$, and a general formula for multiplication of ideals written as ideal numbers (Theorem 3.6.1). Specific calculations of products of ideals typically involve the same methods used in solving a quadratic congruence modulo a composite integer.

(7) In some quadratic domains, there are ideals that cannot be written in any way as a product of prime ideals. In particular, this can occur for an ideal $A$ of $D_\Delta$, where $\Delta = \Delta(d, \gamma)$, if $N(A)$ and $\gamma$ have a prime common divisor. We define an ideal to be *complete* if $\gcd(N(A), \gamma) = 1$. Every complete ideal can be written as a product of prime ideals, uniquely aside from order. In particular, this is true for every nontrivial ideal of a *complete* quadratic domain, that is, $D_\Delta$, where $\Delta = \Delta(d, 1)$, the set of all quadratic integers in the field $\mathbb{Q}(\sqrt{d})$.

(8) The prime ideal factorization of a complete ideal $A = g[a : k]$ is straightforward in practice, essentially the same as factoring $g$ and $a$ as rational integers. Examples of distinct irreducible factorizations in a quadratic domain can be explained by breaking the corresponding principal ideals into prime ideal factors.

The definition of ideals supersedes our previous notion of ideal numbers of a particular discriminant in a precise and concrete way. Nonetheless, our ideal number notation allows us to view ideals in numerical form, a computational approach that we will continue to develop and exploit in the following chapters.

# Part Two: Quadratic Forms and Ideals

**Overview.** In Part One, questions about representations of integers by certain quadratic forms motivated the definition of quadratic domains and their ideals. Our goal in the next two chapters is to continue this development by connecting quadratic forms and ideals more closely and completely. Specific questions concerning representations of integers by quadratic forms continue to be our main focus.

In Chapter 4, we consider quadratic forms as objects of study in their own right with the definition of the set $\mathcal{Q}_\Delta$ of quadratic forms of a particular discriminant. We define a relation of *equivalence* on $\mathcal{Q}_\Delta$, and we establish that equivalent forms represent precisely the same collection of integers. We determine a criterion for proper representation of an integer by some form of a particular discriminant, and derive a formula for the number of representations of an integer by a given form, with an equivalence relation on ordered pairs introduced to count these representations correctly. A relation of *genus equivalence* on forms further characterizes these representations.

Chapter 4 also introduces another useful departure from standard notation with the definition of a new representation for quadratic forms. We will see that every quadratic form of a fixed discriminant can be written as $(a \ : \ k)$, where $a$ and $k$ are integers that satisfy precisely the same criterion that makes $A = [a \ : \ k]$ into an ideal of the quadratic domain with the same discriminant. In Chapter 4, we find that many aspects of quadratic forms can be described using this *ideal notation*. In particular, we develop a reduction process by which we can determine a specific representation of an integer by a given quadratic form.

In Chapter 5, we exploit the similar notation introduced for quadratic forms and for ideals in several ways. We show that the relation of equivalence on quadratic forms provides us with a similar equivalence relation on ideals of a quadratic domain, and we develop a precise correspondence between classes of ideals and classes of quadratic forms under these relations. In the reverse direction, we

use the operation of ideal multiplication to describe a similar operation of composition on quadratic form classes. Using these operations, we define similar group structures on classes of ideals and on classes of quadratic forms.

The concepts introduced in Chapter 5 allow us to view classes of ideals of negative discriminant and classes of positive definite quadratic forms as identical. The same is true for classes of ideals of positive discriminant and classes of indefinite quadratic forms, aside from a slight complication that we will note in this case. We use this viewpoint extensively in the remainder of the text.

**Requirements for Part Two.** We will assume that the reader is familiar with the definition and properties of matrix multiplication, which we use to define equivalence relations on the set of quadratic forms of a particular discriminant. We will find in particular that certain properties of these relations require the concept of groups, especially groups of $2 \times 2$ matrices under multiplication. We occasionally use group terminology, such as subgroups, cosets of a subgroup in a larger group, conjugates of a subgroup, and the action of a group on a set, within this context. Some properties of groups are introduced in exercises, particularly in §4.2. More details appear in Appendix C as needed.

# 4

# Quadratic Forms

We began our study of quadratic number theory with questions about sums of two squares. We saw that we could use the uniqueness of irreducible factorization in the Gaussian integers to describe the integers represented by $x^2 + y^2$. In §2.5, we found that we could similarly describe representations of integers by the principal form of discriminant $\Delta$ in cases where $D_\Delta$ is a unique factorization domain. While we found that unique factorization into irreducible elements is the exception in quadratic domains, we demonstrated in Chapter 3 that unique factorization into prime ideals occurs in every complete quadratic domain, and with every complete ideal in an arbitrary quadratic domain.

Our goal now is to apply prime ideal factorization to representations of integers by arbitrary binary quadratic forms. In this chapter, we compile definitions and terminology for these quadratic forms as objects in their own right. In particular, we introduce in §4.1 a notation for quadratic forms that is very similar to our numerical notation for ideals. Using an equivalence relation on quadratic forms defined in §4.2, we establish a criterion for representation of an integer by some quadratic form of a particular discriminant, and a formula for the number of such representations in §4.3. In Chapter 5, we will then see that our notation allows us to apply, in several ways, a close connection between quadratic forms and ideals.

## 4.1 Classification of Quadratic Forms

The following definition generalizes examples of quadratic expressions previously considered.

**Definition.** A *binary quadratic form*, which we will call simply a *quadratic form*, is a homogeneous degree two polynomial in two variables,

$$f(x,y) = ax^2 + bxy + cy^2, \tag{4.1.1}$$

with integer *coefficients* $a$, $b$, and $c$. The *discriminant* of $f$ is

$$\Delta = \Delta(f) = b^2 - 4ac,$$

and we denote the set of all quadratic forms of discriminant $\Delta$ as $\mathcal{Q}_\Delta$. We say that $f$ *represents* the integer $m$ if $f(q,r) = m$ for some integers $q$ and $r$, and that $f$ *properly represents* $m$ if $f(q,r) = m$ with $\gcd(q,r) = 1$.

If $f(q,r) = aq^2 + bqr + cr^2 = m$, then direct calculation shows that

$$4am = (2aq + br)^2 - \Delta r^2 \quad \text{and} \quad 4cm = (2cr + bq)^2 - \Delta q^2. \tag{4.1.2}$$

If $\Delta$ is a square, we can factor the right-hand side of each equation in (4.1.2) and solve for $q$ and $r$ by elementary means. We will assume instead that $\Delta$ is not a square. (Then $\Delta$ is a *discriminant* as defined in §2.2.) In that case, $f(q,r) = 0$ if and only if $q = 0 = r$. In particular, $f(1,0) = a$ and $f(0,1) = c$ cannot be zero. If $\Delta$ is positive, then (4.1.2) shows that $f$ can represent either positive or negative integers. If $\Delta$ is negative, then all values of $f(q,r)$ have the same sign as $a$ when $(q,r) \neq (0,0)$.

**Definition.** Let $f(x,y) = ax^2+bxy+cy^2$ be a quadratic form, with discriminant $\Delta = b^2 - 4ac$.

(1) If $\Delta$ is positive, we say that $f$ is *indefinite*.

(2) If $\Delta$ is negative and $a$ is positive, we say that $f$ is *positive definite*.

(3) If $\Delta$ is negative and $a$ is negative, we say that $f$ is *negative definite*.

**Definition.** If $f(x,y) = ax^2+bxy+cy^2$ is a quadratic form, we define the *index* of $f$ to be $\gamma(f) = \gcd(a,b,c)$. We say that $f$ is *primitive* if $\gamma(f) = 1$.

If $\gamma(f) = \gamma$, with $a = \gamma a_1$, $b = \gamma b_1$, and $c = \gamma c_1$, then

$$\Delta(f) = \gamma^2(b_1^2 - 4a_1c_1) = \gamma^2\Delta_1$$

with $\Delta_1 \equiv 0$ or $1 \pmod 4$. It follows that the index of a quadratic form $f$ of discriminant $\Delta$ divides the index of $\Delta$, as defined in (2.2.1). That is, if $\Delta = \Delta(d,\gamma)$, then $\gamma(f)$ divides $\gamma$ for each $f$ in $\mathcal{Q}_\Delta$. In particular, if $\Delta$ is a primitive discriminant, then all quadratic forms in $\mathcal{Q}_\Delta$ are primitive.

**The Matrix of a Quadratic Form.** If $f$ is a quadratic form, we can associate a particular $2\times 2$ matrix to $f$, and calculate $f(q,r)$ for integers $q$ and $r$ via matrix multiplication. This will be useful for several definitions in this chapter.

**Definition.** If $f(x,y) = ax^2 + bxy + cy^2$ is a quadratic form, then the *matrix* of $f$ is

$$M_f = \begin{bmatrix} 2a & b \\ b & 2c \end{bmatrix}. \tag{4.1.3}$$

The matrix of $f$ is *symmetric*, that is, $M_f^T = M_f$. (In general, $A^T$ denotes the *transpose* of a matrix $A$, that is, the matrix obtained by interchanging the rows and columns of $A$.) The discriminant of $f$ is the negative of the determinant of $M_f$. If $\mathbf{x}$ is a column matrix with entries $q$ and $r$, then

$$\mathbf{x}^T M_f \mathbf{x} = \begin{bmatrix} q & r \end{bmatrix} \cdot \begin{bmatrix} 2a & b \\ b & 2c \end{bmatrix} \cdot \begin{bmatrix} q \\ r \end{bmatrix} = [2f(q,r)]. \tag{4.1.4}$$

We may write $f(q,r) = f(\mathbf{x}) = \frac{1}{2}\mathbf{x}^T M_f \mathbf{x}$ in this case, identifying $\mathbf{x}$ with the ordered pair $(q,r)$, and $f(\mathbf{x}) = m$ with the $1\times 1$ matrix having $m$ as its single entry.

**Definition.** If $A$ is a $2\times 2$ matrix, define the *conjugate* of $A$, written as $\overline{A}$, to be the matrix obtained by changing the sign of the off-diagonal entries of $A$. That is, if $A = \begin{bmatrix} q & s \\ r & t \end{bmatrix}$, then $\overline{A} = \begin{bmatrix} q & -s \\ -r & t \end{bmatrix}$.

**Exercise 4.1.1.** Let $A$ and $B$ be $2\times 2$ matrices.

(a) Show that the determinant of $A$ equals the determinant of $\overline{A}$.

(b) Show that $\overline{A} + \overline{B} = \overline{A+B}$.

(c) Show that $\overline{A}\cdot\overline{B} = \overline{A\cdot B}$.

**Definition.** Let $f(x,y) = ax^2 + bxy + cy^2$ be a quadratic form of discriminant $\Delta$. Then the *conjugate* of $f$ is $\overline{f}(x,y) = ax^2 - bxy + cy^2$, the *negative* of $f$ is $-f(x,y) = -ax^2 - bxy - cy^2$, and the *negative conjugate* of $f$ is $-\overline{f}(x,y) = -ax^2 + bxy - cy^2$.

If $f$ is an element of $\mathcal{Q}_\Delta$, then $\overline{f}$, $-f$, and $-\overline{f}$ are likewise elements of $\mathcal{Q}_\Delta$. We have the following relation between the matrix of $f$ and the matrices of these associated forms:

$$M_{(\overline{f})} = \overline{M_f}, \qquad M_{(-f)} = -M_f, \qquad M_{(-\overline{f})} = -\overline{M_f}.$$

**Exercise 4.1.2.** Let $f(x,y) = ax^2 + bxy + cy^2$ and let

$$\overline{f}(x,y) = ax^2 - bxy + cy^2 \quad \text{and} \quad -f(x,y) = -ax^2 - bxy - cy^2$$

be its conjugate and negative, respectively.

(a) Show that if $f(q,r) = m$, then $\overline{f}(q,-r) = m$.

(b) Show that $f$ represents an integer $m$ if and only if $\overline{f}$ represents $m$.

(c) Show that $f$ represents $m$ if and only if $-f$ represents $-m$.

**Ideal Notation for Quadratic Forms.** The following observation allows us to classify all quadratic forms of discriminant $\Delta$, using a notation similar to that of ideals of the quadratic domain $D_\Delta$.

**Proposition 4.1.1.** *Let $\phi(x)$ be the principal polynomial and let $\varepsilon$ be the basis index of some discriminant $\Delta$. If $f(x,y) = ax^2 + bxy + cy^2$ is a quadratic form of discriminant $\Delta$, then $k = \frac{b-\varepsilon}{2}$ is an integer and $\phi(k) = ac$. Conversely, if $a$ and $k$ are integers for which $a$ divides $\phi(k)$, and we let $b = \phi'(k)$ and $c = \frac{1}{a}\phi(k)$, then $f(x,y) = ax^2 + bxy + cy^2$ is a quadratic form of discriminant $\Delta$.*

*Proof.* If $f(x,y) = ax^2 + bxy + cy^2$ is a quadratic form with $\Delta = b^2 - 4ac$, then $b$ has the same parity as $\Delta$, as does $\varepsilon$, as we saw in §2.2. So $k = \frac{b-\varepsilon}{2}$ is an integer, and we find that

$$\begin{aligned}\phi(k) &= \left(\frac{b-\varepsilon}{2}\right)^2 + \varepsilon\left(\frac{b-\varepsilon}{2}\right) + \frac{\varepsilon^2-\Delta}{4} \\ &= \frac{b^2 - 2b\varepsilon + \varepsilon^2 + 2b\varepsilon - 2\varepsilon^2 + \varepsilon^2 - \Delta}{4} = \frac{b^2-\Delta}{4} = ac.\end{aligned}$$

Conversely, let $a$ and $k$ be integers for which $a$ divides $\phi(k)$, say with $\phi(k) = ac$, and let $b = \phi'(k) = 2k + \varepsilon$. Then

$$b^2 - 4ac = \phi'(k)^2 - 4\phi(k) = 4k^2 + 4\varepsilon k + \varepsilon^2 - 4\left(k^2 + \varepsilon k + \frac{\varepsilon^2-\Delta}{4}\right) = \Delta,$$

so that $f(x,y) = ax^2 + bxy + cy^2$ has discriminant $\Delta$. □

Thus for a fixed discriminant $\Delta$, binary quadratic forms $f$ in $\mathcal{Q}_\Delta$ are in one-to-one correspondence with pairs of integers $a$ and $k$ for which $a$ divides $\phi_\Delta(k)$. With this in mind, we introduce the following notation.

**Definition.** If $f(x,y) = ax^2 + bxy + cy^2$ is a quadratic form of discriminant $\Delta$, and $k = \frac{b-\varepsilon}{2}$, where $\varepsilon = \varepsilon_\Delta$, then we also write $f = (a : k)_\Delta$, or $f = (a : k)$ if $\Delta$ is apparent from the context. Conversely, if $\phi(x)$ is the principal polynomial

of some discriminant $\Delta$, and $a$ and $k$ are integers for which $a$ divides $\phi(k)$, we write $f = (a : k)$ to denote the quadratic form $f(x, y) = ax^2 + bxy + cy^2$, where $b = \phi'(k)$ and $c = \frac{1}{a}\phi(k)$. We refer to $f(x, y) = ax^2 + bxy + cy^2$ as *standard notation* for a quadratic form $f$, and to $(a : k)$ as *ideal notation* for $f$, because of its similarity to our way of writing ideals of a quadratic domain.

**Example.** Since $a = 1$ divides $\phi(0) = \frac{\varepsilon^2 - \Delta}{4}$, we have that

$$(1 : 0)_\Delta = x^2 + \varepsilon xy + \frac{\varepsilon^2 - \Delta}{4} y^2.$$

This is same as the principal form, $\phi(x, y)$, of discriminant $\Delta$ as defined in equation (2.2.6). That is, $\phi = (1 : 0)$ in every set $\mathcal{Q}_\Delta$. ◊

**Example.** Let $\Delta = 13$, so that $\phi(x) = x^2 + x - 3$. For a particular integer $a$, we can determine all elements $(a : k)$ in $\mathcal{Q}_{13}$ by solving the congruence $x^2 + x - 3 \equiv 0 \pmod{a}$. For example, we find that $x^2 + x - 3 \equiv 0 \pmod{3}$ has solutions 0 and 2. So $\mathcal{Q}_{13}$ contains $(3 : k)$ and $(-3 : k)$ if and only if $k \equiv 0$ or $2 \pmod{3}$. Here $b = 2k + 1$ and $ac = k^2 + k - 3$, so that

$$(3 : 0) = 3x^2 + xy - y^2, \qquad (-3 : 2) = -3x^2 + 5xy - y^2,$$

and so forth. On the other hand, $x^2 + x - 3 \equiv 0 \pmod{5}$ has no solutions, so that $\mathcal{Q}_{13}$ contains no elements of the form $(5 : k)$ or $(-5 : k)$. ◊

**Exercise 4.1.3.** For each of the following quadratic forms $f(x, y)$, calculate the discriminant of $f$ and write $f$ using ideal notation.

(a) $f(x, y) = 5x^2 - 3xy + 7y^2$.

(b) $f(x, y) = 3x^2 - 6xy + 2y^2$.

(c) $f(x, y) = 6x^2 + 10xy + y^2$.

**Exercise 4.1.4.** Let $\Delta = -31$. For each of the following values of $a$, find (a pattern for) all values of $k$ for which $(a : k)$ is an element of $\mathcal{Q}_\Delta$.

(a) $a = 5$.

(b) $a = 7$.

(c) $a = 35$.

**Exercise 4.1.5.** Let $f(x, y) = ax^2 + bxy + cy^2$ be a quadratic form of discriminant $\Delta$, and suppose that $f = (a : k)$ in ideal notation.

(a) Show that $\overline{f} = (a : -k - \varepsilon)$.

(b) Show that $-f = (-a : -k - \varepsilon)$.

(c) Show that $-\overline{f} = (-a : k)$.

## 4.2 Equivalence of Quadratic Forms

We saw in §4.1 that if $f$ is a quadratic form, then we can associate a particular $2 \times 2$ matrix to $f$, and calculate $f(q, r)$ for integers $q$ and $r$ via matrix multiplication. In this section, we demonstrate that this viewpoint allows us to define several equivalence relations on the set of all quadratic forms of some fixed discriminant, an important step in classifying these forms.

**Definition.** Let

$$\Gamma = \left\{ U = \begin{bmatrix} q & s \\ r & t \end{bmatrix} \mid q, r, s, t \in \mathbb{Z} \text{ and } \det U = qt - rs = 1 \right\}.$$

We refer to an element of $\Gamma$ as a *unimodular* matrix. If $M_f$ is the matrix of a quadratic form as in (4.1.3), and $U$ is unimodular as above, then

$$\begin{aligned} U^T M_f U &= \begin{bmatrix} q & r \\ s & t \end{bmatrix} \cdot \begin{bmatrix} 2a & b \\ b & 2c \end{bmatrix} \cdot \begin{bmatrix} q & s \\ r & t \end{bmatrix} \\ &= \begin{bmatrix} 2(aq^2 + bqr + cr^2) & 2aqs + b(qt + rs) + 2crt \\ 2aqs + b(qt + rs) + 2crt & 2(as^2 + bst + ct^2) \end{bmatrix} \end{aligned}$$

is the matrix of a quadratic form $g$ given by

$$(aq^2 + bqr + cr^2)x^2 + (2aqs + b(qt + rs) + 2crt)xy + (as^2 + bst + ct^2)y^2. \quad (4.2.1)$$

We write $g = f \circ U$ to mean that $g$ is obtained from $f$ via $U$ in this way.

**Exercise 4.2.1.** Show that the set $\Gamma$ of all unimodular matrices is a group under matrix multiplication. (Assume that the set of all nonsingular $2 \times 2$ matrices with real number entries is a group under matrix multiplication. Thus it suffices to show that $\Gamma$ is closed under multiplication, and that the inverse of an element of $\Gamma$ is also in $\Gamma$.)

**Exercise 4.2.2.** Let $f$ be a quadratic form. If $U$ is a unimodular matrix and $V = -U$, show that $f \circ U = f \circ V$.

The quadratic forms $f$ and $g = f \circ U$ have the same discriminant, since $\det(U^T M_f U) = \det(U^T) \cdot \det(M_f) \cdot \det(U) = \det(M_f)$. Thus we can view the mapping that takes $f$ to $f \circ U$ as a function on the set $\mathcal{Q}_\Delta$ for a fixed discriminant $\Delta$. More precisely, the following exercise indicates that we have a *group action* by $\Gamma$ on the set $\mathcal{Q}_\Delta$.

**Exercise 4.2.3.** Let $I$ be the $2 \times 2$ identity matrix, and let $U$ and $V$ be unimodular matrices. Let $f$, $g$, and $h$ be quadratic forms in $\mathcal{Q}_\Delta$ for some discriminant $\Delta$.
(a) Show that $f \circ I = f$.

(b) Show that if $g = f \circ U$, then $f = g \circ U^{-1}$.

(c) Show that if $g = f \circ U$ and $h = g \circ V$, then $h = f \circ (UV)$.

**Definition.** Let $H$ be a subgroup of the group $\Gamma$ of $2 \times 2$ unimodular matrices. Then we define a relation $\sim_H$ on the set $\mathcal{Q}_\Delta$ of quadratic forms of determinant $\Delta$ by saying that $f \sim_H g$ if and only if $g = f \circ U$ for some $U$ in $H$. If $H$ is the entire group $\Gamma$, we write $\sim_H$ simply as $\sim$. We say that $f$ is *equivalent* to $g$, and that $f$ and $g$ are in the same *class*, if $f \sim g$.

**Exercise 4.2.4.** If $H$ is a subgroup of $\Gamma$, show that $\sim_H$ is an equivalence relation on $\mathcal{Q}_\Delta$. Show that if $f \sim_H g$ for some subgroup $H$ of $\Gamma$, then $f \sim g$ is also true.

**Exercise 4.2.5.** Let $f$ and $g$ be quadratic forms of discriminant $\Delta$, with the negatives of $f$ and $g$ defined as in §4.1. Show that if $f$ is equivalent to $g$, then $-f$ is equivalent to $-g$. Specifically, show that if $g = f \circ U$, then $-g = -f \circ U$.

**Exercise 4.2.6.** Let $f$ and $g$ be quadratic forms of discriminant $\Delta$, with the conjugates of $f$ and $g$ defined as in §4.1. Show that if $f$ is equivalent to $g$, then $\overline{f}$ is equivalent to $\overline{g}$. Specifically, show that if $g = f \circ U$, then $\overline{g} = \overline{f} \circ \overline{U}$, where $\overline{U}$ is the conjugate of $U$ as defined in §4.1.

**Equivalence of Quadratic Forms in Ideal Notation.** We can apply $U$ to a form written in ideal notation, according to the following proposition.

**Proposition 4.2.1.** *Let $\phi(x)$ be the principal polynomial of discriminant $\Delta$, and let $f = (a : k)$ be in $\mathcal{Q}_\Delta$, with $\phi(k) = ac$ and $\phi'(k) = b$. Let $U = \begin{bmatrix} q & s \\ r & t \end{bmatrix}$ be a unimodular matrix. Then $g = f \circ U = (m : \ell)$, where*

$$m = f(q,r) = aq^2 + bqr + cr^2 \quad \text{and} \quad \ell = aqs + brs + crt + k. \tag{4.2.2}$$

*Proof.* Since $qt - rs = 1$, we see that

$$\begin{aligned} \frac{(2aq + b(qt + rs) + 2crt) - \varepsilon}{2} &= \frac{2(aqs + brs + crt) + b - \varepsilon}{2} \\ &= aqs + brs + crt + k. \end{aligned}$$

The expression for $g$ as $(m : \ell)$ then follows directly from equation (4.2.1). □

If $f = (a : k)$ is equivalent to $g = (m : \ell)$, then equation (4.2.2) shows that $f$ properly represents $m$. (Note that $q$ and $r$ cannot have a prime common divisor since $qt - rs = 1$.)

**Exercise 4.2.7.** Verify that $f = (13 : 7)$ is a quadratic form of discriminant $\Delta = -35$. For each of the following unimodular matrices $U$, calculate the form $f \circ U$ in ideal notation.

(a) $U = \begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix}$.

(b) $U = \begin{bmatrix} 7 & 3 \\ -5 & -2 \end{bmatrix}$.

(c) $U = \begin{bmatrix} 4 & 9 \\ 3 & 7 \end{bmatrix}$.

In practice, we will often be able to restrict our attention to two particular types of unimodular matrices, specified in the following two propositions.

**Proposition 4.2.2.** *Let $(a : k)$ be a quadratic form of discriminant $\Delta$, so that $\phi(k) = ac$ for some integer $c$, where $\phi(x) = x^2 + \varepsilon x + \frac{\varepsilon^2 - \Delta}{4}$ is the principal polynomial of discriminant $\Delta$. Then*

$$(a : k) \sim (c : -k - \varepsilon). \tag{4.2.3}$$

*Proof.* Let $b = \phi'(k)$ so that $f(x, y) = ax^2 + bxy + cy^2$ in standard form. We have that

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 2a & b \\ b & 2c \end{bmatrix} \cdot \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 2c & -b \\ -b & 2a \end{bmatrix},$$

so that $f \sim g$, where $g(x, y) = cx^2 - bxy + ay^2$. We can write $g = (c : \ell)$, where $\ell = \frac{-b-\varepsilon}{2} = -\frac{b-\varepsilon}{2} - \varepsilon = -k - \varepsilon$. □

**Definition.** We refer to $g(x, y) = cx^2 - bxy + ay^2$ as the *involution* of $f(x, y) = ax^2 + bxy + cy^2$. Notice that the involution of $g(x, y)$ returns us to $f(x, y)$. When using ideal notation, we will write $(a : k) \leftrightarrow (c : -k - \varepsilon)$ for this relation.

**Exercise 4.2.8.** Show that $H = \left\{ \begin{bmatrix} 1 & u \\ 0 & 1 \end{bmatrix} \mid u \in \mathbb{Z} \right\}$ is a subgroup of the group of unimodular matrices.

**Definition.** Let $H$ be defined as in Exercise 4.2.8, so that $\sim_H$ is an equivalence relation on $\mathcal{Q}_\Delta$. We write $\sim_H$ as $\simeq$ in this case, and say that $f$ is *norm equivalent* to $g$, or that $f$ and $g$ are in the same *norm class*, if $f \simeq g$.

**Proposition 4.2.3.** *If $(a : k)$ is a quadratic form of discriminant $\Delta$, then $(a : k)$ is norm equivalent to $(m : \ell)$ if and only if $m = a$ and $\ell \equiv k \pmod{a}$.*

*Proof.* Let $\phi(k) = ac$ and $\phi'(k) = b$ so that $f(x, y) = ax^2 + bxy + cy^2$. If $u$ is an integer, then

$$\begin{bmatrix} 1 & 0 \\ u & 1 \end{bmatrix} \cdot \begin{bmatrix} 2a & b \\ b & 2c \end{bmatrix} \cdot \begin{bmatrix} 1 & u \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 2a & b + 2au \\ b + 2au & 2(c + bu + au^2) \end{bmatrix},$$

so that $f \simeq g$, where $g(x,y) = ax^2 + (b+2au)xy + (c+bu+au^2)y^2$. In ideal notation, $g = (m : \ell)$ if and only if $m = a$ and

$$\ell = \frac{b+2au-\varepsilon}{2} = \frac{b-\varepsilon}{2} + au = k + au,$$

so that $\ell \equiv k \pmod{a}$. □

**Definition.** We refer to $g = (a : k+au)$ as the *translation* of $f = (a : k)$ by $u$. We have that $(a : k) \simeq (a : k+au)$ for all integers $u$. Thus it is also true that $(a : k) \sim (a : k+au)$ for all $u$. We will also write $(a : k) \to_u (a : k+au)$ for this translation.

The following example illustrates how we might use involutions and translations to simplify the class representative of a quadratic form.

**Example.** Let $\Delta = -23$ so that $\phi(x) = x^2 + x + 6$. We find that $\phi(18) = 348 = 87 \cdot 4$, with $\phi'(18) = 37$, so that $f = (87 : 18) = 87x^2 + 37xy + 4y^2$ is a quadratic form of discriminant $\Delta$. Using a sequence of involutions and translations from Propositions 4.2.2 and 4.2.3, then

$$(87 : 18) \leftrightarrow (4 : -19) \to_5 (4 : 1) \leftrightarrow (2 : -2) \to_1 (2 : 0),$$

so that $f$ is equivalent to the quadratic form $g = (2 : 0) = 2x^2 + xy + 3y^2$. Specifically, we find that $g = f \circ U$ with

$$U = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 5 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} -1 & -1 \\ 5 & 4 \end{bmatrix},$$

as one can verify. Here $U$ is the product of the unimodular matrices for the involutions and translations that convert $f$ to $g$. ◊

**Exercise 4.2.9.** Let $\Delta = -51$. Verify that $f = (57 : 16)$ is an element of $\mathcal{Q}_\Delta$. Use a sequence of involutions and translations to show that $f$ is equivalent to $g = (3 : 1)$, and find a matrix $U$ for which $g = f \circ U$.

The reader might recognize a similarity between the procedure in this example and the *reduction* algorithms that we developed for ideal forms of Gaussian integers (Theorem 1.5.3), and then for ideal numbers in an arbitrary quadratic domain (Theorem 2.4.3). We will say more about this process in Chapters 6 and 10, where we will also use the following proposition.

**Proposition 4.2.4.** *Let $\phi(x)$ be the principal polynomial of discriminant $\Delta$, and let $f = (a : k)$ in $\mathcal{Q}_\Delta$, with $ac = \phi(k)$ and $b = \phi'(k)$. If $U$ is a unimodular matrix with $q$ and $r$ the entries of its first column, then $f \circ U \simeq (m : \ell)$, where $m = aq^2 + bqr + cr^2$ and $\ell$ satisfies the congruences*

$$q\ell \equiv cr + kq \pmod{m} \quad \text{and} \quad r\ell \equiv (k-b)r - aq \pmod{m}.$$

Here $q$ and $r$ must be relatively prime, and so Exercise 0.1.11 shows that this pair of congruences has a unique solution modulo $m$. The main claim of the proposition is that the first column of $U$ is sufficient to determine $f \circ U$ up to norm equivalence.

*Proof.* Let $s$ and $t$ be integers so that $qt-rs = 1$. All integer solutions of $qx-ry = 1$ are given by $(x, y) = (t + ru, s + qu)$ for some integer $u$. (This is an application of Theorem 0.1.5.) Thus $U$ has the form

$$U = \begin{bmatrix} q & s+qu \\ r & t+ru \end{bmatrix} = \begin{bmatrix} q & s \\ r & t \end{bmatrix} \cdot \begin{bmatrix} 1 & u \\ 0 & 1 \end{bmatrix},$$

and $f \circ U$ is unique up to norm equivalence.

Now $\ell = aqs + brs + crt + k$ by equation (4.2.2). We find that

$$\begin{aligned} q\ell &= aq^2s + bqrs + cqrt + qk \\ &= (aq^2 + bqr + cr^2)s + cr(qt - rs) + qk = ms + cr + qk, \end{aligned}$$

since $m = aq^2 + bqr + cr^2$ and $qt - rs = 1$. So $q\ell \equiv cr + kq \pmod{m}$. With $rs = qt - 1$, so that $\ell = aqs + bqt + crt + (k - b)$, we find in a similar way, multiplying both sides by $r$, that $r\ell = mt+(k-b)r-aq$, so that $r\ell \equiv (k-b)r-aq \pmod{m}$. □

## 4.3 Representations of Integers by Quadratic Forms

We can now use equivalence of quadratic forms to give a formula for the number of representations of an integer by a particular quadratic form. Throughout this section, we identify an ordered pair of integers $(q, r)$ with the column matrix $\mathbf{x}$ having entries $q$ and $r$. We say that $\mathbf{x}$ is *primitive* if $\gcd(q, r) = 1$. If $f(x, y)$ is a quadratic form, we also write $f(q, r)$ as $f(\mathbf{x})$. Recall that we have $f(\mathbf{x}) = \frac{1}{2}\mathbf{x}^T M_f \mathbf{x}$, where $M_f$ is the matrix of $f$.

Our first theorem shows that equivalent forms represent, and properly represent, the same collection of integers.

**Theorem 4.3.1.** *Let $f$ and $g$ be equivalent quadratic forms, and suppose that $m$ is an integer represented by $f$. Then there is a one-to-one correspondence between ordered pairs $\mathbf{x} = (q, r)$ for which $f(\mathbf{x}) = m$ and $\mathbf{y} = (s, t)$ for which $g(\mathbf{y}) = m$. In this case,* $\gcd(q, r) = \gcd(s, t)$.

*Proof.* Let $U$ be a unimodular matrix for which $g = f \circ U$, and let $\mathbf{y} = U^{-1}\mathbf{x}$. Using properties of inverses and transposes, we find that

$$m = \tfrac{1}{2} \cdot \mathbf{x}^T M_f \mathbf{x} = \tfrac{1}{2} \cdot \mathbf{x}^T (U^{-1})^T \cdot U^T M_f U \cdot U^{-1}\mathbf{x} = \tfrac{1}{2} \cdot \mathbf{y}^T M_g \mathbf{y},$$

so that $g(\mathbf{y}) = m$. Conversely, if $g(\mathbf{y}) = m$ and $\mathbf{x} = U\mathbf{y}$, then $f(\mathbf{x}) = m$. The matrix equations show that the entries of $\mathbf{y}$ can be written as combinations of the entries of $\mathbf{x}$, and conversely, so that those entries have the same greatest common divisor. □

**Example.** Let $f(x, y) = x^2 + xy + 2y^2$. Since

$$\begin{bmatrix} 7 & 2 \\ 10 & 3 \end{bmatrix} \cdot \begin{bmatrix} 2 & 1 \\ 1 & 4 \end{bmatrix} \cdot \begin{bmatrix} 7 & 10 \\ 2 & 3 \end{bmatrix} = \begin{bmatrix} 142 & 205 \\ 205 & 296 \end{bmatrix},$$

then $f$ is equivalent to $g(x, y) = 71x^2 + 205xy + 148y^2$. Now $f(4, -9) = 142$, and so $g$ represents 142 also. In fact, since

$$\begin{bmatrix} 7 & 10 \\ 2 & 3 \end{bmatrix}^{-1} \cdot \begin{bmatrix} 4 \\ -9 \end{bmatrix} = \begin{bmatrix} 3 & -10 \\ -2 & 7 \end{bmatrix} \cdot \begin{bmatrix} 4 \\ -9 \end{bmatrix} = \begin{bmatrix} 102 \\ -71 \end{bmatrix},$$

we find that $g(102, -71) = 142$. ◊

**Exercise 4.3.1.** Let $f(x, y) = 3x^2 - 5xy + 4y^2$, a quadratic form of discriminant $\Delta = -23$, and note that $f(2, 1) = 6$. For each of the following unimodular matrices $U$, find the quadratic form $g = f \circ U$, and find a solution of $g(x, y) = 6$.

(a) $U = \begin{bmatrix} 1 & -3 \\ 0 & 1 \end{bmatrix}$.

(b) $U = \begin{bmatrix} 2 & -3 \\ -3 & 5 \end{bmatrix}$.

(c) $U = \begin{bmatrix} 7 & 9 \\ 3 & 4 \end{bmatrix}$.

**Corollary 4.3.2.** *Equivalent quadratic forms have the same index.*

*Proof.* Let $f(x, y) = ax^2 + bxy + cy^2$ with $\gamma = \gcd(a, b, c)$ the index of $f$. Then $\gamma$ divides $f(q, r)$ for every pair of rational integers $q$ and $r$. Suppose that $f \sim g$ and that $\gamma'$ is the index of $g$. Theorem 4.3.1 implies that $f(1, 0) = a$, $f(0, 1) = c$, and $f(1, 1) = a + b + c$ must be represented by $g$ also. Then $\gamma'$ is a common divisor of $a$, $c$, and $b = (a + b + c) - a - c$, and so $\gamma'$ divides $\gamma$. The same argument in reverse shows that $\gamma$ divides $\gamma'$, and then $f$ and $g$ must have the same index. □

The following theorem provides an important necessary condition for an integer $m$ to be properly represented by a particular quadratic form.

**Theorem 4.3.3.** *Let $\phi(x)$ be the principal polynomial of discriminant $\Delta$. Then an integer $m$ is properly represented by some quadratic form of discriminant $\Delta$ if and only if $\phi(x) \equiv 0 \pmod{m}$ has a solution.*

*Proof.* Suppose that $f(x,y)$ is a quadratic form of discriminant $\Delta$ and that $f(q,r) = m$ with $\gcd(q,r) = 1$. Then there are integers $s$ and $t$ so that $qt - rs = 1$, and we can form the unimodular matrix $U = \begin{bmatrix} q & s \\ r & t \end{bmatrix}$. If $g = f \circ U$, then Proposition 4.2.1 implies that $g = (m : \ell)$ for some integer $\ell$. But Proposition 4.1.1 shows that such a quadratic form can exist only when $m$ divides $\phi(\ell)$. So $\phi(x) \equiv 0 \pmod{m}$ must have a solution. Conversely, if $\ell$ is a solution of $\phi(x) \equiv 0 \pmod{m}$, then a quadratic form $g = (m : \ell)$ exists with discriminant $\Delta$. But then $g(1,0) = m$, so that $m$ is properly represented by some quadratic form of discriminant $\Delta$. □

Theorem 4.3.3 does not imply that *every* quadratic form of discriminant $\Delta$ represents all eligible values of $m$. For example, if $\Delta = -20$ so that $\phi(x) = x^2 + 5$, then the congruence $\phi(x) \equiv 0 \pmod{3}$ has solutions $x = 1$ and $x = -1$. But $m = 3$ is not represented by $\phi(x,y) = x^2 + 5y^2$, the principal form of discriminant $\Delta = -20$. (Following the method of the proof of Theorem 4.3.3, we find that $(3 : 1) = 3x^2 + 2xy + 2y^2$ in $\mathcal{Q}_\Delta$ represents 3, however.)

**Automorphs of Quadratic Forms.** In the remainder of this section, we will see that the *number* of proper representations of an integer $m$ by quadratic forms in $\mathcal{Q}_\Delta$ is essentially the number of solutions of $\phi(x) \equiv 0 \pmod{m}$. The following definition and results provide our method of counting representations in the right way.

**Definition.** Let $f$ be a quadratic form in $\mathcal{Q}_\Delta$ for some discriminant $\Delta$. Then a unimodular matrix $U$ is called an *automorph* of $f$ if $f \circ U = f$. We denote the set of all automorphs of $f$ as $\mathrm{Aut}(f)$.

**Exercise 4.3.2.** If $f$ is a quadratic form, show that $\mathrm{Aut}(f)$ is a subgroup of the group $\Gamma$ of all unimodular matrices.

We can describe all automorphs of an arbitrary quadratic form as follows.

**Proposition 4.3.4.** *If $f(x,y) = ax^2 + bxy + cy^2$, then*

$$\mathrm{Aut}(f) = \left\{ \begin{bmatrix} q & \frac{-cr}{a} \\ r & q + \frac{br}{a} \end{bmatrix} \;\middle|\; f(q,r) = a, \text{ and } a \text{ divides both } br \text{ and } cr \right\}.$$

*Proof.* If $f = (a : k)$ in ideal notation and $U = \begin{bmatrix} q & s \\ r & t \end{bmatrix}$ is a unimodular matrix, then Proposition 4.2.1 implies that $f \circ U = f$ if and only if $a = aq^2 + bqr + cr^2 = f(q,r)$ and $k = aqs + brs + crt + k$, so that $aqs + brs + crt = 0$. Assuming that these equations hold, then

$$as = (aq^2 + bqr + cr^2)s - (aqs + brs + crt)q = cr(rs - qt) = -cr$$

and

$$at = (aq^2 + bqr + cr^2)t - (aqs + brs + crt)r = (aq + br)(qt - rs) = aq + br.$$

Solving these equations for $s$ and $t$ yields the expression for $U$ in Proposition 4.3.4. The assumption that $a$ divides both $br$ and $cr$ is necessary and sufficient to ensure that $U$ has integer entries, and if $f(q, r) = a$, then the determinant of any such matrix equals 1. □

Note that $q = \pm 1$ and $r = 0$ always satisfy the requirements of Proposition 4.3.4. It follows that $\mathrm{Aut}(f)$ always contains $I$ and $-I$, where $I$ is the $2 \times 2$ identity matrix.

**Exercise 4.3.3.** Let $b$ and $c$ be integers for which $b^2 - 4c < -4$. Use Proposition 4.3.4 and equation (4.1.2) to show that $I$ and $-I$ are the only automorphs of $f(x, y) = x^2 + bxy + cy^2$.

**Proposition 4.3.5.** *Let $f$ be an element of $\mathcal{Q}_\Delta$ for some $\Delta$. If $f$ is equivalent to $g$, say with $g = f \circ V$, then $g = f \circ W$ if and only if $W = UV$ for some automorph $U$ of $f$. In this case, $U'$ is an automorph of $g$ if and only if $U' = V^{-1}UV$ for some automorph $U$ of $f$.*

*Proof.* If $W = UV$ for some automorph $U$ of $f$, then $f \circ W = (f \circ U) \circ V = f \circ V = g$. Conversely, if $f \circ W = g$, then $f \circ WV^{-1} = g \circ V^{-1} = f$, so that $WV^{-1}$ is an automorph of $f$. But then $W = UV$ for some automorph $U$ of $f$.

Now $g \circ V^{-1}UV = f \circ UV = f \circ V = g$, so that $V^{-1}UV$ is an automorph of $g$. Conversely, if $U'$ is an automorph of $g$, then $f \circ VU' = g \circ U' = g$. But then, by the preceding part of this proof, $VU' = UV$ for some automorph $U$ of $f$, so that $U' = V^{-1}UV$. □

In group terminology, Proposition 4.3.5 shows that if $f \sim g$ in $\mathcal{Q}_\Delta$, then the set of all $W$ for which $g = f \circ W$ is a right coset of $\mathrm{Aut}(f)$ in $\Gamma$, and that $\mathrm{Aut}(g)$ is a conjugate of $\mathrm{Aut}(f)$. In practice then, it will suffice to describe the automorphs of class representatives of quadratic forms of discriminant $\Delta$. We will do so for $\Delta < 0$ in Chapter 6 and for $\Delta > 0$ in Chapter 10.

**Equivalence of Representations.** Using automorphs of a quadratic form $f$, we can define an equivalence relation on representations of a particular integer $m$ by $f$ as follows.

**Definition.** If $\mathbf{x}$ and $\mathbf{y}$ are ordered pairs of integers and $f$ is a quadratic form, we say that $\mathbf{x}$ is *$f$-equivalent* to $\mathbf{y}$, and write $\mathbf{x} \sim_f \mathbf{y}$, if there is an automorph $U$ of $f$ for which $\mathbf{y} = U\mathbf{x}$. If $\mathbf{x} \sim_f \mathbf{y}$, then

$$f(\mathbf{y}) = \tfrac{1}{2} \cdot \mathbf{y}^T M_f \mathbf{y} = \tfrac{1}{2} \cdot (U\mathbf{x})^T M_f (U\mathbf{x}) = \tfrac{1}{2} \cdot \mathbf{x}^T (U^T M_f U)\mathbf{x} = f(\mathbf{x}).$$

The *number of representations* of an integer $m$ by $f$ is then defined to be the number of distinct $f$-equivalence classes of $\mathbf{x}$ for which $f(\mathbf{x}) = m$.

**Exercise 4.3.4.** If $f$ is a quadratic form of discriminant $\Delta$, show that the relation of $f$-equivalence is an equivalence relation on the set $\mathbb{Z} \times \mathbb{Z}$ (viewed as a set of $2 \times 1$ matrices with integer entries).

We have the following connection between proper representations of $m$ by $f$ and equivalence of quadratic forms.

**Theorem 4.3.6.** *Let $f = (a : k)$ be a quadratic form with discriminant $\Delta$. Then for every nonzero integer $m$, the number of distinct proper representations of $m$ by $f$ is equal to the number of distinct congruence classes of $\ell$ modulo $m$ for which $(a : k) \sim (m : \ell)$.*

Thus the number of distinct proper representations of $m$ by any $f$ in $\mathcal{Q}_\Delta$ is no larger than the number of solutions of $\phi(x) \equiv 0 \pmod{m}$, where $\phi(x)$ is the principal polynomial of discriminant $\Delta$.

*Proof.* Suppose that $f(\mathbf{v}) = m$, where $\mathbf{v} = (q, r)$ is primitive. There are integers $s$ and $t$ with $qt - rs = 1$, so that $V = \begin{bmatrix} q & s \\ r & t \end{bmatrix}$ is a unimodular matrix, and then $f \circ V = (m : \ell)$ for some $\ell$ by Proposition 4.2.1. We will show that the function $\sigma$ that sends $\mathbf{v}$ to $\ell$ is a bijection between $f$-equivalence classes of proper representations of $m$ by $f$ and congruence classes $\ell$ modulo $m$ for which $f \sim (m : \ell)$.

We first show that $\ell$ is well-defined modulo $m$. If $qt - rs = 1$, then we know that *all* pairs of integers $x$ and $y$ for which $qx - ry = 1$ are given by $(x, y) = (t + ru, s + qu)$ for some integer $u$. Thus all unimodular matrices whose first column is $\mathbf{v}$ have the form

$$VU = \begin{bmatrix} q & s \\ r & t \end{bmatrix} \cdot \begin{bmatrix} 1 & u \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} q & s + qu \\ r & t + ru \end{bmatrix}.$$

But now $f \circ VU = (m : \ell) \circ U = (m : \ell + mu)$ by Proposition 4.2.3, and so $\ell$ is unique modulo $m$.

Next we show that $\sigma$ is well-defined. Suppose that $\mathbf{v} \sim_f \mathbf{w}$, so that there is an automorph $T$ of $f$ for which $\mathbf{w} = T\mathbf{v}$. If we let $W = TV$, then the first column of $W$ is $\mathbf{w}$, and we find that $f \circ W = (f \circ T) \circ V = f \circ V = (m : \ell)$. So $\sigma$ is independent of the choice of $\mathbf{v}$ within its $f$-equivalence class.

To show that $\sigma$ is injective, suppose that $\sigma(\mathbf{v}) = \sigma(\mathbf{w})$. Then there are unimodular matrices $V$ and $W$, having first columns $\mathbf{v}$ and $\mathbf{w}$, respectively, for which $f \circ V = (m : \ell)$ and $f \circ W = (m : \ell')$, where $\ell' \equiv \ell \pmod{m}$. We can select a matrix $U = \begin{bmatrix} 1 & u \\ 0 & 1 \end{bmatrix}$ so that $(m : \ell) \circ U = (m : \ell')$, and then $f \circ VU = f \circ W$. By Proposition 4.3.5, there is an automorph $T$ of $f$ for which $W = TVU$. But

now we see that the first columns of $W$ and $TV$ are the same, which implies that $\mathbf{w} = T\mathbf{v}$, that is, $\mathbf{v} \sim_f \mathbf{w}$. Thus $\mathbf{v}$ and $\mathbf{w}$ are in the same $f$-equivalence class, and $\sigma$ is injective.

Finally, suppose that $\ell$ is some integer for which $(a : k) \sim (m : \ell)$. Then by definition there is a unimodular matrix $V$ so that $f \circ V = (m : \ell)$. If $\mathbf{v}$ is the first column of $V$, then $\mathbf{v}$ must be primitive since $\det V = 1$, and $f(\mathbf{v}) = m$. But then $\sigma(\mathbf{v})$ is the congruence class of $\ell$ modulo $m$, and $\sigma$ is surjective. Since we have established that $\sigma$ is a bijection, then the number of distinct proper representations of $m$ by $f$ is equal to the number of distinct congruence classes of $\ell$ modulo $m$ for which $(a : k) \sim (m : \ell)$. □

**Example.** Let $\Delta = -23$, so that $\phi(x) = x^2 + x + 6$, and let $m = 87 = 3 \cdot 29$. Here $\left(\frac{-23}{3}\right) = 1 = \left(\frac{-23}{29}\right)$, so there are four solutions of $\phi(x) \equiv 0 \pmod{87}$, which we find to be $x = 18, -19, 39$, and $-40$. Theorem 4.3.3 implies that there is at least one quadratic form $f$ in $\mathcal{Q}_{-23}$ that properly represents 87. We can go further by Theorem 4.3.6 to say that there are essentially four distinct proper representations of 87 by *classes* of forms of discriminant $\Delta = -23$.

In an example in §4.2, we found that $f = (87 : 18) \sim (2 : 0) = g$, specifically that $(2 : 0) = (87 : 18) \circ U$ with $U = \begin{bmatrix} -1 & -1 \\ 5 & 4 \end{bmatrix}$. Since $f(1,0) = 87$, then $g(x,y) = 2x^2 + xy + 3y^2$ must also represent 87. Using the proof of Theorem 4.3.1, we find in fact that

$$\begin{bmatrix} q \\ r \end{bmatrix} = U^{-1} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 4 & 1 \\ -5 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 4 \\ -5 \end{bmatrix}$$

satisfies $g(q,r) = 87$, as one can verify. ◊

**Exercise 4.3.5.** Show that $(87 : 39) \sim (1 : 0)$ in $\mathcal{Q}_{-23}$. Use that fact to find a representation of 87 by $h(x,y) = x^2 + xy + 6y^2$.

## 4.4 Genera of Quadratic Forms

We conclude Chapter 4 by introducing another equivalence relation on quadratic forms of a fixed discriminant $\Delta$. This relation is based on the following restrictions on representations of integers by *primitive* quadratic forms.

**Proposition 4.4.1.** *Let $f(x,y) = ax^2 + bxy + cy^2$ be a primitive quadratic form, and let $p$ be a prime number that divides $\Delta = b^2 - 4ac$. Suppose that $m$ and $n$ are integers represented by $f$, and that $p$ divides neither $m$ nor $n$. If $p$ is odd, then $\left(\frac{m}{p}\right) = \left(\frac{n}{p}\right)$. If $p = 2$ and $\Delta_0 = \frac{\Delta}{4}$, then the following statements are true.*

(1) *If $\Delta_0 \equiv 3 \pmod 4$ or $\Delta_0 \equiv 4 \pmod 8$, then $mn \equiv 1 \pmod 4$.*

(2) *If* $\Delta_0 \equiv 2 \pmod 8$, *then* $mn \equiv 1$ *or* $7 \pmod 8$.

(3) *If* $\Delta_0 \equiv 6 \pmod 8$, *then* $mn \equiv 1$ *or* $3 \pmod 8$.

(4) *If* $\Delta_0 \equiv 0 \pmod 8$, *then* $mn \equiv 1 \pmod 8$.

Note that if a discriminant $\Delta$ is even, then $\Delta \equiv 0 \pmod 4$, so that $\Delta_0$ is an integer as given above.

*Proof.* If $p$ divides $\Delta = b^2 - 4ac$ and $p$ divides either $a$ or $c$, then $p$ also divides $b$. So if we assume that $f$ is primitive, then $a$ or $c$ (or both) is *not* divisible by $p$. To simplify the proof, we will assume that $p$ does not divide $a$. It then suffices to establish the statements above with $a$ in place of $n$.

Recall from equation (4.1.2) that if $f(q, r) = m$ for some $q$ and $r$, then $4am = (2aq + br)^2 - \Delta r^2$. If $p$ divides $\Delta$, then $4am$ is congruent to a square modulo $p$. In particular, if $p$ is odd and $p$ does not divide $m$, then $\left(\frac{4am}{p}\right) = 1$, from which it follows immediately that $\left(\frac{m}{p}\right) = \left(\frac{a}{p}\right)$.

Now suppose that $p = 2$ divides $\Delta$, so that $b$ is even. In this case, we have

$$am = \left(aq + \frac{b}{2} \cdot r\right)^2 - \frac{\Delta}{4} \cdot r^2 = t^2 - \Delta_0 r^2,$$

with $\Delta_0 = \frac{\Delta}{4}$, for some integers $t$ and $r$. The square of an integer $t$ is congruent to 0 modulo 4 (if $t$ is even) or to 1 modulo 8 (if $t$ is odd). Assume first that $\Delta_0$ is odd, as are $a$ and $m$. If $\Delta_0 \equiv 1 \pmod 4$, we find that $am$ is congruent to $1 - 0$ or $0 - 1$ modulo 4, so that there is no restriction on this product. But if $\Delta_0 \equiv 3 \pmod 4$, then $am$ is congruent to $1 - 0$ or $0 - 3$ modulo 4, that is, $am \equiv 1 \pmod 4$.

Now assume that $\Delta_0$ is even. Here $t$ must be odd if $a$ and $m$ are both odd. We conclude that $am$ is congruent to $1 - 0$ modulo 8 if $r$ is even, and $am$ is congruent to $1 - \Delta_0$ modulo 8 if $r$ is odd. Our conclusions in each of cases (1)–(4) follow directly. □

**Definition.** Let $f(x, y) = ax^2 + bxy + cy^2$ be a primitive quadratic form of discriminant $\Delta$. Then we define a collection of *genus symbols* for $f$ as follows. If $p$ is an odd prime dividing $\Delta$, and $m$ is an integer represented by $f$ with $p$ not dividing $m$, let $\left(\frac{f}{p}\right) = \left(\frac{m}{p}\right)$. If $p = 2$ divides $\Delta$, with $\Delta_0 = \frac{\Delta}{4}$, and $m$ is an odd integer represented by $f$, then:

(1) If $\Delta_0 \equiv 0$ or $3 \pmod 4$, let $\left(\frac{-1}{f}\right) = \begin{cases} 1, & \text{if } m \equiv 1 \pmod 4, \\ -1, & \text{if } m \equiv 3 \pmod 4. \end{cases}$

(2) If $\Delta_0 \equiv 0$ or $2 \pmod 8$, let $\left(\frac{2}{f}\right) = \begin{cases} 1, & \text{if } m \equiv 1 \text{ or } 7 \pmod 8, \\ -1, & \text{if } m \equiv 3 \text{ or } 5 \pmod 8. \end{cases}$

(3) If $\Delta_0 \equiv 0$ or $6 \pmod 8$, let $\left(\frac{-2}{f}\right) = \begin{cases} 1, & \text{if } m \equiv 1 \text{ or } 3 \pmod 8, \\ -1, & \text{if } m \equiv 5 \text{ or } 7 \pmod 8. \end{cases}$

If $\Delta < 0$, we also let $\left(\frac{f}{\infty}\right)$ equal 1 if $m > 0$ and $-1$ if $m < 0$.

Proposition 4.4.1 shows that genus symbols are well-defined. When $\Delta$ is negative, the symbol $\left(\frac{f}{\infty}\right)$ merely distinguishes between positive definite and negative definite forms. In practice, we can always use $f(1,0) = a$ or $f(0,1) = c$ in place of $m$ in calculating the relevant genus symbols.

**Example.** Let $f(x,y) = 15x^2 - 10xy + 6y^2$, with discriminant

$$\Delta = (-10)^2 - 4 \cdot 15 \cdot 6 = -260 = -1 \cdot 2^2 \cdot 5 \cdot 13.$$

Here $\frac{\Delta}{4} = -65 \equiv 3 \pmod 4$, so the symbols $\left(\frac{f}{5}\right)$, $\left(\frac{f}{13}\right)$, $\left(\frac{-1}{f}\right)$, and $\left(\frac{f}{\infty}\right)$ are defined. Since 5 does not divide $c = 6$, then $\left(\frac{f}{5}\right) = \left(\frac{6}{5}\right) = \left(\frac{1}{5}\right) = 1$. We can use $a = 15$ for each of the other symbols. We find that $\left(\frac{f}{13}\right) = \left(\frac{15}{13}\right) = \left(\frac{2}{13}\right) = -1$, $\left(\frac{-1}{f}\right) = -1$ since $15 \equiv 3 \pmod 4$, and $\left(\frac{f}{\infty}\right) = 1$ since 15 is positive. ◊

**Definition.** If $f$ and $g$ are primitive quadratic forms in $\mathcal{Q}_\Delta$ for some $\Delta$, and $f$ and $g$ have the same collection of genus symbols, then we say that $f$ is in the same *genus* as $g$ (pluralized as *genera*), or that $f$ is *genus equivalent* to $g$, and we write $f \approx g$. More generally, if $f$ and $g$ have the same index, $\gamma(f) = \gamma = \gamma(g)$, with $f(x,y) = \gamma \cdot f_1(x,y)$ and $g(x,y) = \gamma \cdot g_1(x,y)$, we define $f$ to be genus equivalent to $g$ if and only if $f_1 \approx g_1$.

Genus equivalence is an equivalence relation on $\mathcal{Q}_\Delta$. Furthermore, Theorem 4.3.1 shows that if $f$ is equivalent to $g$, then $f$ is genus equivalent to $g$, since then $f$ and $g$ represent the same integers, and so must have the same collection of genus symbols. Thus we can view a genus of forms as being made up of classes of forms.

**The Number of Genera of a Discriminant.** If there are $t$ genus symbols defined for quadratic forms of some discriminant $\Delta$, then there are $2^t$ different ways in which we can assign those symbols the values $+1$ or $-1$. But not all combinations of these symbols take place in practice. We describe those that can occur in the next two propositions. We will assume that if $f(x,y)$ is a quadratic form of discriminant $\Delta$, then there is some odd positive integer $q$ that is relatively prime to $\Delta$ so that $f$ represents $q$ (or $f$ represents $-q$ when $f$ is negative definite).

**Proposition 4.4.2.** *Let $f$ be a quadratic form of primitive discriminant $\Delta$. Then the product of all genus symbols defined for $f$ must equal* 1.

*Proof.* If $\Delta$ is a primitive discriminant, we can write

$$\Delta = (-1)^e \cdot 2^j \cdot p_1 \cdots p_k \cdot p_{k+1} \cdots p_\ell,$$

where each $p_i$ is a distinct odd prime, with $p_i \equiv 3 \pmod 4$ for $1 \le i \le k$ and $p_i \equiv 1 \pmod 4$ for $k+1 \le i \le \ell$, and where $e = 0$ or 1 and $j = 0$, 2, or 3. (Either $k$ or $\ell - k$ might equal 0.) Let $f$ be a quadratic form of discriminant $\Delta$, assumed at first to be positive definite, so that $\left(\frac{f}{\infty}\right) = 1$, if $\Delta < 0$. Suppose that $q$ is an odd positive integer represented by $f$, relatively prime to $\Delta$. By Theorem 4.3.3, we know that $\phi(x) \equiv 0 \pmod q$ must have a solution, where $\phi(x)$ is the principal polynomial of discriminant $\Delta$, so it follows that the Jacobi symbol $\left(\frac{\Delta}{q}\right)$ must equal 1. (See Exercise 0.3.5.) If $p_i \equiv 1 \pmod 4$, then $\left(\frac{p_i}{q}\right) = \left(\frac{q}{p_i}\right)$, while if $p_i \equiv 3 \pmod 4$, then $\left(\frac{p_i}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{-p_i}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{q}{p_i}\right)$. (See Exercise 0.2.7.) So we find that

$$\begin{aligned} 1 = \left(\frac{\Delta}{q}\right) &= \left(\frac{-1}{q}\right)^e \left(\frac{2}{q}\right)^j \left(\frac{p_1}{q}\right) \cdots \left(\frac{p_k}{q}\right) \cdot \left(\frac{p_{k+1}}{q}\right) \cdots \left(\frac{p_\ell}{q}\right) \\ &= \left(\frac{-1}{q}\right)^{e+k} \left(\frac{2}{q}\right)^j \left(\frac{q}{p_1}\right) \cdots \left(\frac{q}{p_k}\right) \cdot \left(\frac{q}{p_{k+1}}\right) \cdots \left(\frac{q}{p_\ell}\right). \end{aligned} \quad (4.4.1)$$

Each $\left(\frac{q}{p_i}\right)$ is the same as the genus symbol $\left(\frac{f}{p_i}\right)$ for $1 \le i \le \ell$. We now consider four cases, one of which must occur if $\Delta$ is primitive.

(1) If $\Delta \equiv 1 \pmod 4$, then $j = 0$, and we find that if $e = 0$, then $k$ is even, while if $e = 1$, then $k$ is odd. So $e + k$ is even in either case, and equation (4.4.1) becomes $1 = \left(\frac{f}{p_1}\right) \cdots \left(\frac{f}{p_\ell}\right)$. That is, the product of all defined genus symbols equals 1.

(2) If $\frac{\Delta}{4} \equiv 3 \pmod 4$, then $j = 2$, and $k$ is odd when $e = 0$ but $k$ is even if $e = 1$. Now $e + k$ is odd in each case, so that equation (4.4.1) becomes $1 = \left(\frac{-1}{q}\right)\left(\frac{f}{p_1}\right) \cdots \left(\frac{f}{p_\ell}\right)$. Here $\left(\frac{-1}{q}\right) = \left(\frac{-1}{f}\right)$, and again the product of all genus symbols equals 1.

(3) If $\frac{\Delta}{4} \equiv 2 \pmod 8$ (or equivalently $\frac{\Delta}{8} \equiv 1 \pmod 4$), then $j = 3$, and we again find that $e + k$ is even in every case. So now $1 = \left(\frac{2}{q}\right)\left(\frac{f}{p_1}\right) \cdots \left(\frac{f}{p_\ell}\right)$. Here $\left(\frac{2}{q}\right) = \left(\frac{2}{f}\right)$ is a defined genus symbol.

(4) If $\frac{\Delta}{4} \equiv 6 \pmod 8$, then $j = 3$ and $e+k$ is odd. In this case, equation (4.4.1) implies that $1 = \left(\frac{-1}{q}\right)\left(\frac{2}{q}\right)\left(\frac{f}{p_1}\right)\cdots\left(\frac{f}{p_\ell}\right) = \left(\frac{-2}{q}\right)\left(\frac{f}{p_1}\right)\cdots\left(\frac{f}{p_\ell}\right)$. Here $\left(\frac{-2}{q}\right) = \left(\frac{-2}{f}\right)$ is a defined genus symbol.

So if $\Delta$ is positive, or if $\Delta$ is negative and $f$ is positive definite, then the product of all genus symbols equals 1. If $g$ is negative definite, then $g = -f$ for some positive definite quadratic form $f$, and if $f$ represents $q$ as above, then $g$ represents $-q$. We find that $\left(\frac{g}{p_i}\right) = \left(\frac{-q}{p_i}\right) = -\left(\frac{f}{p_i}\right)$ for $1 \le i \le k$, but $\left(\frac{g}{p_i}\right) = \left(\frac{f}{p_i}\right)$ for $k+1 \le i \le \ell$. Also $\left(\frac{-1}{g}\right) = -\left(\frac{-1}{f}\right)$ since if $q \equiv 1 \pmod 4$, then $-q \equiv 3 \pmod 4$. But $\left(\frac{2}{g}\right) = \left(\frac{2}{f}\right)$ since $q \equiv 1$ or $7 \pmod 8$ if and only if $-q \equiv 1$ or $7 \pmod 8$. In each of the four cases above, we find that an odd number of symbols are changed in sign, but since $\left(\frac{g}{\infty}\right) = -1$, we still have the product of all defined genus symbols equal to 1. □

**Proposition 4.4.3.** *Let $\Delta = \Delta(d,\gamma)$ for some $\gamma > 1$ and let $\Delta_1 = \Delta(d,1)$. If $f$ is a primitive quadratic form of discriminant $\Delta$, then the product of all genus symbols for $f$ that are also defined for a quadratic form of discriminant $\Delta_1$ must equal 1. If $\frac{\Delta}{4} \equiv 0 \pmod 8$, so that $\left(\frac{-1}{f}\right)$, $\left(\frac{2}{f}\right)$, and $\left(\frac{-2}{f}\right)$ are all defined, then their product must equal 1. Any other genus symbols defined for $f$ can equal either 1 or $-1$.*

*Proof.* Suppose that $q$ is an odd positive integer, relatively prime to $\Delta$, that is represented by $f$. If $\Delta = \gamma^2\Delta_1$ with $\Delta_1$ primitive, we have that $\left(\frac{\Delta}{q}\right) = \left(\frac{\Delta_1}{q}\right)$. The proof of Proposition 4.4.2 shows that the product of all genus symbols defined for $\Delta_1$ must equal 1. If $\left(\frac{-1}{f}\right)$, $\left(\frac{2}{f}\right)$, and $\left(\frac{-2}{f}\right)$ are all defined, we find by testing all possibilities for $q$ modulo 8 that the product of these symbols must be 1. There are no restrictions on any remaining symbols. □

We illustrate the claims of these propositions with some examples to conclude this section. Here the listing of certain quadratic forms of a particular genus is by trial-and-error. We will see a systematic method of finding representatives of all possible classes and genera of quadratic forms of negative discriminant in §6.1 and of positive discriminant in §10.1 and §10.2.

**Example.** Let $\Delta = \Delta(6,1) = 24 = 2^3 \cdot 3$, a primitive discriminant. The genus symbols defined for a form $f$ of discriminant $\Delta$ are $\left(\frac{f}{3}\right)$ and $\left(\frac{-2}{f}\right)$. Their product must equal 1, so there are only two possible genera. We find that $f(x,y) = x^2 - 6y^2$

is a quadratic form of discriminant $\Delta = 24$ with $\left(\frac{f}{3}\right) = 1 = \left(\frac{-2}{f}\right)$, while for $g(x,y) = 2x^2 - 3y^2$, we have $\left(\frac{g}{3}\right) = -1 = \left(\frac{-2}{g}\right)$. ◊

**Example.** Let $\Delta = \Delta(6,2) = 96 = 2^5 \cdot 3$, so that $\Delta_1 = 24$ in the notation of Proposition 4.4.3. From the preceding example, we see that $2x^2 - 12y^2$ and $4x^2 - 6y^2$ are forms of index two in $\mathcal{Q}_\Delta$, representing distinct genera. (We do not define genus symbols for these forms, however.) For primitive forms, the genus symbols $\left(\frac{f}{3}\right)$, $\left(\frac{-2}{f}\right)$, $\left(\frac{-1}{f}\right)$, and $\left(\frac{2}{f}\right)$ are defined, but we must have $\left(\frac{f}{3}\right)\left(\frac{-2}{f}\right) = 1$, as for $\Delta_1 = 24$. There is no restriction on $\left(\frac{-1}{f}\right)$, but then $\left(\frac{-2}{f}\right)\left(\frac{-1}{f}\right)\left(\frac{2}{f}\right) = 1$. So there are at most four genera. In fact, we find the following representatives of each possible genus:

$$\begin{aligned} ++++ &: \quad x^2 - 24y^2 \\ ---+ &: \quad -x^2 + 24y^2 \\ ++-- &: \quad 3x^2 - 8y^2 \\ --+- &: \quad -3x^2 + 8y^2. \end{aligned}$$

Here we write the symbols as $+$ or $-$, in order as $\left(\frac{f}{3}\right)$, $\left(\frac{-2}{f}\right)$, $\left(\frac{-1}{f}\right)$, and $\left(\frac{2}{f}\right)$. ◊

**Example.** Let $\Delta = \Delta(2,15) = 1800 = 2^3 \cdot 3^2 \cdot 5^2$, so that $\Delta_1 = 8$. The genus symbols $\left(\frac{2}{f}\right)$, $\left(\frac{f}{3}\right)$, and $\left(\frac{f}{5}\right)$ are defined for elements of $\mathcal{Q}_\Delta$, with $\left(\frac{2}{f}\right) = 1$ the only restriction. We find the following representatives of the possible genera of primitive forms:

$$\begin{aligned} +++ &: \quad x^2 - 450y^2 \\ +-+ &: \quad -x^2 + 450y^2 \\ +-- &: \quad 2x^2 - 225y^2 \\ ++- &: \quad -2x^2 + 225y^2 \end{aligned}$$

with symbols $\left(\frac{2}{f}\right)$, $\left(\frac{f}{3}\right)$, and $\left(\frac{f}{5}\right)$ in order. ◊

**Exercise 4.4.1.** In each part, find all genus symbols that are defined for a primitive quadratic form of discriminant $\Delta$, determine the combinations of genus symbols that can actually occur, and find an example of a quadratic form having that collection of genus symbols.

(a) $\Delta = 21$.

(b) $\Delta = 28$.

(c) $\Delta = 56$.

(d) $\Delta = 84$.

(e) $\Delta = 112$.

(f) $\Delta = 224$.

## Quadratic Forms—Review

In this chapter, we introduced collections $\mathcal{Q}_\Delta$ of quadratic forms $f(x, y) = ax^2 + bxy + cy^2$ of a fixed discriminant $\Delta$ as our objects of study, with the question of which integers are *represented* by $f$ as our main motivation. We summarize our main definitions and results as follows.

(1) Elements of $\mathcal{Q}_\Delta$ are in one-to-one correspondence with pairs $(a : k)$ for which $a$ divides $\phi(k)$, where $\phi(x)$ is the principal polynomial of discriminant $\Delta$. In this way, we define an alternative notation for a quadratic form $f$, which we call *ideal notation* because of its similarity to our notation for ideals of the quadratic domain of discriminant $\Delta$.

(2) There is a relation of *equivalence* on quadratic forms of a given discriminant defined in terms of matrix multiplication. Equivalent forms represent the same collection of integers.

(3) The number of representations of a particular integer $m$ by some quadratic form of discriminant $\Delta$ is essentially the same (using *automorphs* of a form, and a relation of *$f$-equivalence* on ordered pairs) as the number of solutions of the congruence $\phi(x) \equiv 0 \pmod{m}$.

(4) There is a relation of *genus equivalence* on quadratic forms of a particular discriminant, defined in terms of congruence classes of integers represented by a given form. We can determine the number of distinct equivalence classes (*genera*) of $\mathcal{Q}_\Delta$ under this relation in terms of the prime factorization of $\Delta$.

In the following chapter, we explore the connection between quadratic forms and ideals, which is suggested by our similar notation for both types of objects.

# 5

# Correspondence between Forms and Ideals

Let $\phi(x)$ be the principal polynomial of some discriminant $\Delta$. In Chapter 3, we showed that every primitive ideal of the quadratic domain $D_\Delta$ can be expressed as

$$A = [a : k] = \{ma + n(k + z) \mid m, n \in \mathbb{Z}\},$$

where $a$ and $k$ are integers for which $a$ divides $\phi(k)$, and $z$ is the basis element of discriminant $\Delta$. In Chapter 4, we found that every quadratic form of discriminant $\Delta$ can be written as

$$f = (a : k) = ax^2 + bxy + cy^2,$$

where $\phi(k) = ac$, so that $a$ again divides $\phi(k)$, and $\phi'(k) = b$. This similarity suggests a close relation between quadratic forms with a particular discriminant $\Delta$ and ideals of the quadratic domain $D_\Delta$. Our goal in this chapter is to justify this similar "ideal number" notation for ideals and quadratic forms by exploring connections between these objects more fully.

In §5.1 and §5.2, we define an equivalence relation on ideals of a quadratic domain. We will find that equivalence classes of ideals and of quadratic forms (under the equivalence relation introduced in §4.2) are essentially identical. In §5.3, we introduce an operation of composition on classes of quadratic forms. We will establish that this operation is interchangeable with ideal multiplication, as defined and computed in §3.4 and §3.6. We conclude this chapter with the definition of a group structure on equivalence classes of ideals or of quadratic domains in §5.4. In later chapters, we will see how we can apply these *class groups* to describe representations of integers by quadratic forms.

## 5.1 Equivalence of Ideals

We can define a mapping from quadratic forms to ideals as follows.

**Definition.** If $f = (a : k)$ is a quadratic form of discriminant $\Delta$, then $A_f = [a : k]$ is a primitive ideal of $D_\Delta$, which we call the *ideal of* $f$.

As noted above, $A_f$ is in fact an ideal of $D_\Delta$ since $a$ divides $\phi(k)$. If $k = \frac{b-\varepsilon}{2}$ and $z = \frac{\varepsilon+\sqrt{\Delta}}{2}$ as in (2.2.2), then $k + z = \frac{b+\sqrt{\Delta}}{2}$. Therefore, if $f(x, y) = ax^2 + bxy + cy^2$ is a quadratic form of discriminant $\Delta$, then we can also express this ideal as

$$A_f = \left\{ ma + n\left(\frac{b+\sqrt{\Delta}}{2}\right) \mid m, n \in \mathbb{Z} \right\}.$$

It is also true that if $A = [a : k]$ is an ideal of $D_\Delta$, then $(a : k)$ is a quadratic form of discriminant $\Delta$. But we have noted that $[a : k] = [-a : k]$ and $[a : k] = [a : \ell]$ if $\ell \equiv k \pmod{a}$, whereas $(a : k) \neq (-a : k)$ and $(a : k) = (a : \ell)$ only when $k = \ell$. Thus a mapping in this direction is not well-defined. In this section, we define an equivalence relation on ideals, and we will then establish a precise correspondence between *equivalence classes* of ideals and of quadratic forms.

**Definition.** Let $A$ and $B$ be nontrivial ideals of $D = D_\Delta$. We say that $A$ is *equivalent* to $B$, written $A \sim B$, if there is a nonzero rational integer $m$ and a nonzero element $\upsilon$ of $D$ so that $mA = \upsilon B$.

The definition of ideal equivalence is often given as $A \sim B$ if $wA = \upsilon B$ for nonzero elements $w$ and $\upsilon$ of $D$. But since then $N(w)A = \overline{w} \cdot wA = (\overline{w}\upsilon)B$, we may assume without loss of generality that $w$ is a rational integer.

**Exercise 5.1.1.** Show that $\upsilon B = \{\upsilon x \mid x \in B\}$ is equal to the product of ideals $\langle \upsilon \rangle B$.

We compile some important properties of this relation in the following propositions and exercises.

**Proposition 5.1.1.** *Equivalence of ideals is an equivalence relation on the set of nontrivial ideals of a quadratic domain $D$.*

*Proof.* Let $A$, $B$, and $C$ be nontrivial ideals of $D$.

(1) Since $1 \cdot A = 1 \cdot A$, then $A \sim A$ and $\sim$ is reflexive.

(2) Suppose that $A \sim B$, so that $mA = \upsilon B$ for some nonzero integer $m$ and nonzero element $\upsilon$ of $D$. Then $\overline{\upsilon}(\upsilon B) = \overline{\upsilon}(mA)$, implying that $N(\upsilon)B = (m\overline{\upsilon})A$. So $B \sim A$ and $\sim$ is symmetric.

(3) Suppose that $A \sim B$ and $B \sim C$, so that $mA = \upsilon B$ and $nB = wC$ for some nonzero integers $m$ and $n$, and nonzero elements $\upsilon$ and $w$ of $D$. Then $(mn)A = n(mA) = n(\upsilon B) = \upsilon(nB) = (\upsilon w)C$, so that $A \sim C$, and $\sim$ is transitive. □

**Proposition 5.1.2.** *A nontrivial ideal $A$ of a quadratic domain $D$ is a principal ideal if and only if $A$ is equivalent to $D$ (as an ideal of itself).*

*Proof.* If $A = \langle u \rangle$, then $1 \cdot A = u \cdot D$, so that $A \sim D$. Conversely, suppose that $A \sim D$, so that $mA = \upsilon D$ for some $m \neq 0$ in $\mathbb{Z}$ and $\upsilon \neq 0$ in $D$. Then $\upsilon = \upsilon \cdot 1 = mu$ for some $u$ in $A$. Since $mA = muD$ with $m \neq 0$, then $A = uD = \langle u \rangle$, a principal ideal. □

**Exercise 5.1.2.** Let $A_1$, $A_2$, $B_1$, and $B_2$ be nontrivial ideals of a quadratic domain $D$. Show that if $A_1$ is equivalent to $B_1$ and $A_2$ is equivalent to $B_2$, then $A_1A_2$ is equivalent to $B_1B_2$.

**Exercise 5.1.3.** If $A$ is a nontrivial ideal of a quadratic domain $D$, and $\upsilon$ is a nonzero element of $D$, show that $\upsilon A$ is equivalent to $A$.

**Exercise 5.1.4.** If $A$ and $B$ are nontrivial ideals of a quadratic domain $D$, and $A$ is equivalent to $B$, show that $\overline{A}$ is equivalent to $\overline{B}$.

**Proposition 5.1.3.** *If $A$ and $B$ are equivalent ideals of a quadratic domain $D$, then $A$ and $B$ have the same index.*

*Proof.* Suppose that $A \sim B$, so that $mA = \upsilon B$ for some $m \neq 0$ in $\mathbb{Z}$ and $\upsilon \neq 0$ in $D$. Then $\langle m \rangle A = \langle \upsilon \rangle B$, so that

$$\gamma(\langle m \rangle A) = \operatorname{lcm}(\gamma(\langle m \rangle), \gamma(A)) = \operatorname{lcm}(\gamma(\langle \upsilon \rangle), \gamma(B)) = \gamma(\langle \upsilon \rangle B),$$

by Theorem 3.6.6. But a principal ideal always has index 1 by Corollary 3.6.4. It follows that $\operatorname{lcm}(\gamma(\langle m \rangle), \gamma(A)) = \gamma(A)$ and $\operatorname{lcm}(\gamma(\langle \upsilon \rangle), \gamma(B)) = \gamma(B)$, and so $\gamma(A) = \gamma(B)$. □

**Exercise 5.1.5.** If $f$ is a quadratic form of discriminant $\Delta$ and $A_f$ is its corresponding ideal of $D_\Delta$, show that the index of $f$ is the same as the index of $A_f$.

**Proposition 5.1.4.** *Let $A$ and $B$ be nontrivial ideals of a quadratic domain $D$. If $A\overline{B}$ is a principal ideal, then $A$ is equivalent to $B$. Conversely, if $A$ is equivalent to $B$ and $\gamma(A) = 1$, then $A\overline{B}$ is a principal ideal.*

*Proof.* Suppose that $A\overline{B}$ is a principal ideal. Since a principal ideal has index 1, it follows that $\gamma(A\overline{B}) = \operatorname{lcm}(\gamma(A), \gamma(\overline{B})) = 1$ and thus $\gamma(A) = 1 = \gamma(\overline{B})$. Now Proposition 5.1.2 implies that $A\overline{B} \sim D$, and so $(A\overline{B})B \sim DB$ by Exercise 5.1.2.

But $DB = B$, and $(A\overline{B})B = (B\overline{B})A = N(B)A$ using Theorem 3.4.2. Thus we have $A \sim N(B)A \sim B$ by Exercise 5.1.3.

Conversely, suppose that $A \sim B$, and that $\gamma(A) = 1$, so that $\gamma(B) = 1$ by Proposition 5.1.3. Now $A\overline{B} \sim B\overline{B}$ by Exercise 5.1.2, and $B\overline{B} = \langle N(B)\rangle$ is a principal ideal by Theorem 3.4.2. □

The converse statement of Proposition 5.1.4 is not generally true without the additional assumption that $\gamma(A) = 1$. For example, consider $A = [2 : 0]$ in $D = D_{-12}$, for which $\gamma(A) = 2$. Here $A$ is equivalent to itself, but $A\overline{A} = A^2 = 2[2 : 0]$ is not a principal ideal of $D$. Otherwise, $A = [2 : 0]$ would be principal, but we demonstrated that this is not the case in an example in §3.6.

We now state and prove our main result for this section, connecting equivalence of quadratic forms to equivalence of ideals.

**Theorem 5.1.5.** *Let $f = (a : k)$ and $f_1 = (a_1 : k_1)$ be quadratic forms of discriminant $\Delta$, and let $A = A_f = [a : k]$ and $A_1 = A_{f_1} = [a_1 : k_1]$ be the corresponding ideals of $D_\Delta$. If $f$ is equivalent to $f_1$, then $A$ is equivalent to $A_1$.*

*Proof.* Let $D = D_\Delta = \{m + nz \mid m, n \in \mathbb{Z}\}$, where $z = z_\Delta$. Let $w = k + z$ and $\overline{w} = k + \overline{z}$, and let $\phi(x)$ be the principal polynomial of discriminant $\Delta$. We can write $f(x, y) = ax^2 + bxy + cy^2$, where

$$ac = \phi(k) = w\overline{w} \qquad \text{and} \qquad b = \phi'(k) = w + \overline{w}. \tag{5.1.1}$$

Let $U = \begin{bmatrix} q & s \\ r & t \end{bmatrix}$ be a unimodular matrix for which $f_1 = f \circ U$, so that

$$a_1 = aq^2 + bqr + cr^2 \qquad \text{and} \qquad k_1 = aqs + brs + crt + k, \tag{5.1.2}$$

as in Proposition 4.2.1.

We will show that $a_1 A = \upsilon A_1$, where $\upsilon = qa + rw$, so that $A \sim A_1$ as ideals of $D = D_\Delta$. We first establish that

$$\upsilon \cdot a_1 = a_1(qa + rw) \qquad \text{and} \qquad \upsilon \cdot w_1 = a_1(sa + tw), \tag{5.1.3}$$

where $w_1 = k_1 + z = aqs + brs + crt + w$, using (5.1.2). This will imply that $\upsilon A_1$ is a subset of $a_1 A$, since the typical element of $\upsilon A_1$, namely $\upsilon(ma_1 + nw_1) = m(\upsilon a_1) + n(\upsilon w_1)$, is then a $\mathbb{Z}$-combination of $a_1 a$ and $a_1 w$. The first equation in (5.1.3) is immediate from the definition of $\upsilon$. For the second, note that

$$\begin{aligned} \upsilon w_1 &= (qa + rw)(aqs + brs + crt + w) \\ &= a^2q^2s + abqrs + acqrt + aqw + aqrsw + br^2sw + cr^2tw + rw^2 \end{aligned} \tag{5.1.4}$$

and

$$\begin{aligned} a_1(sa + tw) &= (aq^2 + bqr + cr^2)(sa + tw) \\ &= a^2q^2s + abqrs + acr^2s + aq^2tw + bqrtw + cr^2tw. \end{aligned} \tag{5.1.5}$$

Subtracting (5.1.5) from (5.1.4) produces

$$vw_1 - a_1(sa + tw) = acr(qt - rs) + aqw + aqw(rs - qt) + brw(rs - qt) + rw^2$$
$$= acr - brw + rw^2 = r(w\overline{w} - (w + \overline{w})w + w^2) = r(w\overline{w} - w^2 - w\overline{w} + w^2) = 0,$$

using the fact that $qt - rs = 1$ (as $U$ is unimodular), and the expressions for $ac$ and $b$ in (5.1.1).

Now we show that

$$a_1 \cdot a = v(ta_1 - rw_1) \qquad \text{and} \qquad a_1 \cdot w = v(-sa_1 + qw_1). \tag{5.1.6}$$

Here the equations of (5.1.3) imply that

$$v(ta_1 - rw_1) = tva_1 - rvw_1 = t(a_1(qa + rw)) - r(a_1(sa + tw))$$
$$= a_1(qta + rtw - rsa - rtw) = a_1(qt - rs)a = a_1 a$$

and

$$v(-sa_1 + qw_1) = -sva_1 + qvw_1 = -s(a_1(qa + rw)) + q(a_1(sa + tw))$$
$$= a_1(-qsa - rsw + qsa + qtw) = a_1(qt - rs)w = a_1 w.$$

The equations in (5.1.6) establish that $a_1 A \subseteq vA_1$ and complete the proof. □

The following special case of Theorem 5.1.5, corresponding to the involution of a quadratic form, will be particularly useful.

**Corollary 5.1.6.** *Let $A = [a : k]$ be an ideal of a quadratic domain $D_\Delta$. Let $\phi(x)$ be the principal polynomial of discriminant $\Delta$. If $\phi(k) = ac$ for some integer $c$, then $A$ is equivalent to the ideal $C = [c : -k - \varepsilon]$, with $cA = (k + z)C$.*

*Proof.* For quadratic forms, we have $(a : k) \sim (c : -k - \varepsilon)$ by Proposition 4.2.2, so the equivalence of $A = [a : k]$ and $C = [c : -k - \varepsilon]$ is immediate from Theorem 5.1.5. Specifically, $(c : -k - \varepsilon) = (a : k) \circ \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, so the proof of Theorem 5.1.5 shows that $cA = vC$, where $v = 0 \cdot a + 1 \cdot (k + z) = k + z$. □

**Example.** Let $\Delta = \Delta(-79, 1) = -79$, so that $z = \frac{1+\sqrt{-79}}{2}$ and $\phi(x) = x^2 + x + 20$. Since $\phi(45) = 110 \cdot 19$, we have that $A = [110 : 45]$ is an ideal of $D_{-79}$. Corollary 5.1.6 implies that $A \sim C$, where $C = [19 : -46]$, specifically with $19A = (45 + z)C$. Notice that $C$ can also be written as $[19 : -8]$. Relabeling this ideal as $A_1$ and applying Corollary 5.1.6 again, we then find that $A_1 = [19 : -8] \sim [4 : 7] = [4 : -1] = C_1$, with $4A_1 = (-8 + z)C_1$. Combining these calculations, we have

$$4 \cdot 19A = 4 \cdot (45 + z)C = (45 + z) \cdot 4A_1 = (45 + z)(-8 + z)C_1.$$

This equation simplifies to $2A = (-10 + z)C_1$ (using the calculation that $z^2 = -20 + z$), which shows directly that $[110 : 45] \sim [4 : -1]$. ◊

**Exercise 5.1.6.** Let $D = D_{-79}$, as in the preceding example. For each ideal $A = [a : k]$ of $D$ below, use Corollary 5.1.6 to find an ideal $B = [b : \ell]$ with $b < 5$ that is equivalent to $A$. In each case, find a nonzero rational integer $m$ and an element $v$ of $D$ so that $mA = vB$.

(a) $A = [80 : 19]$.

(b) $A = [80 : -36]$.

(c) $A = [178 : 59]$.

(d) $A = [320 : -100]$.

(e) $A = [325 : 80]$.

(f) $A = [325 : -120]$.

(g) $A = [356 : 59]$.

(h) $A = [712 : 59]$.

These examples illustrate a reduction process for ideals similar to the one for ideal numbers in Theorem 2.4.3. We will use this process extensively in Chapter 6.

## 5.2 Quadratic Forms Associated to an Ideal

We saw in Theorem 5.1.5 that if $f = (a : k)$ and $f_1 = (a_1 : k_1)$ are equivalent quadratic forms of discriminant $\Delta$, then the corresponding ideals $A = [a : k]$ and $A_1 = [a_1 : k_1]$ are equivalent in the quadratic domain $D_\Delta$. Our main result for this section is the following theorem establishing a partial converse of Theorem 5.1.5.

**Theorem 5.2.1.** *Let $A = [a : k]$ and $A_1 = [a_1 : k_1]$ be primitive ideals of a quadratic domain $D$, with $a$ and $a_1$ positive. Suppose that $gA = vA_1$ for some $g \neq 0$ in $\mathbb{Z}$ and $v \neq 0$ in $D$, so that $A$ is equivalent to $A_1$. Then the following statements are true.*

(1) *If $N(v)$ is positive, then $(a : k)$ is equivalent to $(a_1 : k_1)$.*

(2) *If $N(v)$ is negative, then $(a : k)$ is equivalent to $(-a_1 : k_1)$.*

If $\Delta$ is negative, then $N(v) > 0$ for every nonzero element of $D = D_\Delta$. So in that case, an equivalence between ideals, $[a : k] \sim [a_1 : k_1]$ with $a$ and $a_1$ positive, establishes a corresponding equivalence of *positive definite* quadratic forms, $(a : k) \sim (a_1 : k_1)$. More caution is necessary when $\Delta$ is positive, as the following examples illustrate.

**Example.** Let $D = D_\Delta$ with $\Delta = \Delta(3,1) = 12$, so that $z = \sqrt{3}$ and $\phi(x) = x^2 - 3$, and consider the principal ideal $A = \langle 1 + z \rangle$. We find, using Theorem 3.2.2, that $A$ can be written as $[2 : 1]$. Since $A$ is principal, we know that $A \sim D = [1 : 0]$, specifically with $1 \cdot A = (1 + z)D$. Here $N(1 + z) = -2$, and so Theorem 5.2.1 implies that $(2 : 1) \sim (-1 : 0)$ in $\mathcal{Q}_{12}$, that is, $f(x,y) = 2x^2 + 2xy - y^2$ is equivalent to $f_1(x,y) = -x^2 + 3y^2$.

In this example, $f$ is not equivalent to $\phi = (1 : 0) = x^2 - 3y^2$. Notice that $f(0,1) = -1$. On the other hand, since $x^2 - 3y^2 \equiv x^2 + y^2 \pmod 4$ and a sum of two squares cannot be congruent to 3 modulo 4, we find that $\phi$ cannot represent $-1$. But equivalent forms must represent the same integers. ◊

**Example.** Consider the quadratic domain $D = D_8$, so that $z = \sqrt{2}$. If $A = D = [1 : 0]$, then we have $A \sim A$ with $1 \cdot A = 1 \cdot A$. Since $N(1) = 1 > 0$, it follows that $(1 : 0)$ is equivalent to $(1 : 0)$, as is obvious in any case. But note in this example that $1 + z$ is a unit in $D$, and so $D = \langle 1 + z \rangle$. Thus it is also true that $1 \cdot A = (1 + z)A$, and since $N(1 + z) = 1 - 2 = -1$, then $(1 : 0)$ is equivalent to $(-1 : 0)$ as well. ◊

**Ordered Bases for Ideals.** To lead to the proof of Theorem 5.2.1 at the end of this section, we define a correspondence between each $\mathbb{Z}$-basis for an ideal $A$ and some quadratic form. Recall that a set $S = \{u, v\}$ is a $\mathbb{Z}$-basis for an ideal $A$ of a quadratic domain $D$ if each element of $A$ can be written uniquely as $mu + nv$ for some rational integers $m$ and $n$. When we write $A = g[a : k]$, we are stating that $\{ga, gk + gz\}$ is a $\mathbb{Z}$-basis for $A$. We have the following connection between this $\mathbb{Z}$-basis and the quadratic form $f = (a : k)$.

**Proposition 5.2.2.** *Let $a$ be positive, and suppose that $A = g[a : k]$ is an ideal of the quadratic domain $D$ of discriminant $\Delta$. Let $u = ga$ and $v = gk + gz$, and let $w$ be an element of $A$, written as $w = mu + nv$. Then the norm of $w$ is $N(w) = N(A) \cdot f(m,n)$, where $f = (a : k)$ in $\mathcal{Q}_\Delta$. Furthermore, $\overline{u}v - u\overline{v} = N(A) \cdot \sqrt{\Delta}$.*

*Proof.* If $\phi(x)$ is the principal polynomial of discriminant $\Delta$, and $\phi(k) = ac$ and $\phi'(k) = b$, then $f(x,y) = ax^2 + bxy + cy^2$. When $w = mu + nv$, we have

$$N(w) = (mu + nv)(m\overline{u} + n\overline{v}) = (u\overline{u})m^2 + (u\overline{v} + \overline{u}v)mn + (v\overline{v})n^2. \qquad (5.2.1)$$

If $u = ga$, then $u\overline{u} = g^2a^2$, and since $z = \frac{\varepsilon + \sqrt{\Delta}}{2}$ and $\overline{z} = \frac{\varepsilon - \sqrt{\Delta}}{2}$, we find that

$$u\overline{v} + \overline{u}v = ga \cdot g(k + \overline{z}) + ga \cdot g(k + z) = g^2a(2k + \varepsilon) = g^2ab,$$

while

$$v\overline{v} = g(k + z) \cdot g(k + \overline{z}) = g^2\left(k^2 + \varepsilon k + \frac{\varepsilon^2 - \Delta}{4}\right) = g^2 \cdot \phi(k) = g^2ac.$$

Therefore,

$$\begin{aligned} N(w) &= g^2a^2m^2 + g^2abmn + g^2acn^2 \\ &= g^2a(am^2 + bmn + cn^2) = N(A) \cdot f(m,n), \end{aligned}$$

since $N(A) = g^2a$ if $a$ is positive. Finally,

$$\overline{u}v - u\overline{v} = ga \cdot g(k+z) - ga \cdot g(k+\overline{z}) = g^2a(z-\overline{z}) = N(A) \cdot \sqrt{\Delta},$$

as claimed. □

More generally, we can associate a quadratic form with each example of a $\mathbb{Z}$-basis of an ideal $A$. We begin with the following observation.

**Proposition 5.2.3.** *Let $A$ be an ideal of a quadratic domain $D$, and let $S = \{u, v\}$ be a $\mathbb{Z}$-basis for $A$. Then $T = \{u_1, v_1\}$ is also a $\mathbb{Z}$-basis for $A$ if and only if $u_1 = qu + rv$ and $v_1 = su + tv$ for some $q$, $r$, $s$, and $t$ in $\mathbb{Z}$ with $qt - rs = \pm 1$. In this case, $\overline{u_1}v_1 - u_1\overline{v_1} = (qt - rs)(\overline{u}v - u\overline{v})$.*

*Proof.* Since $S$ is a $\mathbb{Z}$-basis for $A$, we can write $u_1 = qu + rv$ and $v_1 = su + tv$ for some $q, r, s$, and $t$ in $\mathbb{Z}$, and thus any $\mathbb{Z}$-combination of $T$ is also a $\mathbb{Z}$-combination of $S$. We find that

$$tu_1 - rv_1 = (qt - rs)u \quad \text{and} \quad -su_1 + qv_1 = (qt - rs)v,$$

so if $qt - rs = \pm 1$, then any $\mathbb{Z}$-combination of $S$ is likewise a $\mathbb{Z}$-combination of $T$. It follows that $T$ is a $\mathbb{Z}$-basis for $A$ in that case.

Conversely, if $T$ is a $\mathbb{Z}$-basis for $A$, then we can write $u = q_1u_1 + r_1v_1$ and $v = s_1u_1 + t_1v_1$ for some $q_1, r_1, s_1$, and $t_1$ in $\mathbb{Z}$. In that case,

$$u = q_1(qu + rv) + r_1(su + tv) = (qq_1 + sr_1)u + (rq_1 + tr_1)v,$$

so that $qq_1 + sr_1 = 1$ and $rq_1 + tr_1 = 0$, and

$$v = s_1(qu + rv) + t_1(su + tv) = (qs_1 + st_1)u + (rs_1 + tt_1)v,$$

implying that $qs_1 + st_1 = 0$ and $rs_1 + tt_1 = 1$. But then

$$\begin{bmatrix} q & s \\ r & t \end{bmatrix} \cdot \begin{bmatrix} q_1 & s_1 \\ r_1 & t_1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

and since the determinant of each matrix is a rational integer, this implies that $qt - rs = \pm 1$.

Finally, we find that

$$\begin{aligned} \overline{u_1}v_1 - u_1\overline{v_1} &= (q\overline{u} + r\overline{v})(su + tv) - (qu + rv)(s\overline{u} + t\overline{v}) \\ &= (qsu\overline{u} + qt\overline{u}v + rsu\overline{v} + rtv\overline{v}) - (qsu\overline{u} + qtu\overline{v} + rs\overline{u}v + rtv\overline{v}) \\ &= qt(\overline{u}v - u\overline{v}) - rs(\overline{u}v - u\overline{v}) = (qt - rs)(\overline{u}v - u\overline{v}), \end{aligned}$$

as claimed. □

Combining Propositions 5.2.2 and 5.2.3, we have that if $\{u, v\}$ is a $\mathbb{Z}$-basis for an ideal $A$ of $D_\Delta$, then $\overline{u}v - u\overline{v} = \pm N(A) \cdot \sqrt{\Delta}$. In fact, we can assume that $\overline{u}v - u\overline{v} = N(A) \cdot \sqrt{\Delta}$ by interchanging $u$ and $v$ if necessary. We will say that $\{u, v\}$ is an *ordered basis* for $A$ if this equation holds. By Proposition 5.2.3, if $S = \{u, v\}$ is an ordered basis for $A$, then $S_1 = \{u_1, v_1\}$ is also an ordered basis for $A$ if and only if $u_1 = qu + rv$ and $v_1 = su + tv$ with $U = \begin{bmatrix} q & s \\ r & t \end{bmatrix}$ a *unimodular* matrix, that is, $qt - rs = 1$. Here $U$ is uniquely determined by the two ordered bases. We write $\{u_1, v_1\} = \{u, v\} \circ U$, or $S_1 = S \circ U$, to indicate that $S_1 = \{u_1, v_1\}$ is obtained from $S = \{u, v\}$ in this way.

**Example.** Let $\Delta = -4$ so that $D = \mathbb{Z}[i]$ and $\phi(x) = x^2 + 1$. Here $A = [10 : 3]$ is an ideal of $D$ since $\phi(3) = 10 \cdot 1$, and we have that $\{10, 3 + i\}$ is an ordered basis for $A$. (We can confirm that $\overline{10} \cdot (3 + i) - 10 \cdot (\overline{3 + i}) = 10(3 + i) - 10(3 - i) = 20i = 10 \cdot \sqrt{-4} = N(A) \cdot \sqrt{\Delta}$.) Using the unimodular matrix $U = \begin{bmatrix} 3 & 7 \\ 2 & 5 \end{bmatrix}$, we find that $\{10, 3 + i\} \circ U = \{36 + 2i, 85 + 5i\}$ is also an ordered basis for $A$. ◊

**Exercise 5.2.1.** Verify that $A = [8 : 3]$ is an ideal of the quadratic domain $D = D_{-111}$, so that $S = \{8, 3 + z\}$ is an ordered basis for $A$. For each unimodular matrix $U$ below, find the ordered basis $S_1 = S \circ U$ for $A$.

(a) $U = \begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix}$.

(b) $U = \begin{bmatrix} 4 & -1 \\ 5 & -1 \end{bmatrix}$.

(c) $U = \begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix}$.

**Theorem 5.2.4.** *Let $S = \{u, v\}$ be an ordered basis for $A$, an ideal of the quadratic domain $D = D_\Delta$. Let*

$$a = \frac{u\overline{u}}{N(A)}, \qquad b = \frac{u\overline{v} + \overline{u}v}{N(A)}, \qquad \text{and} \qquad c = \frac{v\overline{v}}{N(A)}. \tag{5.2.2}$$

*Then $a$, $b$, and $c$ are rational integers for which $b^2 - 4ac = \Delta$, so that*

$$f_S(x, y) = ax^2 + bxy + cy^2 \tag{5.2.3}$$

*is an element of $\mathcal{Q}_\Delta$. For all $w = mu + nv$ in $A$, we have that*

$$N(w) = N(A) \cdot f_S(m, n). \tag{5.2.4}$$

**Definition.** If $A$ is a nontrivial ideal of a quadratic domain $D_\Delta$, and $S = \{u, v\}$ is an ordered basis for $A$, we refer to $f_S$ given by equation (5.2.3) as the *quadratic form of $S$*.

*Proof.* Assume first that $A$ is primitive, so that $N(A)$ is the smallest positive rational integer in $A$. Since $u$ and $v$ are elements of $A$, then $u\overline{u}$, $u\overline{v} + \overline{u}v$, and $v\overline{v}$ are also elements of $A$, by the closure properties of an ideal. But each of these elements is equal to its own conjugate in $D$, so is also a rational integer. Thus each is divisible by $N(A)$, implying that $a$, $b$, and $c$ are rational integers. More generally, if $A = gA_1$ for some $g > 1$ in $\mathbb{Z}$, then $u = gu_1$ and $v = gv_1$ for some $u_1$ and $v_1$ in $A_1$. Since $u\overline{u} = g^2 u_1\overline{u_1}$, and similarly for the other elements, we draw the same conclusion about $a$, $b$, and $c$. Now

$$b^2 - 4ac = \frac{1}{(N(A))^2}\left[(u\overline{v} + \overline{u}v)^2 - 4u\overline{u}\cdot v\overline{v}\right] = \frac{1}{(N(A))^2}(\overline{u}v - u\overline{v})^2 = \Delta,$$

since $\{u, v\}$ is an ordered basis for $A$. Finally,

$$\begin{aligned} N(w) &= (mu + nv)(m\overline{u} + n\overline{v}) \\ &= (u\overline{u})m^2 + (u\overline{v} + \overline{u}v)mn + (v\overline{v})n^2 = N(A)(am^2 + bmn + cn^2), \end{aligned}$$

that is, $N(w) = N(A)\cdot f_S(m, n)$. □

**Example.** In the preceding example, we saw that $S = \{36 + 2i, 85 + 5i\}$ is an ordered basis for the ideal $A = [10 : 3]$ of $D = \mathbb{Z}[i]$. If $u = 36+2i$ and $v = 85+5i$, we find that

$$u\overline{u} = 36^2 + 2^2 = 1300, \qquad v\overline{v} = 85^2 + 5^2 = 7250,$$

and

$$u\overline{v} + \overline{u}v = 2(36\cdot 85 - 2\cdot 5\cdot i^2) = 6140.$$

Since $N(A) = 10$, then $f_S(x, y) = 130x^2 + 614xy + 725y^2$. One can verify that the discriminant of $f_S$ is $\Delta = -4$. ◊

**Exercise 5.2.2.** For the ordered basis $S$ in Exercise 5.2.1, find the corresponding quadratic form $f_S$ of $\mathcal{Q}_{-111}$. Do the same for each of the ordered bases obtained in parts (a), (b), and (c) of Exercise 5.2.1.

**Theorem 5.2.5.** *Let $A$ be an ideal of the quadratic domain $D = D_\Delta$, and let $S = \{u, v\}$ and $S_1 = \{u_1, v_1\}$ be ordered bases for $A$, so that $S_1 = S \circ U$ for some unimodular matrix $U$. If $f = f_S$ and $f_1 = f_{S_1}$ are the quadratic forms of these ordered bases, then $f_1 = f \circ U$.*

*Proof.* Let $f(x, y) = ax^2 + bxy + cy^2$, where $a$, $b$, and $c$ are defined for the ordered basis $S = \{u, v\}$ as in equation (5.2.2). Let $U = \begin{bmatrix} q & s \\ r & t \end{bmatrix}$ be the unimodular matrix for which $u_1 = qu + rv$ and $v_1 = su + tv$. We find that

$$u_1\overline{u_1} = q^2 u\overline{u} + qr(u\overline{v} + \overline{u}v) + r^2 v\overline{v} = N(A)(aq^2 + bqr + cr^2),$$

$$u_1\overline{v_1} + \overline{u_1}v_1 = 2qs(u\overline{u}) + (qt + rs)(u\overline{v} + \overline{u}v) + 2rt(v\overline{v})$$
$$= N(A)(2aqs + b(qt + rs) + 2crt),$$

and

$$v_1\overline{v_1} = s^2u\overline{u} + st(u\overline{v} + \overline{u}v) + t^2v\overline{v} = N(A)(as^2 + bst + ct^2).$$

So then

$$f_1(x, y) = (aq^2 + bqr + cr^2)x^2 + (2aqs + b(qt + rs) + 2crt)xy + (as^2 + bst + ct^2)y^2,$$

that is, $f_1 = f \circ U$ by equation (4.2.1). □

We now prove Theorem 5.2.1, using the following fact.

**Exercise 5.2.3.** Show that if $S = \{u, v\}$ is a $\mathbb{Z}$-basis for an ideal $A$ of some quadratic domain $D$, then $T = \{wu, wv\}$ is a $\mathbb{Z}$-basis for the ideal $wA$ of $D$.

*Proof of Theorem* 5.2.1. We know that $S = \{ga, gk + gz\}$ is an ordered basis for $gA$, with $f_S = (a : k)$ the quadratic form of $S$. However, $\{va_1, v(k_1 + z)\}$ is a $\mathbb{Z}$-basis for $vA_1$, as in Exercise 5.2.3, but is not necessarily an ordered basis. Note that $N(vA_1) = N(\langle v\rangle A_1) = N(\langle v\rangle) \cdot N(A_1)$ by Theorem 3.6.6, since a principal ideal has index 1. It follows that $N(vA_1) = N(v) \cdot N(A_1)$ if $N(v)$ is positive, while $N(vA_1) = -N(v) \cdot N(A_1)$ if $N(v)$ is negative.

Suppose first that $N(v)$ is positive, so that $N(vA_1) = N(v) \cdot N(A_1)$. In that case, $S_1 = \{va_1, v(k_1 + z)\}$ is an ordered basis for $vA_1$, since

$$\overline{va_1} \cdot v(k_1 + z) - va_1 \cdot \overline{v(k_1 + z)} = N(v) \cdot a_1(z - \overline{z}) = N(vA_1)\sqrt{\Delta}.$$

We then can show that $f_{S_1} = (a_1 : k_1)$, using the equations of (5.2.2) in Theorem 5.2.4. Specifically,

$$va_1 \cdot \overline{va_1} = v\overline{v}a_1^2 = N(vA_1)a_1,$$

$$va_1 \cdot \overline{v(k_1 + z)} + \overline{va_1} \cdot v(k_1 + z) = N(vA_1)((k_1 + \overline{z}) + (k_1 + z))$$
$$= N(vA_1)b_1,$$

and

$$v(k_1 + z) \cdot \overline{v(k_1 + z)} = v\overline{v} \cdot (k_1 + z)(k_1 + \overline{z}) = N(vA_1)c_1,$$

where $a_1c_1 = \phi(k_1)$ and $b_1 = \phi'(k_1)$. But now since $S$ and $S_1$ are ordered bases for the same ideal, $gA = vA_1$, there is a unimodular matrix $U$ so that $f_S \circ U = f_{S_1}$, by Theorem 5.2.5. Thus $(a : k) \sim (a_1 : k_1)$.

Now suppose that $N(v)$ is negative, so that $N(vA_1) = -N(v) \cdot N(A_1)$. Here we find that $S_1 = \{va_1, -v(k_1 + z)\}$ is an ordered basis for $vA_1$, since

$$\overline{va_1} \cdot -v(k_1 + z) - va_1 \cdot \overline{-v(k_1 + z)} = -N(v) \cdot a_1(z - \overline{z}) = N(vA_1)\sqrt{\Delta}.$$

In this case, the equations of (5.2.2) show that $f_{S_1} = (-a_1 : k_1)$. Specifically,

$$va_1 \cdot \overline{va_1} = N(v)a_1^2 = -N(v) \cdot N(A_1)(-a_1) = N(vA_1)(-a_1),$$

$$\begin{aligned} \upsilon a_1 \cdot \overline{-\upsilon(k_1+z)} + \overline{\upsilon a_1} \cdot -\upsilon(k_1+z) &= -N(\upsilon)\cdot N(A_1)((k_1+\overline{z})+(k_1+z)) \\ &= N(\upsilon A_1)b_1, \end{aligned}$$

and

$$-\upsilon(k_1+z)\cdot\overline{-\upsilon(k_1+z)} = N(\upsilon)\cdot(k_1+z)(k_1+\overline{z}) = N(\upsilon A_1)(-c_1),$$

where $a_1c_1 = (-a_1)(-c_1) = \phi(k_1)$ and $b_1 = \phi'(k_1)$. Again, $S$ and $S_1$ are ordered bases for the same ideal, and so $(a : k) \sim (-a_1 : k_1)$ in this case. □

## 5.3 Composition of Binary Quadratic Forms

In this section, we introduce another important connection between quadratic forms and ideals. We begin with the following claim, stated purely in terms of quadratic forms. If $f_1$ and $f_2$ are primitive quadratic forms of the same discriminant $\Delta$, then there is a form $f$ in $\mathcal{Q}_\Delta$ with the following property:

If $f_1$ represents $m$ and $f_2$ represents $n$, then $f$ represents $mn$.

We will give a formula for such a form $f$ in terms of $f_1$ and $f_2$, and thus define an operation of *composition* on primitive quadratic forms of discriminant $\Delta$. The concept of composition was present in the early development of quadratic forms, particularly in the work of Lagrange, but was made complete and precise by Gauss in *Disquisitiones Arithmeticae* (1801). Here we will demonstrate that composition of quadratic forms is consistent with multiplication of ideals. (The development of ideals was, as we have seen, a later innovation of Kummer and Dedekind.) We begin with some examples and general statements that illustrate a method of composition in practice, and suggest a connection with ideal multiplication.

**Example.** In considering sums of two squares in §1.1, we often used the following equation:

$$(q^2+r^2)(s^2+t^2) = (qs-rt)^2 + (qt+rs)^2.$$

While we established this fact first by direct calculation, it can be better explained using the multiplicative property of norms of Gaussian integers:

$$\begin{aligned} (q^2+r^2)(s^2+t^2) = N(q+ri)\cdot N(s+ti) &= N((q+ri)(s+ti)) \\ &= N((qs-rt)+(qt+rs)i) = (qs-rt)^2+(qt+rs)^2. \end{aligned}$$

If $f(x,y) = x^2+y^2$, this equation implies that if $f$ represents $m$ and $f$ represents $n$, then $f$ represents $mn$. We might interpret this as saying that the composition of $f$ with itself is equal to $f$. Note that in $\mathcal{Q}_{-4}$, we can write $f = (1 : 0)$, with the corresponding ideal given by $A_f = [1 : 0]$. It is the case that $[1 : 0]\cdot[1 : 0] = [1 : 0]$. ◊

We can generalize this example with the following proposition, making a similar claim about the principal form of any discriminant.

**Proposition 5.3.1.** *Let $\phi(x,y) = x^2 + \varepsilon xy + \frac{\varepsilon^2-\Delta}{4}y^2$ be the principal form of some discriminant $\Delta$. Suppose that $\phi(q,r) = m$ and $\phi(s,t) = n$ for some integers $q$, $r$, $s$, and $t$. Then $\phi(u,v) = mn$, where*

$$u = qs - \frac{\varepsilon^2-\Delta}{4}rt \qquad \text{and} \qquad v = qt + rs + \varepsilon rt. \tag{5.3.1}$$

*Proof.* Let $z = z_\Delta$ in the quadratic domain $D = D_\Delta$. By equation (2.2.5), we have that $\phi(q,r) = N(q+rz)$ for every pair of integers $q$ and $r$. Using the multiplicative property of the norm, and the multiplication formula of equation (2.2.8), we then have that

$$mn = \phi(q,r)\cdot\phi(s,t) = N((q+rz)(s+tz)) = N(u+vz) = \phi(u,v),$$

where $u$ and $v$ are given as in equation (5.3.1). □

**Example.** Let $\Delta = -3$ so that $\varepsilon = 1$ and $\phi(x,y) = x^2+xy+y^2$. Proposition 5.3.1 implies that

$$(q^2+qr+r^2)(s^2+st+t^2) = (qs-rt)^2 + (qs-rt)(qt+rs+rt) + (qt+rs+rt)^2,$$

which can be verified by direct calculation. ◊

We now consider a discriminant for which there are distinct classes of quadratic forms.

**Example.** Let $\Delta = -20$, so that $z = \sqrt{-5}$ in the quadratic domain $D = D_\Delta$. Let

$$f = (1:0) = x^2 + 5y^2 \qquad \text{and} \qquad g = (2:1) = 2x^2 + 2xy + 3y^2,$$

quadratic forms of discriminant $\Delta = -20$. Here we find that $f$ and $g$ have different genus symbols,

$$\left(\frac{-1}{f}\right) = 1 = \left(\frac{f}{5}\right) \quad \text{while} \quad \left(\frac{-1}{g}\right) = -1 = \left(\frac{g}{5}\right),$$

so cannot be equivalent to each other. Since $f$ is the principal form of discriminant $-20$, we have that $f(q,r) = N(q+rz)$ for all integers $q$ and $r$. Proposition 5.3.1 implies that if $f(q,r) = m$ and $f(s,t) = n$, then $f(u,v) = mn$, where $u = qs - 5rt$ and $v = qt + rs$.

We will describe similar products of representations by $g$. First we observe the following equation relating a representation by $g$ to the norm of an element of $D$:

$$\begin{aligned} 2g(q,r) = 4q^2 + 4qr + 6r^2 &= (4q^2+4qr+r^2) + 5r^2 \\ &= (2q+r)^2 + 5r^2 = N((2q+r)+rz). \end{aligned} \tag{5.3.2}$$

Notice that $w = (2q + r) + rz = q(2) + r(1 + z)$ is a typical $\mathbb{Z}$-combination of $\{2, 1 + z\}$, an ordered basis of the ideal $A_g = [2 : 1]$. Equation (5.3.2) states that $N(w) = N(A_g) \cdot g(q, r)$, as in equation (5.2.4) of Theorem 5.2.4.

Suppose that $f(q, r) = m$ and $g(s, t) = n$ for some integers $q$, $r$, $s$, and $t$. We will show that $mn$ is represented by $g$. (This outcome is suggested by the fact that $A_f \cdot A_g = [1 : 0] \cdot [2 : 1] = [2 : 1] = A_g$.) Notice that

$$\begin{aligned} 2mn &= f(q, r) \cdot 2g(s, t) = N(q + rz) \cdot N((2s + t) + tz) \\ &= N((q + rz)((2s + t) + tz)) = N((2qs + qt - 5rt) + (qt + 2rs + rt)z), \end{aligned}$$

since $z^2 = -5$. This equals $2g(u, v)$ if

$$2u + v = 2qs + qt - 5rt \quad \text{and} \quad v = qt + 2rs + rt,$$

by equation (5.3.2). Thus if $f(q, r) = m$ and $g(s, t) = n$, then $g(u, v) = mn$, where

$$u = qs - rs - 3rt \qquad \text{and} \qquad v = qt + 2rs + rt.$$

Now suppose that $g(q, r) = m$ and $g(s, t) = n$ for some integers $q$, $r$, $s$, and $t$. Note that $A_g \cdot A_g = [2 : 1] \cdot [2 : 1] = 2[1 : 0]$, since $A_g$ is its own conjugate. With $2[1 : 0]$ equivalent to $A_f = [1 : 0]$, we may conjecture that $mn$ is represented by $f$. We can show as follows that this is the case. Here

$$\begin{aligned} 4mn = 2g(q, r) \cdot 2g(s, t) &= N(((2q + r) + rz)((2s + t) + tz)) \\ &= N((4qs + 2qt + 2rs + rt) + (2qt + rt + 2rs + rt)z + rtz^2) \\ &= N((4qs + 2qt + 2rs - 4rt) + (2qt + 2rs + 2rt)z). \end{aligned}$$

Since $N(2u + 2vz) = 4N(u + vz) = 4f(u, v)$, we conclude that $f(u, v) = mn$, where $u = 2qs + qt + rs - 2rt$ and $v = qt + rs + rt$. ◊

**Exercise 5.3.1.** Let $f(x, y) = x^2 + 5y^2$ and $g(x, y) = 2x^2 + 2xy + 3y^2$. Verify that

$$f(2, 1) = 9, \quad f(3, 1) = 14, \quad g(1, 1) = 7, \quad \text{and} \quad g(2, 1) = 15.$$

Use these facts to help find solutions of the following equations.

(a) $f(x, y) = 126 = 9 \cdot 14$.

(b) $f(x, y) = 105 = 7 \cdot 15$.

(c) $g(x, y) = 63 = 9 \cdot 7$.

(d) $g(x, y) = 98 = 14 \cdot 7$.

(e) $g(x, y) = 135 = 9 \cdot 15$.

(f) $g(x, y) = 210 = 14 \cdot 15$.

**Formula for Composition.** We can generalize the outcome of these examples in the following definition of composition.

**Definition.** Let $f_1 = (a_1 : k_1)$ and $f_2 = (a_2 : k_2)$ be primitive quadratic forms and $\phi(x)$ the principal polynomial of some discriminant $\Delta$. Let $a_3 = k_1 + k_2 + \phi'(0)$ and let $g = \gcd(a_1, a_2, a_3)$. Then we define $f_1 \cdot f_2$ to be the quadratic form $f = (a : k)$, where $a = a_1 a_2 / g^2$ and $k$ satisfies the congruences

$$k \equiv k_1 \pmod{a_1/g}, \qquad k \equiv k_2 \pmod{a_2/g},$$

and

$$a_3 k \equiv k_1 k_2 - \phi(0) \pmod{ag}.$$

(We select $k$ so that $-a < \phi'(k) \leq a$.) We refer to this operation as *composition* of $f_1$ and $f_2$, and we call $f$ the *composite* of $f_1$ and $f_2$.

Note that we do not require $a_1$ or $a_2$ to be positive in this formula. In the congruence statements, we replace each modulus by its absolute value if necessary. We will show that $f = f_1 \cdot f_2$ has the property by which we described composition at the beginning of this section. We begin with the following lemma.

**Lemma 5.3.2.** *Let $D$ be the quadratic domain and $\phi(x)$ the principal polynomial of some discriminant $\Delta$. Let $a$ be a positive integer and let $k$ be an integer so that $a$ divides $\phi(k)$. Let $f = ((-1)^e a : k)$ for some integer $e$. Then for all integers $q$ and $r$,*

$$N(q(-1)^e a + r(k + z)) = (-1)^e a f(q, r), \tag{5.3.3}$$

*where $z = z_\Delta$ and $N$ denotes the norm of an element of $D$.*

*Proof.* Let $w = k + z$, and let $\phi(k) = ac = w\overline{w}$ and $\phi'(k) = b = w + \overline{w}$. If $e$ is even, then $f = (a : k) = ax^2 + bxy + cy^2$, and we find that

$$\begin{aligned} N(qa + rw) &= (qa + rw)(qa + r\overline{w}) \\ &= a^2q^2 + aqr(w + \overline{w}) + r^2(w\overline{w}) = a(aq^2 + bqr + cr^2). \end{aligned}$$

If $e$ is odd, then $f = (-a : k) = -ax^2 + bxy - cy^2$ (since $\phi(k) = -a \cdot -c$), and

$$\begin{aligned} N(-qa + rw) &= (-qa + rw)(-qa + r\overline{w}) \\ &= a^2q^2 - aqr(w + \overline{w}) + r^2(w\overline{w}) = -a(-aq^2 + bqr - cr^2). \end{aligned}$$

Both equations are in the form of (5.3.3). □

We can rephrase Lemma 5.3.2 as saying that if $f = (a : k)$, then

$$N(qa + r(k + z)) = af(q, r)$$

whether $a$ is positive or negative.

**Theorem 5.3.3.** *Let $f_1$ and $f_2$ be primitive quadratic forms of discriminant $\Delta$, and let $f = f_1 \cdot f_2$. If $f_1(q,r) = m$ and $f_2(s,t) = n$ for some integers $q$, $r$, $s$, and $t$, then there are integers $u$ and $v$ so that $f(u,v) = mn$. Specifically, let $f_1 = (a_1 \,:\, k_1)$ and $f_2 = (a_2 \,:\, k_2)$, let $\phi(x)$ be the principal polynomial of discriminant $\Delta$, with $a_3 = k_1 + k_2 + \phi'(0)$ and $g = \gcd(a_1, a_2, a_3)$, and let $f = (a \,:\, k)$ as in the definition of composition. Then $u$ and $v$ satisfy the equations*

$$gv = a_1qt + a_2rs + a_3rt$$

*and*

$$(ga)u = (a_1a_2)qs - a_1(k - k_2)qt - a_2(k - k_1)rs + (k_1k_2 - \phi(0) - a_3k)rt.$$

*Proof.* Let $A_1 = [a_1 \,:\, k_1]$ and $A_2 = [a_2 \,:\, k_2]$ be the ideals of $f_1$ and $f_2$, respectively, and let $A = A_1 \cdot A_2$. The assumption that $f_1$ and $f_2$ are primitive quadratic forms ensures that $A_1$ and $A_2$ have index 1, so the ideal multiplication formula of Theorem 3.6.1 implies that $A = g[a \,:\, k]$, where $g$ and $f = (a \,:\, k)$ are as given in the definition of $f = f_1 \cdot f_2$. Let $w = k + z$, $w_1 = k_1 + z$, and $w_2 = k_2 + z$. We have that

$$N(qa_1 + rw_1) = a_1 \cdot f_1(q,r) = a_1m$$

and

$$N(sa_2 + tw_2) = a_2 \cdot f_2(s,t) = a_2n$$

by Lemma 5.3.2, and so

$$a_1a_2mn = N(qa_1 + rw_1) \cdot N(sa_2 + tw_2) = N((qa_1 + rw_1)(sa_2 + tw_2)). \quad (5.3.4)$$

Now the product $(qa_1 + rw_1)(sa_2 + tw_2)$ is an element of $A_1A_2 = A$ so can be written as $u(ga) + v(gw)$ for some integers $u$ and $v$. But then

$$N(u(ga) + v(gw)) = g^2N(ua + vw) = g^2a \cdot f(u,v), \quad (5.3.5)$$

again by Lemma 5.3.2. Since $g^2a = a_1a_2$ by the definition of composition, combining equations (5.3.4) and (5.3.5) yields the conclusion that $f(u,v) = mn$.

The formulas for $v$ and $u$ in Theorem 5.3.3 are obtained by expanding the product

$$(qa_1 + rw_1)(sa_2 + tw_2) = ((qa_1 + rk_1) + rz)((sa_2 + tk_2) + tz) \quad (5.3.6)$$

and setting that expression equal to

$$u(ga) + v(gw) = ((ga)u + (gk)v) + (gv)z. \quad (5.3.7)$$

Applying the multiplication formula of equation (2.2.8) to (5.3.6) and comparing coefficients of $z$ produces the equation for $gv$. Comparing the coefficients of 1, we find

$$(ga)u + k(gv) = (qa_1 + rk_1)(sa_2 + tk_2) - rt \cdot \phi(0).$$

Using the formula for $gv$ and the definition of $\phi(x)$ produces the equation for $(ga)u$. We omit the details. □

**Example.** Let $\Delta = 21$, so that $\phi(x) = x^2 + x - 5$. Let

$$f_1 = (-3 : 1) = -3x^2 + 3xy + y^2 \quad \text{and} \quad f_2 = (5 : 4) = 5x^2 + 9xy + 3y^2.$$

Here $a_1 = -3$, $a_2 = 5$, and $a_3 = k_1 + k_2 + \phi'(0) = 6$, so that $g = \gcd(-3, 5, 6) = 1$. The composition formula implies that

$$f = f_1 \cdot f_2 = (-15 : 4) = -15x^2 + 9xy - y^2.$$

If $f_1(q, r) = m$ and $f_2(s, t) = n$, then $f(u, v) = mn$, where

$$v = a_1qt + a_2rs + a_3rt = -3qt + 5rs + 6rt$$

and

$$-15u = (a_1a_2)qs - a_1(k - k_2)qt - a_2(k - k_1)rs + (k_1k_2 - \phi(0) - a_3k)rt$$

so that

$$u = -\frac{1}{15}(-15qs + 0qt - 15rs + (4 + 5 - 24)rt) = qs + rs + rt.$$

For example, $f_1(1, 5) = 37$ and $f_2(2, 1) = 41$, so if

$$u = 1(2) + 5(2) + 5(1) = 17 \quad \text{and} \quad v = -3(1)(1) + 5(5)(2) + 6(5)(1) = 77,$$

we find that $f(17, 77) = 1517 = 37 \cdot 41$. ◊

**Example.** Let $\Delta = -84$, so that $\phi(x) = x^2 + 21$. Let

$$f_1 = (2 : 1) = 2x^2 + 2xy + 11y^2 \quad \text{and} \quad f_2 = (3 : 0) = 3x^2 + 7y^2,$$

and then

$$f = f_1 \cdot f_2 = (6 : 3) = 6x^2 + 6xy + 5y^2.$$

If $f_1(q, r) = m$ and $f_2(s, t) = n$, we find that $f(u, v) = mn$ if

$$v = a_1qt + a_2rs + a_3rt = 2qt + 3rs + rt$$

(here $a_3 = k_1 + k_2 + \phi'(0) = 1$) and

$$6u = (a_1a_2)qs - a_1(k - k_2)qt - a_2(k - k_1)rs + (k_1k_2 - \phi(0) - a_3k)rt$$

so that

$$u = \frac{1}{6}(6qs - 6qt - 6rs + (0 - 21 - 3)rt) = qs - qt - rs - 4rt.$$

For example, since $f_1(3, -1) = 23$ and $f_2(2, 1) = 19$, we find that $f(9, -1) = 437 = 23 \cdot 19$. ◊

**Exercise 5.3.2.** In each part, use Theorem 5.3.3 to find a composite form $f$ for the given quadratic forms $f_1$ and $f_2$ in $\mathcal{Q}_\Delta$, and find $u$ and $v$, in terms of $q$, $r$, $s$, and $t$, for which $f_1(q, r) \cdot f_2(s, t) = f(u, v)$.

(a) $f_1(x, y) = x^2 + 2y^2 = f_2(x, y)$ in $\mathcal{Q}_{-8}$.

(b) $f_1(x, y) = 2x^2 + 3y^2 = f_2(x, y)$ in $\mathcal{Q}_{-24}$.

(c) $f_1(x,y) = 2x^2 + xy + 3y^2 = f_2(x,y)$ in $\mathcal{Q}_{-23}$.

(d) $f_1(x,y) = 2x^2 + xy + 3y^2$ and $f_2(x,y) = 2x^2 - xy + 3y^2$ in $\mathcal{Q}_{-23}$.

(e) $f_1(x,y) = 2x^2 + xy + 6y^2 = f_2(x,y)$ in $\mathcal{Q}_{-47}$.

(f) $f_1(x,y) = 2x^2 + xy + 6y^2$ and $f_2(x,y) = 3x^2 + xy + 4y^2$ in $\mathcal{Q}_{-47}$.

(g) $f_1(x,y) = x^2 - 2y^2 = f_2(x,y)$ in $\mathcal{Q}_8$.

(h) $f_1(x,y) = x^2 - 10y^2 = f_2(x,y)$ in $\mathcal{Q}_{40}$.

(i) $f_1(x,y) = 2x^2 - 5y^2 = f_2(x,y)$ in $\mathcal{Q}_{40}$.

(j) $f_1(x,y) = x^2 - 10y^2$ and $f_2(x,y) = 2x^2 - 5y^2$ in $\mathcal{Q}_{40}$.

## 5.4 Class Groups of Ideals and Quadratic Forms

Throughout this chapter, we have made connections between quadratic forms of discriminant $\Delta$ and ideals of the quadratic domain $D_\Delta$. We have seen in particular that the relation of equivalence of quadratic forms carries over to a similar relation on ideals. In §5.3, we found that ideal multiplication induces an operation of composition on primitive quadratic forms. To conclude Chapter 5, we combine these concepts with a multiplication operation defined on classes under equivalence, first for ideals and then for quadratic forms. We first note a connection between principal ideals of a quadratic domain and unique irreducible factorization as follows.

**Principal Ideals.** Recall that a quadratic domain $D$ is called a *principal ideal domain* if every ideal of $D$ is a principal ideal. Corollary 3.6.4 states that every principal ideal of a quadratic domain $D$ has index 1. So if $D$ is not a *complete* quadratic domain, then $D$ cannot be a principal ideal domain.

**Theorem 5.4.1.** *Let $D$ be a quadratic domain. Then $D$ is a principal ideal domain if and only if $D$ is a unique factorization domain.*

In more general examples of integral domains, it is always the case that a principal ideal domain is a unique factorization domain. We will outline the proof of this claim in the following exercises. The converse of this statement is not always true in an arbitrary integral domain. We will prove that it is the case for quadratic domains, however, using properties that we have established in that setting.

**Exercise 5.4.1.** Let $D$ be a quadratic domain. Recall that an element $u$ of $D$ that is neither zero nor a unit is called *irreducible* if when $u = vw$, then either $v$ or

$w$ is a unit in $D$. Show that if $u$ is irreducible in $D$, and $\langle u\rangle \subseteq \langle v\rangle$ for some $v$ in $D$, then either $\langle v\rangle = \langle u\rangle$ or $\langle v\rangle = D$. (We may say that $\langle u\rangle$ is *maximal among principal ideals* in this case.)

**Exercise 5.4.2.** Let $D$ be a quadratic domain, and suppose that $D$ is a principal ideal domain. Use Exercise 5.4.1 to show that if $u$ is an irreducible element of $D$, then $\langle u\rangle$ is a prime ideal of $D$.

**Exercise 5.4.3.** Let $D$ be a quadratic domain. Recall that an element $u$ of $D$ that is neither zero nor a unit is called *prime* if when $u$ divides $vw$ in $D$, then $u$ divides $v$ or $u$ divides $w$. Show that if $\langle u\rangle$ is a prime ideal of $D$, then $u$ is prime as an element of $D$. (Hint: Use the characterization of prime ideals in Proposition 3.3.2.)

**Exercise 5.4.4.** Let $D$ be a quadratic domain. Show that if $D$ is a principal ideal domain, then $D$ is a unique factorization domain. (Hint: Use the fact noted in §2.5 that a quadratic domain $D$ is a unique factorization domain if and only if every irreducible element of $D$ is also prime.)

*Proof of Theorem* 5.4.1. Let $D$ be a quadratic domain. We will show that if $D$ is *not* a principal ideal domain, then $D$ must contain an irreducible element that is not prime, so is not a unique factorization domain. (This indirectly proves the converse of the claim in Exercise 5.4.4, and thus completes the proof of Theorem 5.4.1.)

First note as follows that if not every ideal of $D$ is principal, then $D$ contains a *prime* ideal that is not principal. If $D$ is a complete quadratic domain, then every ideal of $D$ other than $\{0\} = \langle 0\rangle$ and $D = \langle 1\rangle$ can be written as a product of prime ideals. If all prime ideals were principal, then all such products would also be principal. On the other hand, suppose that $D = D_\Delta$ is not a complete quadratic domain, so that $\Delta = \Delta(d, \gamma)$ with $\gamma > 1$, and let $p$ be a prime number dividing $\gamma$. In that case, $P = [p : 0]$ is a prime ideal of $D$ that is not a principal ideal, since we find that $\gamma(P) = p$.

Let $P$ be a prime ideal of $D$ with $P \neq \langle u\rangle$ for all $u$ in $D$. We know that there is a rational prime $p$ contained in $P$, and in this case, $N(P) = p$. (The only other possibility is $N(P) = p^2$, but that occurs only when $P = \langle p\rangle$, which is principal.) We claim that $p$ is an irreducible element in $D$. Otherwise, $p = vw$ for some $v$ and $w$ in $D$ with neither $v$ nor $w$ a unit in $D$. Then $N(p) = p^2 = N(v)N(w)$, which implies that $N(v) = \pm p = N(w)$. On the other hand, since $vw = p$ is in the prime ideal $P$, then either $v$ or $w$ is in $P$. We can assume that $v$ is in $P$ without loss of generality. But now notice that $\langle v\rangle \subseteq P$ and that $N(\langle v\rangle) = |N(v)| = p = N(P)$, from which we conclude that $P = \langle v\rangle$. This is impossible since $P$ is not a principal ideal.

On the other hand, we can show that $p$ is not prime as an element of $D$. Let $v$ be an element of $P$ that is not divisible by $p$. (Such an element must exist since

otherwise $P = \langle p \rangle$.) In that case, $\overline{v}$ is an element of $D$ that is also not divisible by $p$, but then $v\overline{v} = N(v)$ is a rational integer in the ideal $P$. We know that every rational integer in $P$ is divisible by $p$, so we have that $p$ divides $v\overline{v}$, but does not divide either $v$ or $\overline{v}$. Thus $p$ is not prime in $D$, but is irreducible in $D$, and so we conclude that $D$ is not a unique factorization domain. □

**The Ideal Class Group.** In §3.5, we noted that principal ideals of a quadratic domain $D$ might be identified with elements of $D$, while ideals that are not principal play the part of "ideal numbers" that, while not elements of $D$, produce a form of unique irreducible factorization of elements of $D$. We now introduce a definition that we might interpret as determining how many (classes of) such ideal numbers are needed to produce unique factorization.

Let $D = D_\Delta$ be a quadratic domain and consider the collection of all classes of nontrivial ideals of $D$ under the relation of equivalence defined in §5.1. We denote the class of an ideal $A$ as $[A]$. Proposition 5.1.3 implies that we can define the *index* of $[A]$ to be the same as $\gamma(A)$. (That is, this characteristic of an ideal class is well-defined, since if $A$ is equivalent to $B$, then $\gamma(A) = \gamma(B)$.) We write $\mathcal{C}_\Delta$ for the collection of ideal classes of $D_\Delta$ of index 1.

**Proposition 5.4.2.** *Let $D$ be the quadratic domain of discriminant $\Delta$, and let $\mathcal{C}_\Delta$ be the set of all equivalence classes, under the $\sim$ relation, of ideals $A$ for which $\gamma(A) = 1$. Then there is a well-defined operation of multiplication on $\mathcal{C}_\Delta$ given by $[A]\cdot[B] = [AB]$. This operation has the following properties.*

(1) *Multiplication is commutative:* $[A] \cdot [B] = [B] \cdot [A]$ *for all* $[A], [B] \in \mathcal{C}_\Delta$.

(2) *Multiplication is associative:* $([A]\cdot[B])\cdot[C] = [A]\cdot([B]\cdot[C])$ *for all* $[A], [B], [C] \in \mathcal{C}_\Delta$.

(3) *The class of $D$, as an ideal of itself, is an identity element for multiplication:* $[A] \cdot [D] = [A]$ *for all* $[A] \in \mathcal{C}_\Delta$.

(4) *For each* $[A] \in \mathcal{C}_\Delta$, *the class of* $\overline{A}$ *is an inverse for* $[A]$ *under multiplication:* $[A] \cdot [\overline{A}] = [D]$.

In algebraic terminology, Proposition 5.4.2 implies that $\mathcal{C}_\Delta$ has the properties of an *abelian group* under multiplication.

**Definition.** We refer to $\mathcal{C}_\Delta$ as the *ideal class group* of discriminant $\Delta$.

*Proof.* By Exercise 5.1.2, multiplication is a well-defined operation on the set of all classes of nontrivial ideals of $D$. Theorem 3.6.6 implies that $\gamma(AB) = \operatorname{lcm}(\gamma(A), \gamma(B))$, so that $\mathcal{C}_\Delta$ is closed under multiplication. Note that $[D]$ is an element of $\mathcal{C}_\Delta$ for every $\Delta$, since $D = \langle 1 \rangle$ is a principal ideal, so has index 1

by Corollary 3.6.4. Now statements (1), (2), and (3) of this proposition hold in $\mathcal{C}_\Delta$ because they are true for ideal multiplication in general. (See Exercise 3.4.2.) Finally, if $A$ has index 1, then Theorem 3.4.2 implies that $A\overline{A} = \langle N(A)\rangle$, a principal ideal. Notice that Theorem 3.6.6 and Corollary 3.6.4 then imply that $\overline{A}$ must also have index 1. It follows that $[A] \cdot [\overline{A}] = [D]$ in $\mathcal{C}_\Delta$, since a principal ideal is equivalent to $D$ by Proposition 5.1.2. □

Exercise 5.1.3 shows that if $B = \upsilon A$ for some nonzero element $\upsilon$ and nontrivial ideal $A$ of $D = D_\Delta$, then $[B] = [A]$. So we can restrict our attention to *primitive* ideals of $D$ as representatives of elements of $\mathcal{C}_\Delta$. If $A$ and $B$ are primitive ideals, their product is not necessarily primitive. But if $AB = gC$, then $[A] \cdot [B] = [C]$.

In Theorem 5.4.1, we saw that a quadratic domain $D$ is a unique factorization domain if and only if all of its ideals are principal ideals. In that case, $[A] = [D]$ for all ideals $A$ of $D$. So we can now also say that if $D$ is a *complete* quadratic domain (so that $\gamma(A) = 1$ for all ideals $A$ of $D$), then $D$ is a unique factorization domain if and only if its ideal class group is trivial, that is, contains only the identity element $[D]$. In a sense, we may think of the ideal class group as a measure of how far the quadratic domain $D$ is from having unique factorization.

**The Form Class Group.** Let $\mathcal{Q}_\Delta$ be the set of all quadratic forms of some discriminant $\Delta$, and consider the collection of all classes, $[f]$, of elements $f$ of $\mathcal{Q}_\Delta$. We can define the *index* of $[f]$ to be the same as $\gamma(f)$, since Corollary 4.3.2 shows that equivalent forms have the same index. Then let $\mathcal{F}_\Delta$ be the set of all classes of quadratic forms in $\mathcal{Q}_\Delta$ that have index 1, that is, primitive quadratic forms of discriminant $\Delta$. In §5.3, we defined an operation of composition on primitive quadratic forms in $\mathcal{Q}_\Delta$. This operation makes $\mathcal{F}_\Delta$ into a group.

**Proposition 5.4.3.** *Let $\mathcal{F}_\Delta$ be the set of all classes, under the $\sim$ relation, of primitive quadratic forms of discriminant $\Delta$. Then there is a well-defined operation on $\mathcal{F}_\Delta$ given by $[f] \cdot [g] = [f \cdot g]$ (where $f \cdot g$ is the composite of $f$ and $g$), and $\mathcal{F}_\Delta$ is an abelian group under this operation.*

**Definition.** We call $\mathcal{F}_\Delta$ the *form class group* of discriminant $\Delta$. We will usually refer to the operation on $\mathcal{F}_\Delta$ defined above as multiplication.

*Proof.* We show that the operation of multiplication on $\mathcal{F}_\Delta$ is well-defined. Verification of the group properties then follows immediately from the same properties for ideal class multiplication. So suppose that $f_1 = (a_1 : k_1)$ and $f_2 = (a_2 : k_2)$ are equivalent primitive quadratic forms in $\mathcal{Q}_\Delta$ for some $\Delta$. If $A_1 = [a_1 : k_1]$ and $A_2 = [a_2 : k_2]$ are the corresponding ideals of $f_1$ and $f_2$, respectively, then the proof of Theorem 5.1.5 shows that $A_1$ is equivalent to $A_2$, and that we can write $a_2 A_1 = \upsilon A_2$ for some $\upsilon$ with $N(\upsilon) = a_1 a_2$. Similarly, suppose that $g_1 = (b_1 : \ell_1)$ and $g_2 = (b_2 : \ell_2)$ are equivalent, with corresponding ideals

$B_1 = [b_1 : \ell_1]$ and $B_2 = [b_2 : \ell_2]$. Again, we know that $b_2 B_1 = wB_2$ for some $w$ with $N(w) = b_1 b_2$. Let $f_1 \cdot g_1 = (c_1 : m_1)$ and $f_2 \cdot g_2 = (c_2 : m_2)$. We would like to show that $f_1 \cdot g_1$ is equivalent to $f_2 \cdot g_2$. We know that $A_1 B_1 = [c_1 : m_1]$ and $A_2 B_2 = [c_2 : m_2]$ are equivalent, with

$$a_2 b_2 \cdot A_1 B_1 = a_2 A_1 \cdot b_2 B_1 = vA_2 \cdot wB_2 = vw \cdot A_2 B_2.$$

Note that $N(vw) = N(v) \cdot N(w) = a_1 a_2 \cdot b_1 b_2 = (a_1 b_1)(a_2 b_2)$ has the same sign as $c_1 c_2$ by the definition of quadratic form composition. It follows that $f_1 \cdot g_1$ is equivalent to $f_2 \cdot g_2$ in every case by Theorem 5.2.1. □

**Connection between Class Groups.** To conclude this section, we note a general statement about similarities between $\mathcal{C}_\Delta$ and $\mathcal{F}_\Delta$ for the same discriminant $\Delta$. Here we will assume that $\mathcal{C}_\Delta$ is always finite, a fact we will verify in Chapter 6 for $\Delta < 0$ and in Chapter 10 for $\Delta > 0$.

**Proposition 5.4.4.** *Let $\Delta$ be a discriminant, and suppose that*

$$A_1 = [a_1 : k_1], \quad A_2 = [a_2 : k_2], \quad \dots, \quad A_n = [a_n : k_n]$$

*are representatives of all distinct classes of ideals in $\mathcal{C}_\Delta$. Then every primitive quadratic form of discriminant $\Delta$ is equivalent to (at least) one of the following:*

$$\begin{aligned}(a_1 : k_1), \quad (a_2 : k_2), \quad \dots, \quad (a_n : k_n),\\ (-a_1 : k_1), \quad (-a_2 : k_2), \quad \dots, \quad (-a_n : k_n).\end{aligned} \tag{5.4.1}$$

*If $D_\Delta$ has an element of norm $-1$, then $(a_i : k_i) \sim (-a_i : k_i)$ for $1 \le i \le n$, and $\mathcal{F}_\Delta$ consists precisely of the classes of $(a_1 : k_1), (a_2 : k_2), \dots, (a_n : k_n)$. If not, then the classes of the forms in* (5.4.1) *are all distinct, so $\mathcal{F}_\Delta$ has $2n$ elements.*

*Proof.* By Theorem 5.2.1, if $[a_i : k_i] \sim [a_j : k_j]$, then $(a_i : k_i) \sim (a_j : k_j)$ or $(a_i : k_i) \sim (-a_j : k_j)$ or both. So every primitive form in $\mathcal{Q}_\Delta$ is equivalent to at least one of the forms in (5.4.1). On the other hand, by Theorem 5.1.5, we have that if $(a_i : k_i) \sim (a_j : k_j)$ or $(a_i : k_i) \sim (-a_j : k_j)$, then $[a_i : k_i] \sim [a_j : k_j]$. If $v$ is an element of $D = D_\Delta$ with $N(v) = -1$, then $v$ is a unit in $D$ so that $\langle v \rangle = D$. In that case, $1 \cdot A = v \cdot A$ for every ideal, and so $(a_i : k_i) \sim (-a_i : k_i)$ for all $1 \le i \le n$. Conversely, if $(a_i : k_i) \sim (-a_i : k_i)$ for any $i$, then we find, by multiplying the classes of both forms by the inverse of one of those classes, that $(1 : 0) \sim (-1 : 0)$. In that case, $D$ contains an element $v$ of norm $-1$. □

When $\Delta$ is negative, then $N(v) \ge 0$ for all $v$ in $D_\Delta$, so in that case, $\mathcal{F}_\Delta$ always has twice the number of elements as $\mathcal{C}_\Delta$. We will often restrict our attention to positive definite forms, however. When $\Delta$ is negative, we will view $\mathcal{C}_\Delta$ either as the group of ideal classes of $D_\Delta$ or as the subgroup of $\mathcal{F}_\Delta$ consisting of classes of primitive positive definite forms.

When $\Delta$ is positive, then $|\mathcal{F}_\Delta|$ can equal either $|\mathcal{C}_\Delta|$ or $2|\mathcal{C}_\Delta|$. As Proposition 5.4.4 indicates, the determining factor is whether or not $D_\Delta$ contains an element of norm $-1$.

**Example.** If $\Delta = 8$, then $z = \sqrt{2}$ and $N(q+rz) = q^2-2r^2$. We find that $v = 1+z$ is an element of $D_8$ with $N(v) = -1$. So $|\mathcal{F}_8| = |\mathcal{C}_8|$. ◊

**Example.** If $\Delta = 12$, then $z = \sqrt{3}$ and $N(q + rz) = q^2 - 3r^2$. Since $q^2 - 3r^2 \equiv q^2 + r^2 \pmod 4$, we find that there is no $v$ with $N(v) = -1$, as a sum of two squares cannot be congruent to 3 modulo 4. So $|\mathcal{F}_{12}| = 2|\mathcal{C}_{12}|$. ◊

**Exercise 5.4.5.** Let $\Delta = -20$. Assuming (as is the case), that $\mathcal{C}_\Delta$ consists of the classes of $D = [1 : 0]$ and $A = [2 : 1]$, write a complete operation table of the group $\mathcal{C}_\Delta$. Do the same for the group $\mathcal{F}_\Delta$.

**Exercise 5.4.6.** Let $\Delta = -56$. Assuming that $\mathcal{C}_\Delta$ consists of the classes of $D = [1 : 0]$, $A = [2 : 0]$, $B = [3 : 1]$, and $C = [3 : -1]$, write a complete operation table of the group $\mathcal{C}_\Delta$.

## Correspondence between Forms and Ideals—Review

In this chapter, we saw several important connections, which we will use often in the remainder of this text, between quadratic forms of a particular discriminant $\Delta$ and ideals of the quadratic domain $D_\Delta$. We summarize our main results as follows.

(1) There is an equivalence relation on ideals of a quadratic domain $D$ defined by saying that $A$ is *equivalent* to $B$ (written as $A \sim B$) if $mA = vB$ for some $m \neq 0$ in $\mathbb{Z}$ and $v \neq 0$ in $D$.

(2) If $f = (a : k)$ is a quadratic form of discriminant $\Delta$, then there is a corresponding ideal $A_f = [a : k]$ in the quadratic domain $D_\Delta$.

(3) In the reverse direction, if $A = [a : k]$ is an ideal of $D_\Delta$, then we can associate a quadratic form $f_S$ of discriminant $\Delta$ to each *ordered basis* $S$ of $A$. (The definition of $f_S$ appears in Theorem 5.2.4. A $\mathbb{Z}$-basis $S = \{u, v\}$ for $A$ is ordered if $\overline{u}v - u\overline{v} = N(A) \cdot \sqrt{\Delta}$.) A unimodular matrix converts one ordered basis for $A$ into another, and the corresponding quadratic forms are all equivalent to $(a : k)$ (by the definition of equivalence of quadratic forms in Chapter 4).

(4) If $f_S$ is the quadratic form of an ordered basis $S = \{u, v\}$ for some ideal $A$, and $w = mu+nv$ is written as a $\mathbb{Z}$-combination of $S$, then $N(w) = N(A) \cdot f_S(m, n)$.

(5) If $f = (a : k)$ is equivalent to $f_1 = (a_1 : k_1)$, then $A = [a : k]$ is equivalent to $A_1 = [a_1 : k_1]$. Specifically, if $f_1 = f \circ \begin{bmatrix} q & s \\ r & t \end{bmatrix}$, then $a_1 A = vA_1$, where $v = q(a) + r(k + z)$.

(6) Conversely, if $A = [a : k]$ is equivalent to $A_1 = [a_1 : k_1]$, then either $(a : k) \sim (a_1 : k_1)$ or $(a : k) \sim (-a_1 : k_1)$. (It is possible that both of these statements are true when the discriminant of these forms is positive.) Specifically, if $a$ and $a_1$ are positive, and $mA = \upsilon A_1$ for some nonzero $m$ in $\mathbb{Z}$ and nonzero $\upsilon$ in $D$, then $(a : k) \sim (a_1 : k_1)$ if $N(\upsilon)$ is positive, and $(a : k) \sim (-a_1 : k_1)$ if $N(\upsilon)$ is negative.

(7) There is an operation of composition, $f = f_1 \cdot f_2$, on primitive quadratic forms of a particular discriminant. This operation has the property that if $f_1(q, r) = m$ and $f_2(s, t) = n$, then $f(u, \upsilon) = mn$ for some pair of integers $u$ and $\upsilon$ that can be calculated explicitly in terms of $q$, $r$, $s$, and $t$. Composition is essentially the same as ideal multiplication, when applied to quadratic forms in ideal notation.

(8) The set $\mathcal{C}_\Delta$ of classes (under equivalence as defined in this chapter) of ideals of a quadratic domain $D_\Delta$ having index 1 is well-defined. Ideal multiplication is a well-defined operation on this set, and $\mathcal{C}_\Delta$ has the properties of an abelian group under multiplication, which we call the *ideal class group* of discriminant $\Delta$.

(9) Likewise, composition is a well-defined operation on the set $\mathcal{F}_\Delta$ of classes (under equivalence) of primitive quadratic forms of discriminant $\Delta$, and $\mathcal{F}_\Delta$ has the structure of an abelian group, called the *form class group* of discriminant $\Delta$, under composition.

(10) The number of elements in $\mathcal{F}_\Delta$ is either the same as or twice the number of elements in $\mathcal{C}_\Delta$, depending on whether or not $D_\Delta$ contains an element $\upsilon$ with $N(\upsilon) = -1$.

The structure of these class groups and their applications to representations of integers by quadratic forms will be our main consideration in the next two chapters for negative discriminants, and in Chapters 10 and 11 for positive discriminants.

# Part Three: Positive Definite Quadratic Forms

**Overview.** At the conclusion of Part Two, we defined the class groups of ideals and of quadratic forms of a given discriminant. Our goal now is to determine the elements and the algebraic structure of these groups, and to describe the implications of this structure on arithmetic questions, particularly to representations of integers by quadratic forms. For this question, we will discover that both our methods and results differ substantially depending on whether the discriminant is positive or negative. We concentrate on the negative discriminant case in Part Three, with the objective of applying ideal class groups to representations of integers by positive definite quadratic forms.

We develop practical methods of determining the ideal class group of a particular negative discriminant in Chapter 6, beginning with a systematic method of listing class representatives of quadratic forms or ideals under equivalence. Genus equivalence of ideals, carried over from quadratic forms, helps us to describe the group structure of an ideal class group, which we can typically verify with direct calculation.

In Chapter 7, we demonstrate how the ideal class group of a given negative discriminant provides specific information about representations of integers by positive definite quadratic forms of the same discriminant. We define principal square domains as a setting in which this class group provides complete information about the integers represented by various quadratic forms, but also illustrate how some interesting information is obtained in more arbitrary cases. We also describe methods of constructing a representation of an integer by a positive definite quadratic form, when such a representation is known to exist. We emphasize numerical data to confirm our results throughout this chapter.

Finally, in Chapter 8, we explore connections between the class groups of a complete quadratic domain and of one of its subdomains. We will demonstrate a systematic method by which we can build from the class group of some discriminant to the class group of any square multiple of that discriminant. When the

discriminant is negative, we derive a complete formula for the relation between the orders of these groups.

**Requirements for Part Three.** We will establish in Chapter 6 that the ideal class group of a negative discriminant is always finite. In describing the algebraic structure of this group and its implication to positive definite quadratic forms, we will assume a standard classification of finite abelian groups. We state a form of this result below, along with some associated terminology. A proof of this theorem appears in Appendix C.

**Fundamental Theorem of Finite Abelian Groups.** *Let $G$ be a nontrivial abelian group with $n$ elements. Then $G$ is isomorphic to a direct product of cyclic groups, $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_m}$. These factors are unique under the restriction that $n_{i+1}$ divides $n_i$ for $1 \leq i < m$, and $n_m > 1$.*

**Definition.** If $G$ is isomorphic to $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_m}$ with the conditions on $n_i$ noted above, we refer to $(n_1, n_2, \ldots, n_m)$ as the *invariant factor type* of $G$. If $G$ is trivial, we say that its invariant factor type is (1).

If $G$ has invariant factor type $(n_1, n_2, \ldots, n_m)$, then there are elements $a_1, a_2, \ldots, a_m$ in $G$ so that every element in $G$ can be written uniquely as $a = a_1^{r_1} \cdot a_2^{r_2} \cdots a_m^{r_m}$, with $0 \leq r_i < n_i$ for $1 \leq i \leq m$. (Here we are writing the operation of $G$ as multiplication—the elements $a_i$ are typically not unique.) We allow the possibility that $m = 1$, in which case $G$ is cyclic. Since $n_{i+1}$ divides $n_i$ for $1 \leq i < m$, we find that $a^{n_1} = 1$, the identity element of $G$, for all elements $a$ of $G$. Note that $n = n_1 n_2 \cdots n_m$ and that $(n_m)^m$ divides $n$. This places strong restrictions on the possible invariant factors of an abelian group $G$ of a particular order. For instance, if $n$ is squarefree, then an abelian group with $n$ elements must have invariant factor type $(n)$, that is, be cyclic.

In Chapter 8, we use standard results about homomorphisms between groups. Specifically, we refer to the kernel and image of a homomorphism, and assume the algebraic properties of the associated factor group as described in the Fundamental Homomorphism Theorem. Terms are defined as needed, and we emphasize a concrete method of computing the desired groups. Again, more details can be found in Appendix C.

# 6

# Class Groups of Negative Discriminant

When $\Delta$ is a negative discriminant, then the class group of ideals of the quadratic domain $D_\Delta$ can be identified with the group of classes of *positive definite* quadratic forms in $\mathcal{Q}_\Delta$, as we noted in §5.4. In §6.1, we demonstrate a systematic method of listing all distinct classes of positive definite forms of discriminant $\Delta < 0$, and we will see in §6.2 that we can typically determine the algebraic structure of the ideal class group $\mathcal{C}_\Delta$ in this case. The relation of genus equivalence, introduced for quadratic forms, carries over to classes of ideals, and provides further information about the group properties of $\mathcal{C}_\Delta$, as we will see in §6.3.

## 6.1 Reduced Positive Definite Quadratic Forms

If $f$ and $g$ are quadratic forms of discriminant $\Delta$, then $f$ is equivalent to $g$ if and only if $-f$ is equivalent to $-g$. A positive definite quadratic form cannot represent a negative integer, so $f$ cannot be equivalent to $-f$ when $\Delta$ is negative. Thus it will suffice to determine class representatives for positive definite quadratic forms of a particular discriminant $\Delta < 0$, with the negatives of these forms as class representatives of the negative definite forms of the same discriminant. The following definition precisely describes a collection of such representatives.

**Definition.** Let $f(x, y) = ax^2 + bxy + cy^2$ be a quadratic form with $\Delta = b^2 - 4ac < 0$. We say that $f$ is *reduced* if $-a < b \leq a < c$ or if $0 \leq b \leq a = c$.

It is implicit in this definition that $a$ is positive, so that a reduced quadratic form of negative discriminant is positive definite. We do not assume that a reduced form is primitive, but the following two exercises categorize those that are not.

**Exercise 6.1.1.** If $f(x,y) = ax^2+bxy+cy^2$ is a reduced quadratic form of some discriminant $\Delta < 0$, and $g$ is a positive integer, show that $f_1(x,y) = gax^2+gbxy+gcy^2$ is a reduced quadratic form of discriminant $g^2\Delta$.

**Exercise 6.1.2.** If $f_1(x,y) = a_1x^2 + b_1xy + c_1y^2$ is a reduced quadratic form of some discriminant $\Delta < 0$, and $g = \gcd(a_1, b_1, c_1)$ with $a_1 = ga$, $b_1 = gb$, and $c_1 = gc$, show that $f(x,y) = ax^2 + bxy + cy^2$ is a reduced quadratic form of discriminant $\Delta/g^2$.

We can also describe reduced forms in ideal notation as follows.

**Exercise 6.1.3.** Let $f$ be a quadratic form of negative discriminant $\Delta$, written as $f(x,y) = ax^2 + bxy + cy^2$ in standard notation and as $f = (a : k)$ in ideal notation. Let $\phi(x)$ be the principal polynomial of discriminant $\Delta$. Show that $f$ is reduced if and only if either

(1) $a^2 < \phi(k)$ and $-a < \phi'(k) \le a$, or

(2) $a^2 = \phi(k)$ and $0 \le \phi'(k) \le a$.

(Hint: Recall that $\phi(k) = ac$ and $\phi'(k) = b$.)

The following proposition leads to a straightforward method of listing all reduced quadratic forms of a given negative discriminant $\Delta$ in practice.

**Proposition 6.1.1.** *Let $f$ be a reduced quadratic form of discriminant $\Delta < 0$, written as $f = (a : k)$ in ideal notation. Then $3a^2 \le -\Delta$.*

*Proof.* If $\phi(x) = x^2 + \varepsilon x + \frac{\varepsilon^2-\Delta}{4}$ is the principal polynomial of discriminant $\Delta$, then

$$\phi'(x)^2 - 4\phi(x) = (2x+\varepsilon)^2 - 4x^2 - 4\varepsilon x - \varepsilon^2 + \Delta = \Delta$$

for all $x$. When $f = (a : k)$ is reduced, Exercise 6.1.3 shows that $a^2 \le \phi(k)$ and $\phi'(k)^2 \le a^2$. But then $-\Delta = 4\phi(k) - \phi'(k)^2 \ge 4a^2 - a^2 = 3a^2$. □

In §2.4, we defined $u = u_\Delta = \left\lfloor \sqrt{-\Delta/3} \right\rfloor$ as the *upper bound* of a negative discriminant $\Delta$. To list all reduced quadratic forms $f = (a : k)$ of discriminant $\Delta < 0$, we may assume that $0 < a \le u$ by Proposition 6.1.1. For each such $a$, the inequalities satisfied by $\phi'(k)$ in Exercise 6.1.3 indicate that we must look at $\phi(k)$ for $\frac{-a-\varepsilon}{2} < k \le \frac{a-\varepsilon}{2}$. So we might begin by calculating $\phi(k)$ for $\frac{-u-\varepsilon}{2} < k \le \frac{u-\varepsilon}{2}$.

Since $\phi(-k-\varepsilon)=\phi(k)$, it is sufficient to list $\phi(k)$ for $\frac{-\varepsilon}{2}\le k\le\frac{u-\varepsilon}{2}$. We illustrate this procedure with three examples.

**Example.** Let $\Delta=\Delta(-79,1)=-79$ so that $\phi(x)=x^2+x+20$ and $u_\Delta=\left\lfloor\sqrt{79/3}\right\rfloor=5$. With $\phi(-k-1)=\phi(k)$, it suffices to calculate $\phi(k)$ for $0\le k\le 2$, as in the following table.

| $k$ | $0,-1$ | $1,-2$ | $2,-3$ |
|---|---|---|---|
| $\phi(k)$ | 20 | 22 | 26 |

Now for $1\le a\le 5$, we test whether $a$ divides $\phi(k)$ for $\frac{-a-\varepsilon}{2}<k\le\frac{a-\varepsilon}{2}$, that is, when $-a<\phi'(k)\le a$. In each case, there are exactly $a$ such possibilities for $k$. We find the following complete list of reduced quadratic forms in $\mathcal{Q}_{-79}$:

$$(1:0)=x^2+xy+20y^2,\quad (2:0)=2x^2+xy+10y^2,\quad (2:-1)=2x^2-xy+10y^2,$$
$$(4:0)=4x^2+xy+5y^2,\quad \text{and}\quad (4:-1)=4x^2-xy+5y^2.$$

For example, when $a=3$, we test $-2<k\le 1$, and find no solutions; when $a=4$, we test $-\frac{5}{2}<k\le\frac{3}{2}$, and find that 4 divides $\phi(0)=20=\phi(-1)$. Note that $(5:0)$ and $(5:-1)$ are not reduced since $5^2=25$ is larger than $\phi(0)=20=\phi(-1)$. ◊

**Example.** Let $\Delta=\Delta(-15,4)=-240$, with $\phi(x)=x^2+4x+64$ and $\varepsilon=4$. Here $u_\Delta=\left\lfloor\sqrt{240/3}\right\rfloor=8$, and our required information comes from calculating $\phi(k)$ for $-6<k\le 2$, with $\phi(-k-4)=\phi(k)$.

| $k$ | $-2$ | $-3,-1$ | $-4,0$ | $-5,-1$ | $-6,-2$ |
|---|---|---|---|---|---|
| $\phi(k)$ | 60 | 61 | 64 | 69 | 76 |

The complete list of reduced quadratic forms of discriminant $\Delta=-240$ is

$$(1:-2)=x^2+60y^2,\quad (2:-2)=2x^2+30y^2,\quad (3:-2)=3x^2+20y^2,$$
$$(4:-2)=4x^2+15y^2,\quad (4:0)=4x^2+4xy+16y^2,$$
$$(5:-2)=5x^2+12y^2,\quad (6:-2)=6x^2+10y^2,\quad (8:0)=8x^2+4xy+8y^2.$$

Only four of these forms are primitive: $(2:-2)$ and $(6:-2)$ have index 2, while $(4:0)$ and $(8:0)$ have index 4. The form $(8:-4)$ is not reduced since $a^2=64=\phi(-4)$, with $-4<-\frac{\varepsilon}{2}$. ◊

**Example.** Let $\Delta=\Delta(-62,1)=-248$, with $\phi(x)=x^2+62$ and $u_\Delta=9$. Here it suffices to test $-\frac{9}{2}<k\le\frac{9}{2}$, with $\phi(-k)=\phi(k)$, as in the following table.

| $k$ | $0$ | $\pm1$ | $\pm2$ | $\pm3$ | $\pm4$ |
|---|---|---|---|---|---|
| $\phi(k)$ | 62 | 63 | 66 | 71 | 78 |

The complete list of reduced quadratic forms of discriminant $\Delta=-248$ is

$$(1:0)=x^2+62y^2,\quad (2:0)=2x^2+31y^2,$$

$$(3:1) = 3x^2 + 2xy + 21y^2, \quad (3:-1) = 3x^2 - 2xy + 21y^2,$$
$$(6:2) = 6x^2 + 4xy + 11y^2, \quad (6:-2) = 6x^2 - 4xy + 11y^2,$$
$$(7:1) = 7x^2 + 2xy + 9y^2, \quad (7:-1) = 7x^2 - 2xy + 9y^2.$$

The forms $(9:1)$ and $(9:-1)$ are not reduced since $9^2 > \phi(\pm 1)$. ◊

**Exercise 6.1.4.** In each part, find all reduced forms of the given discriminant $\Delta$.

(a) $\Delta = \Delta(-29, 1) = -116$.

(b) $\Delta = \Delta(-29, 2) = -464$.

(c) $\Delta = \Delta(-119, 1) = -119$.

(d) $\Delta = \Delta(-74, 1) = -296$.

(e) $\Delta = \Delta(-85, 1) = -340$.

(f) $\Delta = \Delta(-86, 1) = -344$.

(g) $\Delta = \Delta(-89, 1) = -356$.

(h) $\Delta = \Delta(-105, 1) = -420$.

**Reduction of Positive Definite Quadratic Forms.** We will prove that reduced forms make up a collection of class representatives for all positive definite quadratic forms of a fixed negative discriminant under equivalence. We begin with a preliminary observation.

**Lemma 6.1.2.** *Let $f(x, y) = ax^2 + bxy + cy^2$ be a reduced quadratic form of discriminant $\Delta < 0$. Then $f(q, r) \geq a$ if $q$ and $r$ are not both zero, and $f(q, r) = a$ if and only if one of the following is true:*

(1) $(q, r) = \pm(1, 0)$,

(2) $a = c$ *and* $(q, r) = \pm(0, 1)$,

(3) $a = b = c$ *and* $(q, r) = \pm(-1, 1)$.

*Proof.* Suppose that $f(q, r) = n \leq a$, with $q$ and $r$ not both zero. Since $f(q, r) = f(-q, -r)$, we can assume that $r \geq 0$. Using equation (4.1.2) and Proposition 6.1.1, we have that

$$4a^2 \geq 4an = (2aq + br)^2 - \Delta r^2 \geq -\Delta r^2 \geq 3a^2 r^2.$$

Thus $r = 0$ or $r = 1$. If $r = 0$ and $q \neq 0$, then $n = f(q, r) = aq^2 \geq a$, with equality holding if and only if $q = \pm 1$. This gives us the two solutions of case (1). Now if $r = 1$, then $n = f(q, r) = aq^2 + bq + c = q(aq + b) + c$. With $f$ reduced, so that $-a < b \leq a$, we find that $q(aq + b) \geq 0$ for every integer $q$. Then $n \geq c \geq a$

in every case, with $n = a$ if and only if $a = c$ and either $q = 0$ or $aq + b = 0$. If $q = 0$, we obtain the two solutions in (2). If $q \neq 0$ but $aq + b = 0$, we find that $q = -1$ and $b = a$, and obtain the two solutions in (3). □

**Theorem 6.1.3.** *Every positive definite quadratic form is equivalent to one and only one reduced form.*

*Proof.* Let $f$ be a positive definite quadratic form. We first show that $f$ is equivalent to a reduced form. If not, then we may assume that $a > 0$ is as small as possible so that $f = (a : k)$ in $\mathcal{Q}_\Delta$ is not equivalent to a reduced form. Since $(a : k) \sim (a : k + au)$ for every integer $u$ by Proposition 4.2.3, we can assume that $\frac{-a-\varepsilon}{2} < k \leq \frac{a-\varepsilon}{2}$, that is, $-a < \phi'(k) \leq a$. Let $g = (c : -k - \varepsilon)$, where $\phi(k) = ac$, so that $f \sim g$ by Proposition 4.2.2. We must have $a^2 \leq \phi(k)$, since otherwise $c < a$, so that $g$, and therefore $f$, is equivalent to a reduced form by assumption. If $a^2 < \phi(k)$, or if $a^2 = \phi(k)$ and $0 \leq \phi'(k) \leq a$, then $f$ is reduced by Exercise 6.1.3. Assume instead that $a^2 = \phi(k)$ and $-a < \phi'(k) < 0$, so that $\frac{-a-\varepsilon}{2} < k < -\frac{\varepsilon}{2}$. But now $c = a$, so that $g = (a : -k - \varepsilon)$, and we find that $-\frac{\varepsilon}{2} < -k - \varepsilon < \frac{a-\varepsilon}{2}$, that is, $0 < \phi'(-k - \varepsilon) < a$. Thus $g$ is reduced, and so $f$ must be equivalent to a reduced form.

To show that every positive definite quadratic form is equivalent to only one reduced form, suppose that $f(x, y) = ax^2+bxy+cy^2$ and $f_1(x, y) = a_1x^2+b_1xy+c_1y^2$ are both reduced, and are equivalent, say with $U = \begin{bmatrix} q & s \\ r & t \end{bmatrix}$ a unimodular matrix for which $f_1 = f \circ U$. By equation (4.2.1),

$$a_1 = aq^2 + bqr + cr^2 = f(q, r),$$

$$b_1 = 2aqs + b(qt + rs) + 2crt,$$

and

$$c_1 = as^2 + bst + ct^2 = f(s, t).$$

The first equation shows that $f$ represents $a_1$, so Lemma 6.1.2 implies that $a_1 \geq a$. But since $f = f_1 \circ U^{-1}$, we conclude in the same way that $f_1$ represents $a$, and thus $a \geq a_1$. Therefore $a$ is equal to $a_1$, and we have that $-a < b, b_1 \leq a$ by the definition of reduced forms.

Now with $f(q, r) = a$, Lemma 6.1.2 gives us three pairs of possibilities for $q$ and $r$. If $q = 1$ and $r = 0$, then $\det U = 1$ forces $t = 1$, and thus $b_1 = 2as + b$. But with $-a < b, b_1 \leq a$, this can occur only when $s = 0$. Now $b_1 = b$ and $c_1 = c$, and so $f_1 = f$. The case in which $q = -1$ and $r = 0$ is similar.

Next suppose that $q = 0$ and $r = 1$, which by Lemma 6.1.2 can occur only when $a = c$ and then $0 \leq b \leq a$. Here $\det U = 1$ implies that $s = -1$, so that $b_1 = -b + 2ct = -b + 2at$. With $-a < b_1 \leq a$ and $0 \leq b \leq a$, we have that $-a < b_1 + b \leq 2a$, and conclude that $t = 0$ or $t = 1$. If $t = 0$, we find that

$b_1 = -b$ and $c_1 = a = c$. But now with $a_1 = c_1$ and $f_1$ reduced, we must have $b_1 \geq 0$. This forces $b_1 = 0 = b$, so we conclude that $f_1 = f$. On the other hand, if $t = 1$, then $b_1 = -b + 2a$ and $c_1 = a - b + c$. But here $0 \leq b \leq a$ implies that $a \leq b_1 \leq 2a$. Since we must also have $-a < b_1 \leq a$, the only possibility is that $b_1 = -b + 2a = a$. So in this case, $b_1 = a = b$ and $c_1 = a - b + c = c$, and again $f_1 = f$. The case in which $q = 0$ and $r = -1$ is similar.

Finally, let $q = -1$ and $r = 1$, in which case $a = b = c$ by Lemma 6.1.2. Now $\det U = 1$ implies that $s + t = -1$, and we find that

$$b_1 = -2as + b(-t + s) + 2ct = -2as + a(-t + s) + 2at = a(t - s).$$

With $s = -t - 1$, we then see that $b_1 = a(2t + 1)$, and since $-a < b_1 \leq a$, this implies that $t = 0$ and $s = -1$. Thus $b_1 = a = b$ and $c_1 = a = c$, and so $f_1 = f$. The case in which $q = 1$ and $r = -1$ is similar. □

The first part of the proof of Theorem 6.1.3 suggests a method for finding the reduced form that is equivalent to a given positive definite form, which we illustrate with the following example.

**Example.** Let $\Delta = -79$, so that $\phi(x) = x^2 + x + 20$. We verify that $f = (104 : 36)$ is an element of $\mathcal{Q}_\Delta$ by noting that $\phi(36) = 1352 = 104 \cdot 13$. The following sequence of involutions and translations, similar to an example at the end of §4.1, shows that $f$ is equivalent to one of the reduced forms of discriminant $\Delta = -79$ found in a previous example:

$$(104 : 36) \leftrightarrow (13 : -37) \rightarrow_3 (13 : 2) \leftrightarrow (2 : -3) \rightarrow_1 (2 : -1).$$

Our conclusion is that

$$f(x, y) = 104x^2 + 73xy + 13y^2 \sim 2x^2 - xy + 10y^2 = g(x, y).$$

We can use our sequence of equivalences to verify this conclusion more directly. Each equivalence is obtained from a specific unimodular matrix, and the outcome of the entire sequence comes from the *product* of those matrices as follows:

$$U = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} -1 & -1 \\ 3 & 2 \end{bmatrix}.$$

We leave it to the reader to confirm that $M_g = U^T M_f U$, that is, $g = f \circ U$. ◊

**Exercise 6.1.5.** In each part, verify that $f = (a : k)$ is a quadratic form in $\mathcal{Q}_\Delta$, find the reduced form $g$ in $\mathcal{Q}_\Delta$ to which $f$ is equivalent, and find a unimodular matrix $U$ so that $g = f \circ U$.

(a) $f = (60 : 14)$ in $\mathcal{Q}_{-119}$.

(b) $f = (187 : 17)$ in $\mathcal{Q}_{-340}$.

(c) $f = (179 : 49)$ in $\mathcal{Q}_{-420}$.

**Automorphs of Reduced Positive Definite Forms.** We noted, following the statement of Proposition 4.3.5, that if we wish to find the group of automorphs of an arbitrary quadratic form, it suffices to calculate $\mathrm{Aut}(f)$ for a collection of class representatives $f$ of quadratic forms of a fixed discriminant. We can now do so in every case where $\Delta$ is negative.

**Theorem 6.1.4.** *Let $f(x,y) = ax^2 + bxy + cy^2$ be a reduced quadratic form of discriminant $\Delta < 0$. Then the group $\mathrm{Aut}(f)$ of automorphs of $f$ is one of the following.*

(1) $\left\{\pm\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \pm\begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}, \pm\begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix}\right\}$, *if $a = b = c$.*

(2) $\left\{\pm\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \pm\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\right\}$, *if $a = c$ and $b = 0$.*

(3) $\left\{\pm\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right\}$, *otherwise.*

*Proof.* Lemma 6.1.2 lists all possible solutions of $f(q,r) = a$, so all potential first columns of a unimodular matrix $U$ for which $f \circ U = f$. If $q = 1$ and $r = 0$, then $s = 0$ and $t = 1$ by Proposition 4.3.4. Likewise, if $q = -1$ and $r = 0$, then $s = 0$ and $t = -1$. That is, the identity matrix $I$ and its negative are automorphs of every quadratic form. If $a \neq c$, then Lemma 6.1.2 implies that $I$ and $-I$ can be the only automorphs of $f$.

Now suppose that $a = c$, so that $0 \leq b \leq a$. Proposition 4.3.4 shows in fact that $b = 0$ or $b = a$ and thus there can be no more automorphs in case (3). If $b = 0$, then either $q = 0$ and $r = 1$, in which case $s = -1$ and $t = 0$, or $q = 0$ and $r = -1$, so that $s = 1$ and $t = 0$. This gives us the second pair of automorphs in case (2).

Finally, suppose that $a = b = c$, so that $s = -r$ and $t = q + r$ by Proposition 4.3.4. Substituting the possible values of $q$ and $r$ from Lemma 6.1.2 produces the second and third pairs of automorphs in case (1). □

Notice that cases (1) and (2) of Theorem 6.1.4 can occur only when $\Delta = -3a^2$ or $\Delta = -4a^2$, respectively. If $f$ is a *primitive* positive definite quadratic form of discriminant $\Delta < -4$, then $\mathrm{Aut}(f) = \{I, -I\}$, where $I$ is the identity matrix. When the discriminant of $f$ is $-3$ or $-4$, $\mathrm{Aut}(f)$ contains six or four elements, respectively, but is typically not the same as the group in (1) or (2) above, as the following example illustrates.

**Example.** If $f(x,y) = x^2 + y^2$ and $V = \begin{bmatrix} 5 & 7 \\ 2 & 3 \end{bmatrix}$, a unimodular matrix, we find that $f \circ V = g$ for $g(x,y) = 29x^2 + 82xy + 58y^2$ in $\mathcal{Q}_{-4}$. By Proposition 4.3.5 and

Theorem 6.1.4,

$$\begin{aligned}\mathrm{Aut}(g) &= \{V^{-1}UV \mid U \in \mathrm{Aut}(f)\} \\ &= \left\{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -41 & -58 \\ 29 & 41 \end{bmatrix}, \begin{bmatrix} 41 & 58 \\ -29 & -41 \end{bmatrix}\right\}\end{aligned}$$

is the group of automorphs of $g$. ◊

## 6.2 Calculation of Ideal Class Groups

In §6.1, we determined a specific collection of class representatives for quadratic forms of negative discriminant, which we called *reduced* forms. We extend this definition to ideals of a quadratic domain $D_\Delta$ when $\Delta$ is negative.

**Definition.** Let $D$ be the quadratic domain and $\phi(x) = x^2 + \varepsilon x + \frac{\varepsilon^2 - \Delta}{4}$ the principal polynomial of some negative discriminant $\Delta$. Let $A$ be a primitive ideal of $D$, written as $A = [a : k]$ with $\frac{-a-\varepsilon}{2} < k \leq \frac{a-\varepsilon}{2}$. Then $A$ is *reduced* if $a^2 < \phi(k)$ or if $a^2 = \phi(k)$ and $k \geq -\frac{\varepsilon}{2}$.

Note that every primitive ideal can be written uniquely as $A = [a : k]$ with $a$ positive and $\frac{-a-\varepsilon}{2} < k \leq \frac{a-\varepsilon}{2}$, since the character of $A$ is determined modulo the subnorm of $A$. The conditions on $k$ imply that either $a^2 < \phi(k)$ and $-a < \phi'(k) \leq a$, or $a^2 = \phi(k)$ and $0 \leq \phi'(k) \leq a$, precisely the same as in the definition for a reduced quadratic form $(a : k)$ of negative discriminant written in ideal notation.

**Theorem 6.2.1.** *If $D$ is the quadratic domain of discriminant $\Delta < 0$, then every nontrivial ideal of $D$ is equivalent to exactly one reduced ideal. Thus the ideal class group $\mathcal{C}_\Delta$ consists precisely of (the classes of) the reduced ideals $A$ of $D$ for which $\gamma(A) = 1$.*

*Proof.* Theorems 5.1.5 and 5.2.1 establish a bijection between classes of ideals of $D_\Delta$ and classes of positive definite quadratic forms in $\mathcal{Q}_\Delta$ when $\Delta$ is negative. So this theorem follows from Theorem 6.1.3. □

If $A$ is a reduced ideal, we write its ideal class as $[A]$. When we express $A$ as $[a : k]$, however, we will simplify notation by writing $[A]$ with a single pair of brackets, that is, as $[a : k]$ rather than $[[a : k]]$. To avoid confusion, we will use the $\sim$ symbol to indicate that the classes of two ideals written in this way are equal. We will write $[a : k] = [b : \ell]$ only when the underlying ideals are in fact equal, that is, when $b = \pm a$ and $\ell \equiv k \pmod{a}$.

Let $u_\Delta = \left\lfloor \sqrt{-\Delta/3} \right\rfloor$, the upper bound of a negative discriminant $\Delta$. Applying Proposition 6.1.1 to ideals, we know that if $A = [a : k]$ in $D_\Delta$ is reduced, then $a \le u_\Delta$. We can list all examples of reduced ideals by the same procedure we illustrated for reduced quadratic forms in §6.1. We have seen that $D_\Delta$ has finitely many ideals of any particular norm since $\phi(x) \equiv 0 \pmod{m}$ has finitely many solutions for a given $m$. Thus $\mathcal{C}_\Delta$ is finite when $\Delta$ is negative, and the structure of $\mathcal{C}_\Delta$ is as described in the Fundamental Theorem of Finite Abelian Groups in the introduction to Part Three.

**Example.** Let $D$ be the quadratic domain of discriminant $\Delta(-17, 1) = -68$, so that $\phi(x) = x^2 + 17$. Here $D$ is a complete quadratic domain, and so $\gamma(A) = 1$ for all ideals $A$ of $D$. We have that $u_\Delta = \left\lfloor \sqrt{68/3} \right\rfloor = 4$, so can find all reduced ideals $[a : k]$ by calculating $\phi(k)$ for $-1 \le k \le 2$, using the fact that $\phi(-k) = \phi(k)$, as in the following table.

| $k$ | 0 | $\pm 1$ | $\pm 2$ |
|---|---|---|---|
| $\phi(k)$ | 17 | 18 | 21 |

We conclude that

$$\mathcal{C}_{-68} = \{[1 : 0], [2 : 1], [3 : 1], [3 : -1]\}.$$

For example, when $a = 3$, we test $-\frac{3}{2} < k \le \frac{3}{2}$ and find that 3 divides $\phi(\pm 1) = 18$, with $3^2 \le 18$. But $a = 4$ divides no $\phi(k)$ term with $-2 < k \le 2$.

Here $G = \mathcal{C}_{-68}$ has four elements, so has invariant factor type (4) or (2, 2). We can determine which is the case using the multiplication methods of §3.4 together with involutions of ideals, as in Corollary 5.1.6, for reduction of a product to a reduced form. By trial-and-error, if $[A] = [3 : 1]$, then

$$[A]^2 = [9 : 1] \sim [2 : -1] = [2 : 1].$$

Since $[A]$ does not have order two, we know that $G$ must be cyclic. To confirm this directly, now

$$[A]^3 = [3 : 1] \cdot [2 : 1] = [6 : 1] \sim [3 : -1],$$

and then

$$[A]^4 = [3 : 1] \cdot [3 : -1] = 3[1 : 0] \sim [1 : 0],$$

the identity element of $G$. ◊

**Example.** Let $D = D_{-119}$, so that $\phi(x) = x^2 + x + 30$. With $u_\Delta = \left\lfloor \sqrt{119/3} \right\rfloor = 6$ and $\phi(-k - 1) = \phi(k)$, the following table is sufficient for finding all reduced ideals of $D$.

| $k$ | $-1, 0$ | $-2, 1$ | $-3, 2$ |
|---|---|---|---|
| $\phi(k)$ | 30 | 32 | 36 |

Since $D$ is complete, all reduced ideals are elements of the ideal class group, and we find that $\mathcal{C}_{-119}$ equals

$$\{[1:0],[2:0],[2:-1],[3:0],[3:-1],\\ [4:1],[4:-2],[5:0],[5:-1],[6:2]\}.$$

For example, when $a=6$, we need to test $-\frac{7}{2} < k \le \frac{5}{2}$. Here 6 divides $\phi(0) = 30 = \phi(-1)$, but since $a^2 > \phi(k)$, the ideals $[6:0]$ and $[6:-1]$ are not reduced. Also, 6 divides $\phi(-3) = 36 = \phi(2)$, but with $a^2 = \phi(k)$, only $[6:2]$ is reduced. So $G = \mathcal{C}_{-119}$ has ten elements, and must be cyclic since 10 is squarefree. We verify this with the following calculations of ideal multiplication and reduction, leaving the details for the reader to confirm.

(1) Let $[A] = [3:0]$ (by trial-and-error).

(2) Then $[A]^2 = [9:-3] \sim [4:2] = [4:-2]$.

(3) $[A]^3 = [3:0]\cdot[4:-2] = [12:-6] \sim [5:5] = [5:0]$.

(4) $[A]^4 = [3:0]\cdot[5:0] = [15:0] \sim [2:-1]$.

(5) $[A]^5 = [3:0]\cdot[2:-1] = [6:-3] \sim [6:2]$.

(6) $[A]^6 = [3:0]\cdot[6:2] = [3:0]\cdot[3:-1]\cdot[2:0] = 3[2:0] \sim [2:0]$.

(7) $[A]^7 = [3:0]\cdot[2:0] = [6:0] \sim [5:-1]$.

(8) $[A]^8 = [3:0]\cdot[5:-1] = [15:-6] \sim [4:5] = [4:1]$.

(9) $[A]^9 = [3:0]\cdot[4:1] = [12:-3] \sim [3:2] = [3:-1]$.

(10) $[A]^{10} = [3:0]\cdot[3:-1] = 3[1:0] \sim [1:0]$.

Thus $\mathcal{C}_{-119} = \{[A]^i \mid 0 \le i < 10\}$ with invariant factor type (10). ◊

**Example.** Let $D = D_{-108}$, where $\Delta = \Delta(-3,6) = -108$. Here with $u_\Delta = \left\lfloor \sqrt{108/3} \right\rfloor = 6$, and with $\phi(-k-6) = \phi(k)$ for the principal polynomial $\phi(x) = x^2+6x+36$, the following table is sufficient to determine the reduced ideals of $D$.

| $k$ | $-3$ | $-4,-2$ | $-5,-1$ | $-6,0$ |
|---|---|---|---|---|
| $\phi(k)$ | 27 | 28 | 31 | 36 |

The reduced ideals are

$$[1:-3],\quad [2:-2],\quad [3:-3],\quad [4:-2],\quad [4:-4],\quad [6:0],$$

but not all of these are part of the ideal class group. We find that $\gamma([2:-2]) = 2$, $\gamma([3:-3]) = 3$, and $\gamma([6:0]) = 6$, and so

$$G = \mathcal{C}_{-108} = \{[1:-3],[4:-2],[4:-4]\}.$$

With $|G| = 3$, we know that $G$ is cyclic. We verify that if $[A] = [4 : -2]$, then $[A]^2 = 2[4 : -4] \sim [4 : -4]$ (using Theorem 3.6.1 for example), and then $[A]^3 = \langle 4 \rangle \sim [1 : 0]$. ◊

We will develop an alternative method of determining the class group of a quadratic subdomain in Chapter 8.

**Example.** Let $D = D_{-308}$, with $\phi(x) = x^2 + 77$ and $u_\Delta = \left\lfloor \sqrt{308/3} \right\rfloor = 10$. From the table

| $k$ | 0 | $\pm 1$ | $\pm 2$ | $\pm 3$ | $\pm 4$ | $\pm 5$ |
|---|---|---|---|---|---|---|
| $\phi(k)$ | 77 | 78 | 81 | 86 | 93 | 102 |

we find the following set of reduced ideals of $D$, which equals the ideal class group.

$$G = \mathcal{C}_{-308} = \{[1 : 0], [2 : 1], [3 : 1], [3 : -1], [6 : 1], [6 : -1], [7 : 0], [9 : 2]\}.$$

Note that $[9 : -2]$ is not reduced since $\phi(-2) = 9^2$ with $-2 < -\frac{\varepsilon}{2} = 0$.

There are three possible invariant factor types of abelian groups with eight elements: (8), (4, 2), and (2, 2, 2). But a cyclic group of even order has only one element of order two, while $[2 : 1]^2 = \langle 2 \rangle \sim D$ and $[7 : 0]^2 = \langle 7 \rangle \sim D$ by our classification of prime ideals of $D$. Hence we can eliminate the possibility that $G$ has invariant factor type (8). On the other hand, if $G$ has type (2, 2, 2), then $[A]^2 = [D]$ for all $[A]$. This case can be eliminated by direct calculation, as we show below with $A = [3 : 1]$. So $G$ must have invariant factor type (4, 2). We confirm this as follows, again leaving details to the reader.

(1) Let $[A] = [3 : 1]$.

(2) $[A]^2 = [9 : -2] \sim [9 : 2]$.

(3) $[A]^3 = [3 : 1] \cdot [9 : 2] = [3 : 1] \cdot [3 : -1] \cdot [3 : -1] = 3[3 : -1] \sim [3 : -1]$.

(4) $[A]^4 = 3[1 : 0] \sim [1 : 0] = [D]$.

(5) Let $[B] = [2 : 1]$, so that $[B]^2 = 2[1 : 0] \sim [D]$, as noted above.

(6) $[A] \cdot [B] = [3 : 1] \cdot [2 : 1] = [6 : 1]$.

(7) $[A]^2 \cdot [B] = [9 : 2] \cdot [2 : 1] = [18 : -7] \sim [7 : 7] = [7 : 0]$.

(8) $[A]^3 \cdot [B] = [3 : -1] \cdot [2 : 1] = [6 : -1]$.

Therefore $\mathcal{C}_{-308} = \{[A]^i \cdot [B]^j \mid 0 \le i < 4 \text{ and } 0 \le j < 2\}$. ◊

**Exercise 6.2.1.** For the following values of $\Delta$, list the distinct elements in the ideal class group $\mathcal{C}_\Delta$, and determine the invariant factor type of that group. (Note that many of these values of $\Delta$ are the same as those in Exercise 6.1.4.)

(a) $\Delta = -20$.

(b) $\Delta = -40$.

(c) $\Delta = -47$.

(d) $\Delta = -56$.

(e) $\Delta = -84$.

(f) $\Delta = -116$.

(g) $\Delta = -119$.

(h) $\Delta = -296$.

(i) $\Delta = -340$.

(j) $\Delta = -344$.

(k) $\Delta = -356$.

(l) $\Delta = -420$.

**Exercise 6.2.2.** In §2.6, we claimed that $D_\Delta$ is a unique factorization domain for the following negative values of $\Delta$: $-3$, $-4$, $-7$, $-8$, $-11$, $-19$, $-43$, $-67$, and $-163$. Verify that $\mathcal{C}_\Delta$ is trivial for each of these values of $\Delta$.

## 6.3 Genera of Ideal Classes

In §4.4, we defined a collection of genus symbols for primitive quadratic forms of a given discriminant $\Delta$. In particular, for each odd prime $p$ that divides $\Delta$, the genus symbol $\left(\frac{f}{p}\right)$ is the same as the Legendre symbol $\left(\frac{m}{p}\right)$, where $m$ is any integer not divisible by $p$ that is represented by $f$. (Other symbols might be defined if 2 divides $\Delta$. We will recall these possibilities below, rephrased in terms of ideals.) Genus symbols are consistent with the composition operation defined on primitive forms, in the following sense.

**Proposition 6.3.1.** *Let $f_1$ and $f_2$ be primitive quadratic forms of some discriminant $\Delta$, and let $p$ be an odd prime that divides $\Delta$. If $f_1 \cdot f_2 = f$, then $\left(\frac{f_1}{p}\right) \cdot \left(\frac{f_2}{p}\right) = \left(\frac{f}{p}\right)$.*

We state this proposition only for odd primes as a matter of convenience. The same result holds for all other genus symbols that are defined.

*Proof.* Let $m$ and $n$ be integers represented by $f_1$ and $f_2$, respectively, neither divisible by $p$. Then $f = f_1 \cdot f_2$ represents $mn$ by Theorem 5.3.3, and so $\left(\frac{f}{p}\right) = \left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right) \cdot \left(\frac{n}{p}\right) = \left(\frac{f_1}{p}\right) \cdot \left(\frac{f_2}{p}\right)$. □

Primitive forms $f$ and $g$ in $\mathcal{Q}_\Delta$ are *genus equivalent*, $f \approx g$, if $f$ and $g$ have the same collection of genus symbols. If $f$ is equivalent to $g$, then $f$ is genus equivalent to $g$, so we can view this relation as being defined on the form class group $\mathcal{F}_\Delta$, with the genus symbols of $[f]$ the same as the genus symbols of $f$.

We can carry over the definition of genus symbols and genus equivalence to ideals $A$ having index 1, and to the ideal class group $\mathcal{C}_\Delta$. We restate our definitions for ideals as follows.

**Definition.** Let $A = [a : k]$ be a primitive ideal of $D = D_\Delta$ for which $\gamma(A) = 1$. Let $p$ be a prime number that divides $\Delta$, and suppose that $p$ does not divide $a$. We define *genus symbols* for $A$ as follows. If $p$ is odd, then we let $\left(\frac{A}{p}\right) = \left(\frac{a}{p}\right)$. If $p = 2$ and $\Delta_0 = \frac{\Delta}{4}$, then:

(1) If $\Delta_0 \equiv 0$ or $3 \pmod 4$, let $\left(\frac{-1}{A}\right) = \begin{cases} 1, & \text{if } a \equiv 1 \pmod 4 \\ -1, & \text{if } a \equiv 3 \pmod 4. \end{cases}$

(2) If $\Delta_0 \equiv 0$ or $2 \pmod 8$, let $\left(\frac{2}{A}\right) = \begin{cases} 1, & \text{if } a \equiv 1 \text{ or } 7 \pmod 8 \\ -1, & \text{if } a \equiv 3 \text{ or } 5 \pmod 8. \end{cases}$

(3) If $\Delta_0 \equiv 0$ or $6 \pmod 8$, let $\left(\frac{-2}{A}\right) = \begin{cases} 1, & \text{if } a \equiv 1 \text{ or } 3 \pmod 8 \\ -1, & \text{if } a \equiv 5 \text{ or } 7 \pmod 8. \end{cases}$

If $p$ divides $a$, we let $\phi(k) = ac$ and replace $a$ by $c$ in the calculation of the appropriate symbol. We define genus symbols for the ideal class $[A]$ to be the same as for $A$. If $A$ and $B$ are ideals of $D$ having index 1, we say that $A$ is *genus equivalent* to $B$, and write $A \approx B$, if $A$ and $B$ have the same collection of genus symbols. We also write $[A] \approx [B]$ in this case, defining the same relation on the ideal class group $\mathcal{C}_\Delta$.

Recall that we also defined a symbol $\left(\frac{f}{\infty}\right)$ for quadratic forms of negative discriminant, which distinguishes between positive definite and negative definite forms. This symbol will not be needed for ideals or ideal classes. Genus equivalence is a well-defined equivalence relation on the ideal class group $\mathcal{C}_\Delta$, so we can view $\mathcal{C}_\Delta$ as being partitioned into genera. We note a property of one of these genera in the following definition and proposition.

**Definition.** Let $\mathcal{C}_\Delta$ be the ideal class group of some discriminant $\Delta$. We define the *principal genus* of discriminant $\Delta$, written as $\mathcal{G}_\Delta$, to be the set of all $[A]$ in $\mathcal{C}_\Delta$ for which every defined genus symbol equals 1.

**Proposition 6.3.2.** *For every discriminant $\Delta$, the principal genus $\mathcal{G}_\Delta$ is a subgroup of the ideal class group $\mathcal{C}_\Delta$.*

*Proof.* The class of $D = [1 : 0]$ is contained in $\mathcal{G}_\Delta$ so the principal genus is nonempty. The inverse of $[A] = [a : k]$ is $[\overline{A}] = [a : -k - \varepsilon]$, with the same values of $a$ and $c$, and so the same genus symbols. Thus if $[A]$ is in $\mathcal{G}_\Delta$, then $[\overline{A}]$ is in $\mathcal{G}_\Delta$ as well. Finally, $\mathcal{G}_\Delta$ is closed under multiplication, using Proposition 6.3.1 extended to ideal classes. □

In group terminology, every genus of ideal classes is a coset of $\mathcal{G}_\Delta$ in $\mathcal{C}_\Delta$. It follows that each genus contains the same number of classes.

**Example.** Let $\Delta = -308 = -4 \cdot 7 \cdot 11$. Since $\frac{\Delta}{4} \equiv 3 \pmod 4$, the symbol $\left(\frac{-1}{A}\right)$ is defined, as are $\left(\frac{A}{7}\right)$ and $\left(\frac{A}{11}\right)$. In §6.2, we found that there were eight elements of $G = \mathcal{C}_{-308}$. They can be assigned genus symbols as follows (in order as $\left(\frac{-1}{A}\right)$, $\left(\frac{A}{7}\right)$, and $\left(\frac{A}{11}\right)$):

$$\begin{array}{lcll} +++ & : & [1:0] & [9:2] \\ +-- & : & [6:1] & [6:-1] \\ -+- & : & [2:1] & [7:0] \\ --+ & : & [3:1] & [3:-1] \end{array}$$

For example, with $\phi(1) = 6 \cdot 13$, then for $A = [6 : 1]$ we have $\left(\frac{-1}{A}\right) = 1$ since $13 \equiv 1 \pmod 4$, $\left(\frac{A}{7}\right) = \left(\frac{6}{7}\right) = -1$, and $\left(\frac{A}{11}\right) = \left(\frac{6}{11}\right) = -1$. For $A = [7 : 0]$, with $\phi(0) = 7 \cdot 11$, we have $\left(\frac{-1}{A}\right) = -1$ (since $7 \equiv 3 \pmod 4$), $\left(\frac{A}{7}\right) = \left(\frac{11}{7}\right) = 1$, and $\left(\frac{A}{11}\right) = \left(\frac{7}{11}\right) = -1$. In §6.2, we found that if $[A] = [3 : 1]$ and $[B] = [2 : 1]$, then every element of $G$ can be written uniquely as $[A]^i \cdot [B]^j$ with $0 \le i < 4$ and $0 \le j < 2$. If we write $\mathcal{G}_\Delta$ as $H$, then

$$\begin{gathered} H = \{[D], [A]^2\} = \{[1:0], [9:2]\}, \\ ([A] \cdot [B]) \cdot H = \{[A] \cdot [B], [A]^3 \cdot [B]\} = \{[6:1], [6:-1]\}, \\ [B] \cdot H = \{[B], [A]^2 \cdot [B]\} = \{[2:1], [7:0]\}, \\ [A] \cdot H = \{[A], [A]^3\} = \{[3:1], [3:-1]\} \end{gathered}$$

are the distinct genera of $H$ in $\mathcal{C}_\Delta$. ◊

**Squares of Ideal Classes.** In the preceding example, the principal genus $H = \mathcal{G}_\Delta$ consists of all elements of $G = \mathcal{C}_\Delta$ for which the exponent on each generator is even, that is, all squares of elements of $G$. To conclude this section, we will show that the same is true for every principal genus in the ideal class group of a *complete* quadratic domain. We establish part of this claim as follows.

**Proposition 6.3.3.** *Let $G = \mathcal{C}_\Delta$ and $H = \mathcal{G}_\Delta$ be the ideal class group and principal genus, respectively, of some discriminant $\Delta$. Let $G^2$ be the set of all squares of elements of $G$. Then $G^2$ is a subgroup of $G$ contained in $H$.*

*Proof.* The subset $G^2$ contains $[D]^2 = [D]$. If $[A]^2$ is in $G^2$, then so is its inverse $[\overline{A}]^2$. If $[A]^2$ and $[B]^2$ are in $G^2$, then their product is in $G^2$ as well, since $[A]^2 \cdot [B]^2 = ([A] \cdot [B])^2$. (Note that here we require the commutative property of multiplication in $G$.) So $G^2$ is a subgroup of $G$. If an odd prime $p$ divides $\Delta$, the discriminant of $D$, then $\left(\frac{A^2}{p}\right) = \left(\frac{A}{p}\right)^2 = 1$ by Proposition 6.3.1, and the same is true for every other defined genus symbol. So every element of $G^2$ is included in the principal genus $H$. □

Proposition 6.3.3, combined with the next two results, often helps us determine the invariant factor type of an ideal class group.

**Proposition 6.3.4.** *Let $D$ be a complete quadratic domain of negative discriminant $\Delta$, and let $t$ be the number of distinct prime factors of $\Delta$. Then there are $2^{t-1}$ genera of ideal classes of $D$.*

*Proof.* In all cases, there are precisely $t$ genus symbols defined for an ideal $A$ of $D$, and so $2^t$ possible assignments of $\pm 1$ to those symbols. (If $\frac{\Delta}{4}$ is congruent to 2 or 3 modulo 4, then exactly one symbol among $\left(\frac{-1}{A}\right)$, $\left(\frac{2}{A}\right)$, and $\left(\frac{-2}{A}\right)$ is defined.) But we saw in Proposition 4.4.3 that the product of all genus symbols that are defined must equal 1, thus cutting the number of possibilities in half. □

**Proposition 6.3.5.** *Let $D$ be the quadratic domain of discriminant $\Delta$, and suppose that the ideal class group $G = \mathcal{C}_\Delta$ has invariant factor type $(n_1, n_2, \ldots, n_m)$. Let $\ell$ be the largest integer for which $n_\ell$ is even. Then $G^2$ contains $|G|/2^\ell$ elements.*

We allow the possibility that $\ell = 0$, if all invariant factors are odd. The definition of invariant factors ensures that $n_1, \ldots, n_\ell$ are all even, as $\ell$ is defined.

*Proof.* Let $[A_1], [A_2], \ldots, [A_m]$ be generators of $G = \mathcal{C}_\Delta$. The number of elements in $G^2$ is the number of distinct elements of the form

$$[A_1]^{2r_1} \cdot [A_2]^{2r_2} \cdots [A_m]^{2r_m} = [A_1]^{s_1} \cdot [A_2]^{s_2} \cdots [A_m]^{s_m}.$$

If $n_i$ is odd, then $2r_i \equiv s_i \pmod{n_i}$ has a solution no matter what $s_i$ is, but if $n_i$ is even, a solution exists if and only if $s_i$ is even. The number of possibilities for $s_1, s_2, \ldots, s_m$ is

$$\frac{n_1}{2} \cdots \frac{n_\ell}{2} \cdot n_{\ell+1} \cdots n_m = \frac{n_1 n_2 \cdots n_m}{2^\ell} = \frac{|G|}{2^\ell},$$

and so $|G^2| = |G|/2^\ell$. □

Combining the three preceding propositions, then $|G|/2^\ell \le |G|/2^{t-1}$, so that $\ell \ge t-1$. That is, if $\Delta$ is a primitive discriminant with $t$ distinct prime factors, then the invariant factor type of $\mathcal{C}_\Delta$ has at least $t-1$ even terms.

**Example.** Let $\Delta = \Delta(-182, 1) = -728$, where $-182 = -1 \cdot 2 \cdot 7 \cdot 13$, and let $D = D_{-728}$, a complete quadratic domain. Since $-182 \equiv 2 \pmod 8$, the genus symbols $\left(\frac{2}{A}\right)$, $\left(\frac{A}{7}\right)$, and $\left(\frac{A}{13}\right)$ are defined (and are written in that order in the list below). Using the methods of §6.1 and §6.2, we find that there are twelve reduced ideals of discriminant $-728$. An abelian group of order 12 can have invariant factor type (12) or (6, 2), but since $\Delta$ has $t = 3$ distinct prime factors, there are at least $\ell = 2$ even invariant factors for $\mathcal{C}_\Delta$. So in fact $\mathcal{C}_\Delta$ must have invariant factor type (6, 2). We leave it for the reader to verify that the following are the reduced ideals of discriminant $-728$, partitioned into genera as noted, and that if $A = [3 : 1]$ and $B = [2 : 0]$, then the twelve elements of $\mathcal{C}_{-728}$ can each be expressed uniquely in the form $[A]^i \cdot [B]^j$ with $0 \le i < 6$ and $0 \le j < 2$.

$$\begin{array}{lcllll} +++ & : & [1:0] & [9:4] & [9:-4] \\ +-- & : & [6:2] & [6:-2] & [7:0] \\ -+- & : & [2:0] & [11:4] & [11:-4] \\ --+ & : & [3:1] & [3:-1] & [13:0] \end{array}$$

Specifically, the principal genus is $\{[D], [A]^2, [A]^4\}$, which is also the group of all squares in $\mathcal{C}_\Delta$. ◊

When $G = \mathcal{C}_\Delta$ is the ideal class group of a primitive discriminant $\Delta$, with $H = \mathcal{G}_\Delta$ the principal genus and $G^2$ the subgroup of squares of elements of $G$, we can reverse the containment shown above and thus show that $H = G^2$. Here we require the following result, which is proved in Appendix B.

**Legendre's Theorem.** *Let $a$, $b$, and $c$ be nonzero integers that are squarefree, pairwise relatively prime, and neither all positive nor all negative. Then $ax^2 + by^2 + cz^2 = 0$ has an integer solution $(x, y, z)$ with $\gcd(x, y, z) = 1$ if and only if the following three quadratic congruences each have solutions:*

$$x^2 \equiv -bc \pmod a, \quad x^2 \equiv -ac \pmod b, \quad x^2 \equiv -ab \pmod c. \tag{6.3.1}$$

Assuming Legendre's Theorem, we can prove the following claim.

**Lemma 6.3.6.** *Let $\Delta = \Delta(d, 1)$ be a primitive discriminant. Let $f$ be a quadratic form of discriminant $\Delta$, and let $A = A_f$ be its corresponding ideal. Then $[A]$ is in the principal genus $\mathcal{G}_\Delta$ if and only if $f$ represents some square that is relatively prime to $\Delta$.*

*Proof.* If $f$ represents $m^2$ with $\gcd(m^2, \Delta) = 1$, then $\left(\frac{f}{p}\right) = \left(\frac{m^2}{p}\right) = 1$ for every odd prime $p$ that divides $\Delta$. Since the product of all genus symbols equals 1, this shows that every defined genus symbol for $f$ is 1. So $[A]$, which has the same genus symbols as $f$, is in the principal genus $\mathcal{G}_\Delta$.

Conversely, suppose that $[A]$ is in $\mathcal{G}_\Delta$, which implies that each genus symbol of $f$ is 1. If $f(x, y) = ax^2 + bxy + cy^2$, we have that $f(q, r) = m^2$ if and only if $a(2m)^2 = (2aq + br)^2 - \Delta r^2$ by (4.1.2). We can assume that $a$ is squarefree by writing any square factor as part of the squared expression on the left-hand side of this equation. Letting $g = \gcd(a, d)$, and changing variables, we can rewrite this equation as

$$\frac{a}{g} \cdot x^2 + \frac{d}{g} \cdot y^2 - gz^2 = 0,$$

with the coefficients now squarefree and pairwise relatively prime. Legendre's Theorem implies that this equation has a solution if and only if the congruences of (6.3.1), which become

$$x^2 \equiv d \pmod{a/g}, \qquad x^2 \equiv a \pmod{d/g}, \qquad x^2 \equiv -\frac{ad}{g^2} \pmod{g},$$

all have solutions. If a prime $p$ divides $a$ but not $d$, the first congruence must hold so that $\mathcal{Q}_\Delta$ contains a quadratic form $(a : k)$. If $p$ divides $d$ but not $a$, the second congruence forces $\left(\frac{f}{p}\right) = \left(\frac{a}{p}\right)$ to equal 1. If $p$ divides both $a$ and $d$, then $-ad/g^2$ is congruent to a square multiple of $c$, so the third congruence forces $\left(\frac{f}{p}\right) = \left(\frac{c}{p}\right)$ to equal 1. So $f$ represents a square if and only if all genus symbols of $f$ equal 1, and so $[A]$ is in the principal genus. □

**Proposition 6.3.7.** *Let $\mathcal{C}_\Delta$ be the ideal class group of some primitive discriminant $\Delta$. If $[A]$ is in $\mathcal{G}_\Delta$, the principal genus of discriminant $\Delta$, then $[A] = [B]^2$ for some ideal class $[B]$ in $\mathcal{C}_\Delta$.*

*Proof.* Let $A = [a : k]$, so that $f = (a : k)$ is a quadratic form in $\mathcal{Q}_\Delta$ for which all defined genus symbols are 1. Then $f$ represents a square, say $f(q, r) = m^2$, by Lemma 6.3.6. We can assume that $\gcd(q, r) = 1$ since $f(gq, gr) = g^2 f(q, r)$. So there is a unimodular matrix $U$ with $q$ and $r$ as the entries of the first column of $U$. In that case, $f \circ U = g = (m^2 : \ell)$ for some $\ell$. Since $f$ is equivalent to $g$, we have that $A = A_f$ is equivalent to $A_g = [m^2 : \ell]$. But now $D = D_\Delta$ is a complete

quadratic domain, so that $A_g$ can be factored into prime ideals. In particular, we find that $A_g = B^2$, where $B = [m : \ell]$. So in $\mathcal{C}_\Delta$, we then have $[A] = [B]^2$. □

**Example.** Let $\Delta = -399 = -1 \cdot 3 \cdot 7 \cdot 19$. Since $\Delta$ has $t = 3$ prime factors, there are $\ell = t - 1 = 2$ even invariant factors for $\mathcal{C}_\Delta$. One can show that there are sixteen reduced ideals, which allows either $(8, 2)$ or $(4, 4)$ as the invariant factor type of $G = \mathcal{C}_{-399}$. But we find that if $A = [2 : 0]$, then $[A]$ has order eight in $G$, so that the invariant factor type must be $(8, 2)$. The distinct genera are

$$\begin{array}{lcllll} +++ & : & [1:0] & [4:0] & [4:-1] & [7:3] \\ +-- & : & [3:1] & [10:0] & [10:4] & [10:-5] \\ -+- & : & [2:0] & [2:-1] & [8:3] & [8:-4] \\ --+ & : & [5:0] & [5:-1] & [6:1] & [6:-2] \end{array}$$

with genus symbols in order as $\left(\frac{A}{3}\right)$, $\left(\frac{A}{7}\right)$, and $\left(\frac{A}{19}\right)$. ◊

**Exercise 6.3.1.** For each $\Delta$, list the distinct genera of ideals in the class group $\mathcal{C}_\Delta$, and determine the invariant factor type of that group. Verify that the principal genus $\mathcal{G}_\Delta$ is the same as the subgroup of squares of elements of $\mathcal{C}_\Delta$. (Many of these $\Delta$ values appear in Exercise 6.2.1.)

(a) $\Delta = -20$.

(b) $\Delta = -40$.

(c) $\Delta = -47$.

(d) $\Delta = -56$.

(e) $\Delta = -84$.

(f) $\Delta = -116$.

(g) $\Delta = -119$.

(h) $\Delta = -296$.

(i) $\Delta = -340$.

(j) $\Delta = -344$.

(k) $\Delta = -356$.

(l) $\Delta = -420$.

(m) $\Delta = -191$.

(n) $\Delta = -231$.

(o) $\Delta = -440$.

(p) $\Delta = -724$.

We conclude this section with a general consequence of our results.

**Corollary 6.3.8.** *Let $\Delta$ be a negative integer for which $D = D_\Delta$ is a complete quadratic domain, and let $\mathcal{C}_\Delta$ be the ideal class group of $D$. Then the number of elements in $\mathcal{C}_\Delta$ is odd if and only if $\Delta = -4$, $\Delta = -8$, or $\Delta = -p$ for some prime $p \equiv 3 \pmod 4$.*

*Proof.* Proposition 6.3.4 shows that it is for these values of $\Delta$ that $\mathcal{C}_\Delta$ contains $2^0 = 1$ genus. Then $\mathcal{C}_\Delta$ has invariant factor type $(n_1, n_2, \dots, n_m)$ with each $n_i$ odd, and so $|\mathcal{C}_\Delta| = n_1 n_2 \cdots n_m$ is odd. On the other hand, if $\mathcal{C}_\Delta$ contains $2^\ell$ genera with $\ell$ positive, then $\mathcal{C}_\Delta$ has invariant factor type $(n_1, n_2, \dots, n_m)$ with $n_1$ (at least) even. In that case $|\mathcal{C}_\Delta|$ is also even. □

## Class Groups of Negative Discriminant—Review

In this chapter, we demonstrated a systematic method of determining the class group of ideals, or of quadratic forms, of a fixed negative discriminant.

(1) For negative values of $\Delta$, we have a precisely defined collection of representatives of distinct classes (that is, *reduced* ideals or quadratic forms), which we can construct by a systematic process in practice.

(2) Using a combination of the ideal multiplication and reduction methods developed in previous chapters, we can generally determine the group structure (that is, *invariant factor type*) of a class group of negative discriminant.

(3) The relation of genus equivalence, which we can connect to squares of ideal classes, typically gives us additional restrictions on the possibilities for the structure of a class group.

In the next chapter, we will see that the invariant factor type of an ideal class group sometimes allows us to determine the integers that are represented by a particular quadratic form of a particular discriminant.

# 7

# Representations by Positive Definite Forms

This chapter may be viewed as the culmination of the first half of the text. We have seen how concepts concerning ideals and quadratic forms, such as equivalence and multiplication (or composition), come together with the definition of class groups of these objects. In Chapter 6, we developed a systematic method, for negative discriminants, of determining the structure of these groups. We will now see how these algebraic considerations can be applied to the type of arithmetic problems with which we began our study.

We will concentrate mainly on explaining results that we can illustrate using direct calculation. We begin in §7.1 with the simplest case—domains in which every ideal is a principal ideal, and representations of integers by a corresponding quadratic form. In §7.2, we generalize these results to situations that approximate principal ideal domains most closely, which we define as *principal square domains*. Here also we can give a complete description of which integers are represented by corresponding quadratic forms. We look at some examples of more general quadratic domains in §7.3, and will describe what we can and cannot say about representations by specific quadratic forms in this situation. Finally, we develop some methods of constructing representations of integers in practice, and will see in §7.4 that these calculations are obtained through the same reduction process that determines representatives of a class group.

## 7.1 Negative Discriminants with Trivial Class Groups

In §2.6, we claimed that there are only finitely many negative discriminants $\Delta$ for which $D = D_\Delta$ is a unique factorization domain, namely $\Delta = -3, -4, -7, -8, -11, -19, -43, -67$, and $-163$. We can make the following general statement about the number of distinct representations of a positive integer by the principal form of one of these discriminants.

**Theorem 7.1.1.** *Let $\Delta$ be a negative discriminant for which $D = D_\Delta$ is a unique factorization domain. Then a positive integer $a$ is properly represented by the principal form $\phi(x, y)$ if and only if*

$$a = p^e \cdot p_1^{e_1} \cdot p_2^{e_2} \cdots p_n^{e_n}, \tag{7.1.1}$$

*where $p$ is a prime number dividing $\Delta$, each $p_i$ is a prime number that splits in $D$, each $e_i$ is a positive integer, and $e = 0$ or $e = 1$. In this case, there are $2^n$ distinct $\phi$-equivalence classes of solutions.*

Note that the prime $p$ is uniquely determined by the values of $\Delta$ under consideration, since each one has only one prime divisor.

*Proof.* In Theorem 5.4.1, we saw that a quadratic domain $D$ is a unique factorization domain if and only if every ideal of $D$ is a principal ideal. In that case, the ideal class group of discriminant $D$ is trivial and there is a unique reduced quadratic form of discriminant $\Delta$, namely the principal form $\phi(x, y)$. Theorem 4.3.3 then implies that a positive integer $a$ is properly representated by $\phi(x, y)$ if and only if $\phi(x) \equiv 0 \pmod{a}$ has a solution, where $\phi(x) = \phi(x, 1)$ is the principal polynomial of discriminant $\Delta$. Results about quadratic congruences from §0.2 and §0.3 show that $\phi(x) \equiv 0 \pmod{a}$ has a solution precisely when $a$ has the form of equation (7.1.1), and has precisely $2^n$ solutions in that case. (See Theorem 0.3.4 and Corollary 0.3.3 in particular.) Finally, Theorem 4.3.6 implies that this is the same as the number of $\phi$-equivalence classes of solutions of $\phi(x, y) = a$. □

Theorem 1.6.2 is a consequence of this result, as is the following corollary, which we already noted in part as Exercise 2.5.4.

**Corollary 7.1.2.** *An integer $a$ is properly represented by $x^2 + 2y^2$ if and only if*

$$a = 2^e \cdot p_1^{e_1} \cdot p_2^{e_2} \cdots p_n^{e_n}, \tag{7.1.2}$$

*with each $p_i$ a distinct prime congruent to 1 or 3 modulo 8, each $e_i$ a positive integer, and $e$ is either 0 or 1. If $a > 2$, then the number of proper representations of $a$ as $x^2 + 2y^2$ with $x$ and $y$ both positive is $2^{n-1}$.*

Table 7.1. Proper Representations by $x^2 + 2y^2$

| $y\backslash x$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | | 1 | | | | | | | | | | | |
| 1 | 2 | 3 | 6 | 11 | 18 | 27 | 38 | 51 | 66 | 83 | 102 | 123 | 146 |
| 2 | | 9 | | 17 | | 33 | | 57 | | 89 | | 129 | |
| 3 | | 19 | 22 | | 34 | 43 | | 67 | 82 | | 118 | 139 | |
| 4 | | 33 | | 41 | | 57 | | 81 | | 113 | | | |
| 5 | | 51 | 54 | 59 | 66 | | 86 | 99 | 114 | 131 | | | |
| 6 | | 73 | | | | 97 | | 121 | | | | | |
| 7 | | 99 | 102 | 107 | 114 | 123 | 134 | | | | | | |
| 8 | | 129 | | 137 | | | | | | | | | |

**Exercise 7.1.1.** Table 7.1 lists all proper representations of $a < 150$ by $x^2 + 2y^2$. Verify that the prime factorization of each $a$ that appears in this table and the number of such representations are as claimed in Corollary 7.1.2.

*Proof.* Note that $\phi(x, y) = x^2+2y^2$ is the principal form of discriminant $\Delta = -8$. Here $p = 2$ is the only prime dividing $\Delta$, and an odd prime splits in $D_{-8}$ if and only if $\left(\frac{-8}{p}\right) = 1$. We find that $\left(\frac{-8}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = 1$ if and only if $p \equiv 1 \pmod 8$ (so that $\left(\frac{-1}{p}\right) = 1 = \left(\frac{2}{p}\right)$) or $p \equiv 3 \pmod 8$ (with $\left(\frac{-1}{p}\right) = -1 = \left(\frac{2}{p}\right)$). The identity matrix and its negative are the only automorphs of $\phi(x, y)$ (see Theorem 6.1.4), hence each $(q, r)$ is $\phi$-equivalent only to itself and $(-q, -r)$. If $a > 2$, then each solution $k$ of $x^2 + 2 \equiv 0 \pmod a$ has an incongruent conjugate solution, $-k$, and we find that if $k$ corresponds to a solution $(q, r)$ of $\phi(x, y) = a$, then $-k$ corresponds to the class of $(q, -r)$. Thus if we restrict our attention to solutions of $x^2 + 2y^2 = a$ with $x$ and $y$ both positive, we obtain $2^{n-1}$ distinct solutions. □

For a composite value of $a$, we can use formulas for composition of quadratic forms to describe solutions of $x^2 + y^2 = a$.

**Corollary 7.1.3.** *If $q^2 + 2r^2 = m$ and $s^2 + 2t^2 = n$ with $q$, $r$, $s$, and $t$ positive and $\gcd(q, r) = 1 = \gcd(s, t)$, then solutions of $x^2 + 2y^2 = mn$ in positive integers are given by $(x, y) = (|qs - 2rt|, |qt + rs|)$ and $(x, y) = (|qs + 2rt|, |qt - rs|)$.*

*Proof.* Here $\phi(x, y) = x^2 - 2y^2$ is the principal form of discriminant $\Delta = -8$. Since we have $\phi(q, r) = m = \phi(q, -r)$ and $\phi(s, t) = n$, the expressions for solutions of $\phi(x, y) = mn$ follow immediately from Proposition 5.3.1. □

**Example.** Using Table 7.1, we see that if $q = 3$, $r = 2$, $s = 3$, and $t = 4$, then $\phi(q, r) = 17$ and $\phi(s, t) = 41$. Here $|qs - 2rt| = 7$, $|qt + rs| = 18$, $|qs + 2rt| = 25$, and $|qt - rs| = 6$. We can verify that $\phi(7, 18) = 17 \cdot 41 = 697 = \phi(25, 6)$. ◊

Table 7.2. Proper Representations by $x^2 + 3y^2$

| $y\backslash x$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | | 1 | | | | | | | | | | | |
| 1 | 3 | 4 | 7 | 12 | 19 | 28 | 39 | 52 | 67 | 84 | 103 | 124 | 147 |
| 2 | | 13 | | 21 | | 37 | | 61 | | 93 | | 133 | |
| 3 | | 28 | 31 | | 43 | 52 | | 76 | 91 | | 127 | 148 | |
| 4 | | 49 | | 57 | | 73 | | 97 | | 129 | | | |
| 5 | | 76 | 79 | 84 | 91 | | 111 | 124 | 139 | | | | |
| 6 | | 109 | | | | 133 | | | | | | | |
| 7 | | 148 | | | | | | | | | | | |

**Exercise 7.1.2.** For each of the following values of $a$, use Corollary 7.1.3 to list all the solutions of $x^2 + 2y^2 = a$ in positive integers $x$ and $y$.

(a) $a = 209 = 11 \cdot 19$.

(b) $a = 779 = 19 \cdot 41$.

(c) $a = 1763 = 41 \cdot 43$.

(d) $a = 5289 = 3 \cdot 41 \cdot 43$.

Theorem 7.1.1 applies to the discriminant $\Delta = -3$, for which the principal form is $\phi(x, y) = x^2 + xy + y^2$. For our next example, we will consider representations by the related form $f(x, y) = x^2 + 3y^2$, stating our main result as follows.

**Proposition 7.1.4.** *An integer $a$ is properly represented by $x^2 + 3y^2$ if and only if*

$$a = 2^e \cdot 3^{e_0} \cdot p_1^{e_1} \cdot p_2^{e_2} \cdots p_n^{e_n}, \tag{7.1.3}$$

*with each $p_i$ a distinct prime congruent to 1 modulo 3 and each $e_i$ a positive integer for $1 \le i \le n$, and with $e$ either 0 or 2 and $e_0$ either 0 or 1.*

**Exercise 7.1.3.** Table 7.2 lists all proper representations of $a < 150$ by $x^2 + 3y^2$. Verify that the prime factorization of each $a$ that appears in this table is as claimed in Proposition 7.1.4.

*Proof.* The discriminant of $f(x, y) = x^2 + 3y^2$ is $\Delta = \Delta(-3, 2) = -12$, so that $\phi(x) = x^2 + 2x + 4$ is the principal polynomial of discriminant $\Delta$. It follows that an integer $a$ is properly represented by some form of discriminant $\Delta$ if and only if $\phi(x) \equiv 0 \pmod{a}$ has a solution. Applying Theorem 0.3.4 and other properties of quadratic congruences, we find that this is the case if and only if $a$ is not divisible by 8, by 9, or by an odd prime $p \equiv 2 \pmod 3$. With $u_\Delta = \left\lfloor \sqrt{12/3} \right\rfloor = 2$, there are two reduced forms of discriminant $-12$, namely $(1 : -1) = x^2 + 3y^2$

and $(2 : 0) = 2x^2+2xy+2y^2$, so such an $a$ is properly represented by one of these forms. Since a square is congruent to 0 or 1 modulo 4, we find that $x^2+3y^2$ is odd if $x$ and $y$ have opposite parity, or divisible by 4 if $x$ and $y$ are both odd. On the other hand, since $x^2+xy+y^2$ is odd when $\gcd(x,y) = 1$, proper representations by $g(x,y)$ must be congruent to 2 modulo 4. So $a$ is properly represented by $x^2+3y^2$ if and only if $a$ is in the form of equation (7.1.3). □

Note that the ideal class group of discriminant $\Delta_1 = -12$ is trivial, but that $D_{-12}$ is not a principal ideal domain.

**Exercise 7.1.4.** Suppose that the prime factorization of some $a > 3$ is as given in equation (7.1.3). Show that the number of solutions of $x^2+3y^2 = a$ with $\gcd(x,y) = 1$ and with $x$ and $y$ both positive is $2^{n-1}$ if $e = 0$ and is $2^n$ if $e = 2$.

**Exercise 7.1.5.** Let $f(x,y) = x^2+3y^2$. Use Theorem 5.3.3 (or direct calculation) to show that if $f(q,r) = m$ and $f(s,t) = n$, then $f(u,v) = mn$ for $u = qs-3rt$ and $v = qt+rs$. Use this fact to find all solutions of $x^2+3y^2 = a$ in positive integers $x$ and $y$ for the following values of $a$.

(a) $a = 247 = 13 \cdot 19$.

(b) $a = 589 = 19 \cdot 31$.

(c) $a = 1591 = 37 \cdot 43$.

The following proposition presents a similar result for $x^2+7y^2$. Again, this form is related to a principal form, $\phi(x,y) = x^2+xy+2y^2$, the only reduced form of discriminant $\Delta = \Delta(-7,1) = -7$.

**Proposition 7.1.5.** *An integer $a$ is properly represented by $x^2+7y^2$ if and only if*

$$a = 2^e \cdot 7^{e_0} \cdot p_1^{e_1} \cdot p_2^{e_2} \cdots p_n^{e_n}, \tag{7.1.4}$$

*with each $p_i$ a distinct prime congruent to 1, 2, or 4 modulo 7 and each $e_i$ a positive integer for $1 \le i \le n$, and with $e = 0$ or $e \ge 3$, and $e_0$ either 0 or 1.*

**Exercise 7.1.6.** Table 7.3 lists all proper representations of $a < 150$ by $x^2+7y^2$. Verify that the prime factorization of each $a$ that appears in this table is as claimed in Proposition 7.1.5.

*Proof.* The principal polynomial of discriminant $\Delta = \Delta(-7,2) = -28$ is $\phi(x) = x^2+2x+8$, and there are two reduced forms with discriminant $\Delta$, namely $f = (1 : -1) = x^2+7y^2$ and $g = (2 : 0) = 2x^2+2xy+4y^2$. A positive integer $a$ is properly represented by one of these forms if and only if $\phi(x) \equiv 0 \pmod{a}$ has a solution. Here we find that solutions exist if and only if $a$ is not divisible

Table 7.3. Proper Representations by $x^2 + 7y^2$

| $y\backslash x$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | | 1 | | | | | | | | | | |
| 1 | 7 | 8 | 11 | 16 | 23 | 32 | 43 | 56 | 71 | 88 | 107 | 128 |
| 2 | | 29 | | 37 | | 53 | | 77 | | 109 | | 149 |
| 3 | | 64 | 67 | | 79 | 88 | | 112 | 127 | | | |
| 4 | | 113 | | 121 | | 137 | | | | | | |

by 49 or by a prime $p \equiv 3, 5,$ or $6 \pmod 7$. If such an $a$ is odd, then $a$ cannot be represented by $g$, so must be represented by $f$. On the other hand, if $a$ is even but not divisible by 8, then $a$ cannot be represented by $f$. (The square of an odd integer is congruent to 1 modulo 8. A proper representation by $x^2 + 7y^2$ is even if and only if $x$ and $y$ are both odd, in which case 8 divides $x^2 + 7y^2$.) It remains to consider values of $a$ divisible by 8, which might be represented either by $f$ or by $g$.

In fact, if $a$ is divisible by 8, and $x^2 + 2x + 8 \equiv 0 \pmod a$ has a solution $k$, we can see as follows that $a$ is properly represented by both $f$ and $g$. If $\phi(k) = ac$ and $\phi'(k) = 2k + 2 = b$, then $(a : k) = ax^2 + bxy + cy^2$ is a quadratic form of discriminant $\Delta = -28$. With $a$ even, we see that $k$ is even and so $b \equiv 2 \pmod 4$. But now if $k_1 = k + \frac{a}{2}$, we find that

$$\phi(k_1) = \left(k + \frac{a}{2}\right)^2 + 2\left(k + \frac{a}{2}\right) + 8 = a\left(c + k + 1 + \frac{a}{4}\right).$$

If 4 divides $a$, it follows that $(a : k + \frac{a}{2})$ is a quadratic form of discriminant $\Delta = -28$, which can also be expressed as $ax^2 + (b + a)xy + \left(c + \frac{b}{2} + \frac{a}{4}\right)y^2$. If 8 divides $a$, so that $\frac{a}{4}$ is even and $\frac{b}{2}$ is odd, then $c$ and $c + \frac{b}{2} + \frac{a}{4}$ must have opposite parity, while $b$ and $b + a$ are both even. So we see in this case that $a$ is properly represented by one primitive form and one form of index two. Since equivalent quadratic forms have the same index (Corollary 4.3.2), it follows that $a$ is represented both by $x^2 + 7y^2$ and by $2x^2 + 2xy + 4y^2$. In particular, $a$ is properly represented by $x^2 + 7y^2$ if and only if $a$ is as given by equation (7.1.4). □

**Exercise 7.1.7.** Let $a > 7$ be given as in equation (7.1.4). Show that the number of solutions of $x^2 + 7y^2 = a$ with $\gcd(x, y) = 1$ and with $x$ and $y$ both positive is $2^{n-1}$ if $e = 0$, and is $2^n$ if $e \geq 3$.

**Exercise 7.1.8.** Let $f(x, y) = x^2 + 7y^2$. Show that if $f(q, r) = m$ and $f(s, t) = n$, then $f(u, v) = mn$ for $u = qs - 7rt$ and $v = qt + rs$. For each of the following values of $a$, use this fact to list all proper representations of $a$ by $x^2 + 7y^2$.

(a) $m = 253 = 11 \cdot 23$.

(b) $m = 368 = 2^4 \cdot 23$.

(c) $m = 407 = 11 \cdot 37$.

(d) $m = 781 = 11 \cdot 71$.

(e) $m = 7337 = 11 \cdot 23 \cdot 29$.

We conclude this section with a different type of consequence of a trivial class group.

**Example.** Let $\phi(x) = x^2 + x + 41$, the principal polynomial of discriminant $\Delta = -163$. In the following table, we calculate $\phi(x)$ for $0 \le x \le 6$.

| $x$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| $\phi(x)$ | 41 | 43 | 47 | 53 | 61 | 71 | 83 |

All values of $\phi(x)$ listed so far are prime. In fact, that statement would still be true if we extended this table to $x \le 10$, or $x \le 20$, or $x \le 30$. Perhaps one might even be led to conjecture that $x^2 + x + 41$ is prime for all integers $x$. But a moment's reflection will show that, for instance, $\phi(41)$ is divisible by 41, and so must be composite. The numerical oddity of this long sequence of primes taken on by $\phi(x)$ is often used as an illustration that even a considerable pattern of examples established by computation might be misleading in its apparent implications.

Here we can argue that this property of $\phi(x)$ is not as surprising as it first appears. If $\Delta = -163$, then $u_\Delta = \left\lfloor \sqrt{163/3} \right\rfloor = 7$, so the table above is sufficient to show that $(1 : 0)$ is the only reduced quadratic form of this discriminant. (We could draw the same conclusion with fewer calculations using $-3 \le x \le 3$, as we have done in similar examples previously.) Now Theorem 4.3.3 implies that a prime number $p$ is represented by the principal form $\phi(x, y) = x^2 + xy + 41y^2$ if and only if $x^2 + x + 41 \equiv 0 \pmod{p}$ has a solution. But $\phi(x, y) \ge 41$ if $y \ne 0$, thus $x^2 + x + 41 \equiv 0 \pmod{p}$ cannot have a solution when $p < 41$.

Now notice that $\phi(x) = x^2 + x + 41 < 41^2$ if $0 \le x \le 39$. If any of those $\phi(x)$ values were composite, then it would have a prime divisor $p < 41$. But in that case, $\phi(x) \equiv 0 \pmod{p}$ would have a solution, contrary to what we established above. Thus we must conclude, without direct primality testing, that $\phi(x)$ is prime at least for $0 \le x \le 39$. (In fact, $\phi(40) = 41^2$ is the first composite value of $\phi(x)$.) We are forced to this conclusion by the fact that $\phi(x)$ is prime for $-3 \le x \le 3$, which of course seems far less improbable. ◊

**Exercise 7.1.9.** Show that $x^2 + x + 17$ is prime for all integers $0 \le x \le 15$. (Hint: Show that there is only one reduced quadratic form of discriminant $\Delta = -67$.)

## 7.2 Principal Square Domains

In §5.4, we stated that we might view the ideal class group of a quadratic domain $D$ as a measure of how far $D$ is from having unique factorization. In this section,

we introduce what we might view as our closest approximation to a unique factorization domain. We restrict our attention to *complete* quadratic domains $D$, so that the ideal class group of $D$ contains representatives of all nontrivial ideals of $D$. We saw in §7.1 that if the ideal class group of a quadratic domain $D_\Delta$ is trivial, we can obtain a complete characterization of the integers properly represented by the principal form of discriminant $\Delta$. We will find that a similar characterization exists for the quadratic domains defined by the following proposition.

**Proposition 7.2.1.** *Let $D$ be a complete quadratic domain, that is, the domain of quadratic integers in $\mathbb{Q}(\sqrt{d})$ for some squarefree $d \neq 1$. Then the following properties of $D$ are equivalent.*

(1) *The square of every ideal of $D$ is a principal ideal.*

(2) *The ideal class group $\mathcal{C}_\Delta$ of $D$ has invariant factor type $(2, 2, \dots, 2)$.*

(3) *Every genus of $D$ contains exactly one class.*

(4) *The principal genus of $D$ is $\{[D]\}$.*

**Definition.** If the properties of Proposition 7.2.1 hold for a complete quadratic domain $D$, so that $\mathcal{C}_\Delta$ has invariant factor type $(2, 2, \dots, 2)$ with $\ell$ terms of 2, we say that $D$ is a *principal square domain* of type $\ell$. We allow the possibility that $\ell = 0$, in which case $\mathcal{C}_\Delta$ is trivial. A principal square domain of type $\ell = 0$ is the same as a principal ideal domain.

*Proof.* Let $D = D_\Delta$ be a complete quadratic domain.

(1) $\Rightarrow$ (2): Suppose that $\mathcal{C}_\Delta$ has invariant factor type $(n_1, n_2, \dots, n_m)$, with $[A_1], [A_2], \dots, [A_m]$ as generators. If the square of every ideal is principal, then

$$[A_1]^2 \cdot [A_2]^0 \cdots [A_m]^0 = [A_1^2] = [D] = [A_1]^0 \cdot [A_2]^0 \cdots [A_m]^0.$$

By definition of the invariant factors, then $2 \equiv 0 \pmod{n_1}$, so that $n_1 = 1$ or 2. Since $n_{i+1}$ divides $n_i$ for $1 \leq i < m$, statement (2) follows immediately.

(2) $\Rightarrow$ (3): Suppose that $G = \mathcal{C}_\Delta$ has invariant factor type $(2, 2, \dots, 2)$ with $\ell \geq 0$ terms of 2. Proposition 6.3.5 shows that $G^2$ has only one element, and by Propositions 6.3.3 and 6.3.7, we know that $G^2$ is the same as the principal genus $\mathcal{G}_\Delta$. Since each genus contains the same number of classes, then each genus contains exactly one class of ideals.

(3) $\Rightarrow$ (4): The principal genus of $D$ always contains the ideal class $[D]$. So if each genus has only one class, then the principal genus is $\{[D]\}$.

(4) $\Rightarrow$ (1): The square of every ideal class is in the principal genus by Proposition 6.3.3. If the principal genus is $\{[D]\}$, then the square of every ideal is equiv-

alent to $D$. But then the square of every nontrivial ideal is a principal ideal by Proposition 5.1.2.

Thus properties (1)–(4) are equivalent. □

**Proposition 7.2.2.** *Let $D$ be a principal square domain. If $A$ and $B$ are nontrivial ideals of $D$, then $A$ and $B$ are equivalent if and only if $A$ and $B$ have the same collection of genus symbols. In particular, $A$ is a principal ideal if and only if each of its genus symbols equals* 1.

*Proof.* In a principal square domain, each genus contains only one class of ideals. So $A$ and $B$ are equivalent if and only if $A$ and $B$ are genus equivalent. In particular, $A$ is principal, so that $A \sim D$, if and only if $A$ is in the principal genus of $D$. □

If $D = D_\Delta$ is a principal square domain, we can also say that quadratic forms $f$ and $g$ in $\mathcal{Q}_\Delta$ are equivalent if and only if they have the same collection of genus symbols. In this case, we can describe in full the integers $m$ properly represented by various quadratic forms of discriminant $\Delta$, and we can use equivalence of ideals to calculate solutions of $f(x, y) = m$ when they exist. We will demonstrate our results with examples that are representative of more general cases, and that we can illustrate with direct calculations.

**A Principal Square Domain of Type One.** Let $\Delta = -24$, so that $\phi(x) = x^2 + 6$ is the principal polynomial of discriminant $\Delta$. With $u_\Delta = \left\lfloor \sqrt{24/3} \right\rfloor = 2$, and $\phi(0) = 6$ and $\phi(1) = 7$, we find that there are two reduced quadratic forms of discriminant $\Delta$:

$$f(x, y) = (1 : 0) = x^2 + 6y^2 \qquad \text{and} \qquad g(x, y) = (2 : 0) = 2x^2 + 3y^2.$$

The following proposition classifies all positive integers represented by one of these forms. Recall that $a$ is the *squarefree part* of $m$ if $a = m/r^2$ with $r^2$ the largest square dividing $m$.

**Proposition 7.2.3.** *A positive integer $m$ is properly represented either by $f(x, y) = x^2 + 6y^2$ or by $g(x, y) = 2x^2 + 3y^2$ if and only if $m$ is not divisible by* 4*, by* 9*, or by any prime $p$ congruent to* 13*,* 17*,* 19*, or* 23 *modulo* 24*. Assuming that this is the case, let $a$ be the squarefree part of $m$, and let $t$ be the number of primes $p$ dividing $a$ for which $p =$ 2*, $p =$ 3*, or $p$ is congruent to* 5 *or* 11 *modulo* 24*. Then $m$ is properly represented by $f$ if $t$ is even, and is properly represented by $g$ if $t$ is odd.*

**Exercise 7.2.1.** Table 7.4 lists integers $m < 150$ that are properly represented by $f(x, y) = x^2 + 6y^2$ or $g(x, y) = 2x^2 + 3y^2$. For each one, verify the claim of Proposition 7.2.3.

**Exercise 7.2.2.** Let $p > 3$ be a prime number.

(a) Show that $\left(\frac{2}{p}\right) = 1 = \left(\frac{p}{3}\right)$ if and only if $p \equiv 1$ or $7 \pmod{24}$.

(b) Show that $\left(\frac{2}{p}\right) = -1 = \left(\frac{p}{3}\right)$ if and only if $p \equiv 5$ or $11 \pmod{24}$.

(c) Show that $\left(\frac{2}{p}\right) \neq \left(\frac{p}{3}\right)$ if and only if $p \equiv 13, 17, 19$, or $23 \pmod{24}$.

Table 7.4. Representations by Forms of Discriminant $\Delta = -24$

$x^2 + 6y^2$

| $y\backslash x$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | | 1 | | | | | | | | | | |
| 1 | 6 | 7 | 10 | 15 | 22 | 31 | 42 | 55 | 70 | 87 | 106 | 127 |
| 2 | | 25 | | 33 | | 49 | | 73 | | 105 | | 145 |
| 3 | | 55 | 58 | | 70 | 79 | | 103 | 118 | | | |
| 4 | | 97 | | 105 | | 121 | | 145 | | | | |

$2x^2 + 3y^2$

| $y\backslash x$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| 0 | | 2 | | | | | | | |
| 1 | 3 | 5 | 11 | 21 | 35 | 53 | 75 | 101 | 131 |
| 2 | | 14 | | 30 | | 62 | | 110 | |
| 3 | | 29 | 35 | | 59 | 77 | | 125 | |
| 4 | | 50 | | 66 | | 98 | | 146 | |
| 5 | | 77 | 83 | 93 | 107 | | 147 | | |
| 6 | | 110 | | | | | | | |
| 7 | | 149 | | | | | | | |

*Proof.* An integer $m$ is properly represented by some form of discriminant $\Delta = -24$ if and only if the congruence $\phi(x) \equiv 0 \pmod{m}$ has a solution. For a prime $p > 3$, Exercise 7.2.2 shows that this is the case if and only if $p$ is congruent to 1, 5, 7, or 11 modulo 24. For $p = 2$ and $p = 3$, we find that $\phi(x) \equiv 0 \pmod{p}$ has a solution, but $\phi(x) \equiv 0 \pmod{p^2}$ does not. Thus we obtain the necessary and sufficient conditions on $m$ noted above.

The ideal class group of discriminant $\Delta = -24$ contains two elements, with representatives $D = [1 : 0]$ and $P = [2 : 0]$. Therefore, $\mathcal{C}_\Delta$ has invariant factor type (2), that is, $D = D_{-24}$ is a principal square domain of type one. The genus symbols defined for an ideal $A$ of $D$ are $\left(\frac{2}{A}\right)$ and $\left(\frac{A}{3}\right)$, and by Proposition 7.2.2, $A \sim D$ if $\left(\frac{2}{A}\right) = 1 = \left(\frac{A}{3}\right)$ while $A \sim P$ if $\left(\frac{2}{A}\right) = -1 = \left(\frac{A}{3}\right)$. If $A$ is a primitive

prime ideal with norm $p > 3$, Exercise 7.2.2 implies that the first case occurs if $p \equiv 1$ or $7 \pmod{24}$, and the second case occurs if $p \equiv 5$ or $11 \pmod{24}$. The prime ideals of norm 2 and 3 are equivalent to $P$ as well.

Now let $m$ be a positive integer for which $\phi(x) \equiv 0 \pmod{m}$ has a solution, say $\ell$. Let $m = ar^2$ with $a$ squarefree, and write $a = p_1 \cdots p_t \cdot q_1 \cdots q_s$, where $p_i = 2$, $p_i = 3$, or $p_i \equiv 5$ or $11 \pmod{24}$ for $1 \le i \le t$, and $q_i \equiv 1$ or $7 \pmod{24}$ for $1 \le i \le s$. Then $A = [m : \ell]$ is a primitive ideal of $D$, which we can write as $A = P_1 \cdots P_t \cdot Q_1 \cdots Q_s \cdot R^2$, with each $P_i = [p_i : \ell]$, each $Q_i = [q_i : \ell]$, and $R = [r : \ell]$. In the ideal class group $G = \mathcal{C}_{-24}$, we have $[R]^2 = [D]$ (since $G$ has order two), each $[Q_i] = [D]$, and each $[P_i] = [P]$, so that $[A] = [P]^t$. If $t$ is even, then $A \sim D$, or equivalently $(m : \ell) \sim (1 : 0)$, which implies that $m$ is properly represented by $f(x, y) = x^2 + 6y^2$ by Theorem 4.3.6. If $t$ is odd, then $A \sim P$ and $(m : \ell) \sim (2 : 0)$, so that $m$ is properly represented by $g(x, y) = 2x^2 + 3y^2$. □

**Exercise 7.2.3.** For each of the following values of $m$, indicate whether $m$ is represented by $f(x, y) = x^2+6y^2$, by $g(x, y) = 2x^2+3y^2$, or by neither form. Find all representations of $m$ in positive integers by $f$ or by $g$, if those representations exist. (Here $m$ is prime unless it is expressed as a product.)

(a) $m = 223$.

(b) $m = 227$.

(c) $m = 341 = 11 \cdot 31$.

(d) $m = 354 = 2 \cdot 3 \cdot 59$.

(e) $m = 409$.

(f) $m = 1015 = 5 \cdot 7 \cdot 29$.

**Exercise 7.2.4.** Let $D = D_{-20}$. Show that $D$ is a principal square domain of type one. Show that a positive integer $m$ is properly represented by either $f(x, y) = x^2 + 5y^2$ or $g(x, y) = 2x^2 + 2xy + 3y^2$ if and only if $m$ is not divisible by 4, by 25, or by a prime $p$ congruent to 11, 13, 17, or 19 modulo 20. If $m$ is a positive integer with this property, find necessary and sufficient conditions for a positive integer $m$ to be properly represented by $f(x, y) = x^2+5y^2$ or by $g(x, y) = 2x^2+2xy+3y^2$.

**Exercise 7.2.5.** Show that $D_{-40}$ is a principal square domain of type one. Find necessary and sufficient conditions for a positive integer $m$ to be properly represented by $f(x, y) = x^2 + 10y^2$ or by $g(x, y) = 2x^2 + 5y^2$. Verify your result for all integers $m < 100$.

Table 7.5. Representations by Forms of Discriminant $\Delta = -120$

$x^2 + 30y^2$

| $y\backslash x$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | | 1 | | | | | | | | | |
| 1 | 30 | 31 | 34 | 39 | 46 | 55 | 66 | 79 | 94 | 111 | 130 |
| 2 | | 121 | | 129 | | 145 | | | | | |

$2x^2 + 15y^2$

| $y\backslash x$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| 0 | | 2 | | | | | | | |
| 1 | 15 | 17 | 23 | 33 | 47 | 65 | 87 | 113 | 143 |
| 2 | | 62 | | 78 | | 110 | | | |
| 3 | | 137 | 143 | | | | | | |

$3x^2 + 10y^2$

| $y\backslash x$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0 | | 3 | | | | | |
| 1 | 10 | 13 | 22 | 37 | 58 | 85 | 118 |
| 2 | | 43 | | 67 | | 115 | |
| 3 | | 93 | 102 | | 138 | | |

$5x^2 + 6y^2$

| $y\backslash x$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | | 5 | | | | |
| 1 | 6 | 11 | 26 | 51 | 86 | 131 |
| 2 | | 29 | | 69 | | 149 |
| 3 | | 59 | 74 | | 134 | |
| 4 | | 101 | | 141 | | |

**A Principal Square Domain of Type Two.** Let $\Delta = -120$, so that $\phi(x) = x^2 + 30$ and $u_\Delta = \left\lfloor \sqrt{120/3} \right\rfloor = 6$. Using the following table,

| $x$ | 0 | $\pm 1$ | $\pm 2$ | $\pm 3$ |
|---|---|---|---|---|
| $\phi(x)$ | 30 | 31 | 34 | 39 |

we find that there are four reduced quadratic forms of discriminant $\Delta$:

$$\phi = (1 : 0), \qquad f = (2 : 0), \qquad g = (3 : 0), \qquad h = (5 : 0).$$

In Table 7.5, we compile proper representations of integers $m < 150$ by these forms. We classify the integers properly represented by one of these forms in the following proposition.

**Proposition 7.2.4.** *A positive integer $m$ is properly represented by a quadratic form of discriminant $\Delta = -120$ if and only if $m$ is not divisible by 4, by 9, by 25, or by*

*any prime $p > 5$ for which $\left(\frac{-30}{p}\right) = -1$. Assuming that this is the case, let $a$ be the squarefree part of $m$, let $r$ be the number of prime divisors $p$ of $a$ for which $p = 2$ or $p$ is congruent to 17, 23, 47, or 113 modulo 120, let $s$ be the number of those divisors for which $p = 3$ or $p$ is congruent to 13, 37, 43, or 67 modulo 120, and let $t$ be the number for which $p = 5$ or $p$ is congruent to 11, 29, 59, or 101 modulo 120. Then*

(1) *$\phi(x, y) = x^2 + 30y^2$ properly represents $m$ if $r$, $s$, and $t$ are all even or all odd,*

(2) *$f(x, y) = 2x^2 + 15y^2$ properly represents $m$ if $r$ has the opposite parity from $s$ and $t$,*

(3) *$g(x, y) = 3x^2 + 10y^2$ properly represents $m$ if $s$ has the opposite parity from $r$ and $t$,*

(4) *$h(x, y) = 5x^2 + 6y^2$ properly represents $m$ if $t$ has the opposite parity from $r$ and $s$.*

**Exercise 7.2.6.** Let $p > 5$ be a prime number.

(a) Show that $\left(\frac{2}{p}\right) = 1$, $\left(\frac{p}{3}\right) = 1$, and $\left(\frac{p}{5}\right) = 1$ if and only if $p \equiv 1, 31, 49, 79 \pmod{120}$.

(b) Show that $\left(\frac{2}{p}\right) = 1$, $\left(\frac{p}{3}\right) = -1$, and $\left(\frac{p}{5}\right) = -1$ if and only if $p \equiv 17, 23, 47, 113 \pmod{120}$

(c) Show that $\left(\frac{2}{p}\right) = -1$, $\left(\frac{p}{3}\right) = 1$, and $\left(\frac{p}{5}\right) = -1$ if and only if $p \equiv 13, 37, 43, 67 \pmod{120}$.

(d) Show that $\left(\frac{2}{p}\right) = -1$, $\left(\frac{p}{3}\right) = -1$, and $\left(\frac{p}{5}\right) = 1$ if and only if $p \equiv 11, 29, 59, 101 \pmod{120}$.

**Example.** If $m = 141 = 3 \cdot 47$, we have that $r = 1$, $s = 1$, and $t = 0$. Since $t$ has the opposite parity of $r$ and $s$, Proposition 7.2.4 implies that $m$ is properly represented by $5x^2 + 6y^2$, as we can verify from Table 7.5. ♢

**Exercise 7.2.7.** Verify that each of the integers listed in Table 7.5 satisfies the condition noted in Proposition 7.2.4 for representation of an integer by the appropriate form of discriminant $\Delta = -120$.

*Proof.* The conditions noted on $m$ ensure that $\phi(x) \equiv 0 \pmod{m}$ has a solution, so that $m$ is properly represented by one of the reduced quadratic forms of discriminant $\Delta = -120$. The ideal class group of discriminant $\Delta$ contains four

elements, with representatives $D = [1 : 0]$, $R = [2 : 0]$, $S = [3 : 0]$, and $T = [5 : 0]$. Since each of these ideals is its own conjugate, we see that $\mathcal{C}_\Delta$ has invariant factor type $(2, 2)$, that is, $D = D_{-120}$ is a principal square domain of type $\ell = 2$. Equivalence of an ideal $A$ to one of these forms is determined by the genus symbols $\left(\frac{2}{A}\right)$, $\left(\frac{A}{3}\right)$, and $\left(\frac{A}{5}\right)$. If $A$ is a primitive prime ideal with norm $p > 5$, then the equivalence of $A$ to $D$, $P$, $Q$, or $R$ is determined by $p$ modulo 120, as in Exercise 7.2.6.

Let $m$ be a positive integer for which $\phi(x) \equiv 0 \pmod{m}$ has a solution $\ell$, and let $A = [m : \ell]$. If $r$, $s$, and $t$ are defined as above, we find that $[A] = [R]^r \cdot [S]^s \cdot [T]^t$ in the ideal class group $\mathcal{C}_{-120}$. Since the square of each class equals $[D]$, one can verify that $[A]$ equals $[D]$, $[R]$, $[S]$, or $[T]$ as in cases (1)–(4) listed. For instance, if $r$ and $t$ are odd but $s$ is even, then $[A] = [R] \cdot [T]$. Here $[2 : 0] \cdot [5 : 0] = [10 : 0] \sim [3 : 0]$, so that $[A] = [S]$. The conclusions about representations of $m$ by $\phi$, $f$, $g$, or $h$ follow. □

**Exercise 7.2.8.** Show that $D_{-84}$ is a principal square domain of type two. List the reduced quadratic forms of discriminant $\Delta = -84$, and find necessary and sufficient conditions for a positive integer $m$ to be properly represented by one of those forms.

**Exercise 7.2.9.** Show that $D_{-420}$ is a principal square domain of type three. List the reduced quadratic forms of discriminant $\Delta = -420$. Find a necessary and sufficient condition for $m$ to be properly represented by $f(x, y) = 7x^2 + 15y^2$.

## 7.3 Quadratic Domains that Are Not Principal Square Domains

In the preceding sections of this chapter, we have demonstrated that when the ideal class group of a complete quadratic domain $D_\Delta$ has invariant factor type $(2, 2, \ldots, 2)$ (including the case in which this group is trivial), then we can completely classify the integers that are properly represented by one of the reduced quadratic forms of discriminant $\Delta$. But we found in Chapter 6 that the class group $\mathcal{C}_\Delta$ may have many different invariant factor types when $\Delta$ is negative. In this section, we will investigate the conclusions that we can draw about the existence of representations by positive definite quadratic forms with arbitrary discriminant values. We will concentrate on statements we can make about forms $ax^2 + cy^2$ (where it is easier to illustrate results numerically), and will not attempt to give complete classifications of all integers represented by one of these forms, even in individual examples. But we will illustrate that the structure of the class group $\mathcal{C}_\Delta$ can give us interesting information in general cases.

Table 7.6. Representations by Forms of Discriminant $\Delta = -56$

$x^2 + 14y^2$

| $y\backslash x$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | | 1 | | | | | | | | | | |
| 1 | 14 | 15 | 18 | 23 | 30 | 39 | 50 | 63 | 78 | 95 | 114 | 135 |
| 2 | | 57 | | 65 | | 81 | | 105 | | 137 | | |
| 3 | | 127 | 130 | | 142 | | | | | | | |

$2x^2 + 7y^2$

| $y\backslash x$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| 0 | | 2 | | | | | | | |
| 1 | 7 | 9 | 15 | 25 | 39 | 57 | 79 | 105 | 135 |
| 2 | | 30 | | 46 | | 78 | | 126 | |
| 3 | | 65 | 71 | | 95 | 113 | | | |
| 4 | | 114 | | 130 | | | | | |

**Example.** Let $D = D_\Delta$, where $\Delta = -56$. With $\phi(x) = x^2 + 14$ and $m_\Delta = \left\lfloor \sqrt{56/3} \right\rfloor = 4$, we find four reduced ideals of $D$:

$$[1 : 0], \qquad [2 : 0], \qquad [3 : 1], \qquad [3 : -1]. \tag{7.3.1}$$

Here $[P] = [3 : 1]$ generates $G = \mathcal{C}_{-56}$, with $[P]^2 = [2 : 0]$, $[P]^3 = [3 : -1]$, and $[P]^4 = [1 : 0]$. So $G$ has invariant factor type (4), and is not a principal square domain. Genus equivalence of an ideal $A$ of $D$ is determined by the genus symbols $\left(\frac{2}{A}\right)$ and $\left(\frac{A}{7}\right)$, which must be equal. If $\left(\frac{2}{A}\right) = 1 = \left(\frac{A}{7}\right)$, then $A$ is equivalent to $[1 : 0]$ or $[2 : 0]$; if $\left(\frac{2}{A}\right) = -1 = \left(\frac{A}{7}\right)$, then $A$ is equivalent to $[3 : 1]$ or $[3 : -1]$.

Let $\phi = (1 : 0)$, $f = (2 : 0)$, $g = (3 : 1)$, and $\overline{g} = (3 : -1)$ be the quadratic forms corresponding to the ideals in (7.3.1), that is,

$$\phi(x, y) = x^2 + 14y^2, \qquad f(x, y) = 2x^2 + 7y^2,$$

$$g(x, y) = 3x^2 + 2xy + 5y^2, \qquad \overline{g}(x, y) = 3x^2 - 2xy + 5y^2.$$

Although $g$ and $\overline{g}$ are not equivalent, we have seen that they represent the same integers since $g(x, y) = \overline{g}(x, -y)$ for all $x$ and $y$. In Table 7.6, we compile proper representations of integers $m < 150$ by two of these forms. We make a few of many possible statements about representations of integers by one of these forms in the following proposition. ◊

**Proposition 7.3.1.** *Let $p$ and $q$ be prime numbers other than 2 or 7.*

(1) *Suppose that* $\left(\frac{2}{p}\right) = 1 = \left(\frac{p}{7}\right)$. *Then:*

(a) *Either* $x^2 + 14y^2 = p$ *or* $2x^2 + 7y^2 = p$, *but not both, has a solution in integers.*

(b) *Either* $x^2 + 14y^2 = p$ *or* $x^2 + 14y^2 = 2p$, *but not both, has a solution in integers.*

(c) *Either* $2x^2 + 7y^2 = p$ *or* $2x^2 + 7y^2 = 2p$, *but not both, has a solution in integers.*

(2) *Suppose that* $\left(\frac{2}{p}\right) = -1 = \left(\frac{p}{7}\right)$ *and* $\left(\frac{2}{q}\right) = -1 = \left(\frac{q}{7}\right)$. *Then:*

(a) *If* $p \neq q$, *then both* $x^2 + 14y^2 = pq$ *and* $2x^2 + 7y^2 = pq$ *have solutions in integers.*

(b) *If* $p = q$, *then* $2x^2 + 7y^2 = pq$ *has a solution with* $\gcd(x, y) = 1$, *but* $x^2 + 14y^2 = pq$ *does not.*

**Exercise 7.3.1.** Let $p$ be a prime number other than 2 or 7. Show that:

(a) $\left(\frac{2}{p}\right) = 1 = \left(\frac{p}{7}\right)$ if and only if $p \equiv 1, 9, 15, 23, 25, 39 \pmod{56}$,

(b) $\left(\frac{2}{p}\right) = -1 = \left(\frac{p}{7}\right)$ if and only if $p \equiv 3, 5, 13, 19, 27, 45 \pmod{56}$.

*Proof.* If $p$ is a prime with $\left(\frac{2}{p}\right) = 1 = \left(\frac{p}{7}\right)$ or with $\left(\frac{2}{p}\right) = -1 = \left(\frac{p}{7}\right)$, then $x^2 + 14 \equiv 0 \pmod{p}$ has two solutions, and there are two ideals of $D$ with norm $p$, say $A = [p : k]$ and $\overline{A} = [p : -k]$.

(1) If $\left(\frac{2}{p}\right) = 1 = \left(\frac{p}{7}\right)$, then $A$ and $\overline{A}$ are in the principal genus. Since $[1 : 0]$ and $[2 : 0]$ are their own conjugates, we find that either $A \sim [1 : 0] \sim \overline{A}$ or $A \sim [2 : 0] \sim \overline{A}$. Because we then have $(p : k) \sim (1 : 0) \sim (p : -k)$ or $(p : k) \sim (2 : 0) \sim (p : -k)$, Theorem 4.3.6 implies that $p$ is represented either by $(1 : 0) = x^2 + 14y^2$ or $(2 : 0) = 2x^2 + 7y^2$, but not by both. This establishes statement (a). For statements (b) and (c), note that $A \sim [1 : 0]$ if and only if $A \cdot [2 : 0] \sim [2 : 0]$, and likewise $A \sim [2 : 0]$ if and only if $A \cdot [2 : 0] \sim \langle 2 \rangle \sim [1 : 0]$. Since $A \cdot [2 : 0]$ and $\overline{A} \cdot [2 : 0]$ are the only ideals of $D$ with norm $2p$, the result follows.

(2) Let $A = [p : k]$ and $\overline{A} = [p : -k]$ be the ideals of $D$ of norm $p$, and let $B = [q : \ell]$ and $\overline{B} = [q : -\ell]$ be the ideals of norm $q$. We can select $k$ and $\ell$ so that $A \sim P \sim B$, and then $\overline{A} \sim \overline{P} \sim \overline{B}$, where $P = [3 : 1]$ as above. But now note that $AB \sim P^2 \sim [2 : 0]$ while $A\overline{B} \sim [1 : 0]$. We find that both products are primitive ideals if $A \neq B$, and so conclude that both $x^2 + 14y^2 = pq$ and

$2x^2 + 7y^2 = pq$ have proper solutions, as in statement (a). On the other hand, $AB$ is primitive but $A\overline{B} = \langle p \rangle$ if $A = B$. So in this case, $2x^2 + 7y^2 = pq$ has a proper solution, while $x^2 + 14y^2 = pq$ does not, as claimed in statement (b). (The case of $A\overline{B} = \langle p \rangle$ corresponds to an *improper* solution of $x^2 + 14y^2 = pq$, namely $(x, y) = (p, 0)$.) □

**Example.** If $p = 71$, then $\left(\frac{2}{p}\right) = 1 = \left(\frac{p}{7}\right)$. From Table 7.6, we see that $x^2 + 14y^2$ represents $2p = 142$, but not $p$, while $2x^2 + 7y^2$ represents $p$, but not $2p$. Now $p = 3$ and $q = 13$ are primes for which $\left(\frac{2}{p}\right) = -1 = \left(\frac{p}{7}\right)$. Here we find, again using Table 7.6, that $x^2 + 14y^2$ and $2x^2 + 7y^2$ both represent $pq = 39$. But note that only $2x^2 + 7y^2$ properly represents $p^2 = 9$. ◊

**Exercise 7.3.2.** Show that the primes $p = 3, 5, 13$, and 19 all satisfy $\left(\frac{2}{p}\right) = -1 = \left(\frac{p}{7}\right)$. Verify that the products of two of these distinct primes, that is, 15, 39, 57, 65, 95, and 247, are represented by both $x^2 + 14y^2$ and $2x^2 + 7y^2$, but that the squares of these primes, 9, 25, 169, and 361, are properly represented only by $2x^2 + 7y^2$, as claimed in Proposition 7.3.1.

**Example.** For the next general example, let $D = D_\Delta$, where $\Delta = -104$. Here $\phi(x) = x^2 + 26$ and $m_\Delta = \left\lfloor \sqrt{104/3} \right\rfloor = 5$. From the table

| $x$ | 0 | $\pm 1$ | $\pm 2$ |
|---|---|---|---|
| $\phi(x)$ | 26 | 27 | 30 |

we find that there are six reduced ideals of discriminant $\Delta$:

$$[1 : 0], \qquad [2 : 0], \qquad [3 : 1], \qquad [3 : -1], \qquad [5 : 2], \qquad [5 : -2].$$

The class group, $G = \mathcal{C}_{-104}$, must have invariant factor type (6). Genus equivalence of an ideal $A$ is determined by the genus symbols $\left(\frac{-2}{A}\right)$ and $\left(\frac{A}{13}\right)$, which must be equal. Both symbols are $+1$ for $[3 : 1]$ and $[3 : -1]$, so their ideal classes are in the principal genus and must be squares of other ideal classes. Since $[2 : 0]$ is its own conjugate, its class is its own inverse in $G$. So only $P = [5 : 2]$ and its conjugate are potential generators of $G$. We leave it to the reader to verify that the corresponding quadratic forms of these powers of $P$ are as follows.

$$P^0 : (1 : 0) = x^2 + 26y^2, \qquad P^1 : (5 : 2) = 5x^2 + 4xy + 6y^2,$$

$$P^2 : (3 : -1) = 3x^2 - 2xy + 9y^2, \qquad P^3 : (2 : 0) = 2x^2 + 13y^2,$$

$$P^4 : (3 : 1) = 3x^2 + 2xy + 9y^2, \qquad P^5 : (5 : -2) = 5x^2 - 4xy + 6y^2.$$

Table 7.7. Representations by Forms of Discriminant $\Delta = -104$

$x^2 + 26y^2$

| $y\backslash x$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | | 1 | | | | | | | | | | |
| 1 | 26 | 27 | 30 | 35 | 42 | 51 | 62 | 75 | 90 | 107 | 126 | 147 |
| 2 | | 105 | | 113 | | 129 | | | | | | |

$2x^2 + 13y^2$

| $y\backslash x$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| 0 | | 2 | | | | | | | |
| 1 | 13 | 15 | 21 | 31 | 45 | 63 | 85 | 111 | 141 |
| 2 | | 54 | | 70 | | 102 | | | |
| 3 | | 119 | 125 | | 149 | | | | |

We compile proper representations of integers $m < 150$ by two of these forms in Table 7.7. Proposition 7.3.2 provides examples of conclusions that we can draw about these quadratic forms from the group structure of $G = \mathcal{C}_{-104}$. ♢

**Proposition 7.3.2.** *Let $p$ be a prime number with $p > 5$ and $p \neq 13$.*

(1) *If $\left(\frac{-2}{p}\right) = 1 = \left(\frac{p}{13}\right)$, then one and only one of the following is true.*

   (a) *The equations $x^2 + 26y^2 = p$ and $2x^2 + 13y^2 = 2p$ both have solutions in integers.*

   (b) *The equations $x^2 + 26y^2 = 3p$ and $2x^2 + 13y^2 = 5p$ both have solutions in integers.*

(2) *If $\left(\frac{-2}{p}\right) = -1 = \left(\frac{p}{13}\right)$, then one and only one of the following is true.*

   (a) *The equations $x^2 + 26y^2 = 2p$ and $2x^2 + 13y^2 = p$ both have solutions in integers.*

   (b) *The equations $x^2 + 26y^2 = 5p$ and $2x^2 + 13y^2 = 3p$ both have solutions in integers.*

*Proof.* Let $D = D_{-104}$. In cases (1) and (2), the congruence $\phi(x) = x^2 + 26 \equiv 0 \pmod{p}$ has two solutions, and there are two conjugate ideals of norm $p$ in $D$, say $A = [p : k]$ and $\overline{A} = [p : -k]$. If $\left(\frac{-2}{p}\right) = 1 = \left(\frac{p}{13}\right)$, the class of $A$ is in the principal genus of $G = \mathcal{C}_\Delta$, and so either $A \sim [1 : 0] \sim \overline{A}$, or (changing the sign of $k$ if necessary) $A \sim [3 : 1]$ and $\overline{A} \sim [3 : -1]$. On the other hand,

Table 7.8. Proper Representations by $5x^2 + 13y^2$

| $y\backslash x$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | | 5 | | | | | | | | |
| 1 | 13 | 18 | 33 | 58 | 93 | 138 | 193 | 258 | 333 | 418 |
| 2 | | 57 | | 97 | | 177 | | 297 | | 457 |
| 3 | | 122 | 137 | | 197 | 242 | | 362 | 437 | |
| 4 | | 213 | | 253 | | 333 | | 453 | | |
| 5 | | 330 | 345 | 370 | 405 | | | | | |
| 6 | | 473 | | | | | | | | |

if $\left(\frac{-2}{p}\right) = -1 = \left(\frac{p}{13}\right)$, then either $A \sim [2 : 0] \sim \overline{A}$, or $A \sim [5 : 2]$ and $\overline{A} \sim [5 : -2]$.

Suppose first that $A \sim [1 : 0]$. Then we also have $[2 : 0] \cdot [p : k] = [2p : \ell]$ for some $\ell$, since $p \neq 2$, and $[2p : \ell] \sim [2 : 0]$. For the corresponding quadratic forms, we then have $(p : k) \sim (1 : 0)$ and $(2p : \ell) \sim (2 : 0)$, so that $x^2 + 26y^2$ properly represents $p$ and $2x^2 + 13y^2$ properly represents $2p$ by Theorem 4.3.6. Since ideals of norm $3p$ or $5p$ reduce to other elements of the class group $\mathcal{C}_\Delta$, we cannot also have $3p$ or $5p$ represented by $x^2 + 26y^2$ or $2x^2 + 13y^2$.

Next suppose that $A \sim [3 : 1]$. With $p \neq 3$ and $p \neq 5$, class group calculations show that $A \cdot [3 : -1]$ is a primitive ideal of norm $3p$, equivalent to $[1 : 0]$, while $A \cdot [5 : -2]$ is a primitive ideal of norm $5p$, equivalent to $[2 : 0]$. In this case, $x^2 + 26y^2$ represents $3p$ while $2x^2 + 13y^2$ represents $5p$, by Theorem 4.3.6, and we can use the same result to eliminate the possibility that these forms represent $p$ or $2p$.

The remaining cases are similar, and are left to the reader. □

**Example.** As a final example for this section, we consider integers properly represented by the quadratic form $f(x, y) = 5x^2 + 13y^2$. Table 7.8 is sufficient to determine all integers $m < 500$ that can be so expressed.

The discriminant of $f$ is $\Delta = -260$, so that $\phi(x) = x^2 + 65$. From the table

| $x$ | 0 | $\pm1$ | $\pm2$ | $\pm3$ | $\pm4$ |
|---|---|---|---|---|---|
| $\phi(x)$ | 65 | 66 | 69 | 74 | 81 |

we determine that there are eight reduced forms of discriminant $\Delta$:

$$(1 : 0) = x^2 + 65y^2, \qquad (2 : 1) = 2x^2 + 2xy + 33y^2,$$
$$(3 : 1) = 3x^2 + 2xy + 22y^2, \qquad (3 : -1) = 3x^2 - 2xy + 22y^2,$$
$$(5 : 0) = 5x^2 + 13y^2, \qquad (6 : 1) = 6x^2 + 2xy + 11y^2,$$
$$(6 : -1) = 6x^2 - 2xy + 11y^2, \qquad (9 : 4) = 9x^2 + 8xy + 9y^2.$$

The genus symbols defined for these forms are $\left(\frac{-1}{f}\right)$, $\left(\frac{f}{5}\right)$, and $\left(\frac{f}{13}\right)$. The product of these symbols must equal 1, so there are four distinct genera of these forms,

and the ideal class group $\mathcal{C}_{-260}$ has invariant factor type $(4, 2)$. One can verify that if $P = [3 : 1]$ and $Q = [2 : 1]$, then every element of $\mathcal{C}_\Delta$ can be expressed as $[P]^i \cdot [Q]^j$ with $0 \le i < 4$ and $0 \le j < 2$. ◊

**Proposition 7.3.3.** *Let $p$ be a prime number with $p > 5$ and $p \neq 13$, and let $f(x, y) = 5x^2 + 13y^2$.*

(1) *If $\left(\frac{-1}{p}\right) = 1$, $\left(\frac{5}{p}\right) = 1$, and $\left(\frac{p}{13}\right) = 1$, then either $2p$ or $5p$, but not both, is properly represented by $f$.*

(2) *If $\left(\frac{-1}{p}\right) = 1$, $\left(\frac{5}{p}\right) = -1$, and $\left(\frac{p}{13}\right) = -1$, then either $p$ or $9p$, but not both, is properly represented by $f$.*

(3) *If $\left(\frac{-1}{p}\right) = -1$, $\left(\frac{5}{p}\right) = 1$, and $\left(\frac{p}{13}\right) = -1$, then $3p$ is properly represented by $f$.*

(4) *If $\left(\frac{-1}{p}\right) = -1$, $\left(\frac{5}{p}\right) = -1$, and $\left(\frac{p}{13}\right) = 1$, then $6p$ is properly represented by $f$.*

*Proof.* In each of the four cases, $\phi(x) \equiv 0 \pmod{p}$ has two solutions, so there are two ideals of norm $p$ in $D = D_{-260}$, say $A = [p : k]$ and $\overline{A} = [p : -k]$ for some $k$.

(1) If $\left(\frac{-1}{p}\right) = 1$, $\left(\frac{5}{p}\right) = 1$, and $\left(\frac{p}{13}\right) = 1$, then $A \sim [1 : 0] \sim \overline{A}$ or $A \sim [9 : 4] \sim \overline{A}$. Direct calculation in the ideal class group shows that then either $[5 : 0] \cdot A \sim [5 : 0] \sim [5 : 0] \cdot \overline{A}$ or $[2 : 1] \cdot A \sim [5 : 0] \sim [2 : 1] \cdot \overline{A}$. Thus by Theorem 4.3.6 either $5p$ or $2p$ is properly represented by $f = (5 : 0)$.

(2) If $\left(\frac{-1}{p}\right) = 1$, $\left(\frac{5}{p}\right) = -1$, and $\left(\frac{p}{13}\right) = -1$, then $A \sim [2 : 1] \sim \overline{A}$ or $A \sim [5 : 0] \sim \overline{A}$. In the first situation, $[9 : 4] \cdot A \sim [5 : 0] \sim [9 : 4] \cdot \overline{A}$, and we find that $9p$ is properly represented by $f = (5 : 0)$. In the second situation, $p$ itself is represented by $f$.

(3) If $\left(\frac{-1}{p}\right) = -1$, $\left(\frac{5}{p}\right) = 1$, and $\left(\frac{p}{13}\right) = -1$, then we can select the sign of $k$ to assume that $A = [p : k] \sim [6 : 1]$ and $\overline{A} \sim [6 : -1]$. Here we find that $(3 : 1) \cdot A \sim [5 : 0]$ and $(3 : -1) \cdot \overline{A} \sim [5 : 0]$, implying that $f = (5 : 0)$ properly represents $3p$.

(4) If $\left(\frac{-1}{p}\right) = -1$, $\left(\frac{5}{p}\right) = -1$, and $\left(\frac{p}{13}\right) = 1$, then we can assume that $A \sim [3 : 1]$ and $\overline{A} \sim [3 : -1]$. Now $(6 : 1) \cdot A \sim [5 : 0]$ and $(6 : -1) \cdot \overline{A} \sim [5 : 0]$, implying that $f = (5 : 0)$ properly represents $6p$.

So the conclusions of this proposition hold. □

**Example.** For instance, 11, 19, 31, and 59 are primes $p$ for which $\left(\frac{-1}{p}\right) = -1$, $\left(\frac{5}{p}\right) = 1$, and $\left(\frac{p}{13}\right) = -1$. Thus $f(x, y) = 5x^2 + 13y^2$ properly represents $3p$, that is, 33, 57, 93, and 177, as we can verify from Table 7.8. ◊

**Exercise 7.3.3.** Let $\Delta = -68$.

(a) Calculate the ideal class group $\mathcal{C}_\Delta$.

(b) Show that if $p > 2$ is a prime number for which $\left(\frac{-1}{p}\right) = 1 = \left(\frac{p}{17}\right)$, then $x^2 + 17y^2$ properly represents either $p$ or $2p$, but not both.

(c) Show that if $p > 3$ is a prime number for which $\left(\frac{-1}{p}\right) = -1 = \left(\frac{p}{17}\right)$, then $x^2 + 17y^2$ properly represents $3p$.

**Exercise 7.3.4.** Let $\Delta = -152$.

(a) Calculate the ideal class group $\mathcal{C}_\Delta$.

(b) Show that if $p > 3$ is a prime number for which $\left(\frac{2}{p}\right) = 1 = \left(\frac{p}{19}\right)$, then $x^2 + 38y^2$ properly represents either $p$ or $6p$, but not both.

(c) Show that if $p > 3$ is a prime number for which $\left(\frac{2}{p}\right) = -1 = \left(\frac{p}{19}\right)$, then $x^2 + 38y^2$ properly represents either $2p$ or $3p$, but not both.

## 7.4 Construction of Representations

In the preceding sections of this chapter, we have looked at several examples and general statements on the existence of representations by certain positive definite quadratic forms, based on the structure of corresponding class groups. To conclude Chapter 7, we consider a few methods of producing those solutions in practice. In particular, we will demonstrate that we can apply the process of finding the reduced quadratic form that is equivalent to a given positive definite form as a method of constructing representations by those reduced forms.

**Reduction of Quadratic Forms.** Let $m$ be a positive integer and let $\phi(x)$ be the principal polynomial of some negative discriminant $\Delta$. We have seen (Theorem 4.3.3) that $m$ is properly represented by a quadratic form of discriminant $\Delta$ if and only if $\phi(x) \equiv 0 \pmod{m}$ has a solution, say $\ell$. In this case, $g = (m : \ell)$ is a quadratic form of discriminant $\Delta$, so must be equivalent to precisely one reduced form in $\mathcal{Q}_\Delta$, say $f = (a : k)$. Note that $g$ properly represents $m$, since $g(1, 0) = m$, so the same must be true for $f$. In fact, we can make the following statement.

**Proposition 7.4.1.** *Let $g = (m : \ell)$ and $f = (a : k)$ be quadratic forms of discriminant $\Delta$. Suppose that $g$ is equivalent to $f$, say that $g = f \circ U$ with $U = \left[\begin{smallmatrix} q & s \\ r & t \end{smallmatrix}\right]$. In that case, $f(q,r) = m$, so that $f$ properly represents $m$.*

*Proof.* Let $M_f$ and $M_g$ be the matrices of $f$ and $g$, respectively, so that $M_g = U^T M_f U$. Recall that if $\mathbf{x}$ is an ordered pair of integers, written as a column matrix, then $f(\mathbf{x}) = \frac{1}{2}\mathbf{x}^T M_f \mathbf{x}$. So we find that

$$\begin{aligned} m = g(1,0) &= \tfrac{1}{2} \cdot \begin{bmatrix} 1 & 0 \end{bmatrix} \cdot M_g \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \tfrac{1}{2} \cdot \begin{bmatrix} 1 & 0 \end{bmatrix} \cdot (U^T M_f U) \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} \\ &= \tfrac{1}{2} \cdot \begin{bmatrix} 1 & 0 \end{bmatrix} \begin{bmatrix} q & r \\ s & t \end{bmatrix} \cdot M_f \cdot \begin{bmatrix} q & s \\ r & t \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} \\ &= \tfrac{1}{2} \cdot \begin{bmatrix} q & r \end{bmatrix} \cdot M_f \cdot \begin{bmatrix} q \\ r \end{bmatrix} = f(q,r). \end{aligned}$$

Here $\gcd(q,r) = 1$ since $U$ is a unimodular matrix. □

The process of reducing $g$ to $f$ by a sequence of involutions and translations allows us to write $g = f \circ U$ in practice. We illustrate the approach with an example, which we will then generalize.

**Example.** Let $\Delta = \Delta(-5,1) = -20$, so that $\phi(x) = x^2 + 5$. If $m = 83$, we find that $\phi(x) \equiv 0 \pmod{83}$ has $\ell = 24$ as a solution. Using notation introduced in §4.2, we find that

$$(83 : 24) \leftrightarrow (7 : -24) \to_3 (7 : -3) \leftrightarrow (2 : 3) \to_{-1} (2 : 1).$$

The resulting quadratic form $f = (2 : 1)$ is reduced, and can be written in standard form as $f(x,y) = 2x^2 + 2xy + 3y^2$. Specifically, this sequence of involutions and translations shows that

$$\begin{aligned} f &= g \circ \left( \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \right) \\ &= g \circ \left( \begin{bmatrix} 0 & -1 \\ 1 & 3 \end{bmatrix} \cdot \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix} \right) = g \circ \begin{bmatrix} -1 & 1 \\ 3 & -4 \end{bmatrix}. \end{aligned}$$

It follows that

$$g = f \circ \begin{bmatrix} -1 & 1 \\ 3 & -4 \end{bmatrix}^{-1} = f \circ \begin{bmatrix} -4 & -1 \\ -3 & -1 \end{bmatrix},$$

and so, by Proposition 7.4.1, $f(-4,-3) = 83$. ◊

The procedure of this example can be generalized. First note that in the process of reducing a quadratic form $g = (m : \ell)$, we often use an involution followed by a translation to obtain a form $f = (a : k)$ with $k$ minimal in absolute value. It will be convenient to write $g \leftrightarrow_u f$ as an abbreviation for the involution/translation sequence $g \leftrightarrow f_1 \rightarrow_u f$.

**Proposition 7.4.2.** *Let $g = (m : \ell)$ and $f = (a : k)$ be quadratic forms of discriminant $\Delta$, and suppose that $g$ is equivalent to $f$ by a sequence of involutions and translations as follows:*

$$g \leftrightarrow_{u_1} f_1 \leftrightarrow_{u_2} \cdots \leftrightarrow_{u_{n-1}} f_{n-1} \leftrightarrow_{u_n} f. \tag{7.4.1}$$

*Let $U$ be the following unimodular matrix:*

$$U = \begin{bmatrix} q & s \\ r & t \end{bmatrix} = \begin{bmatrix} u_n & 1 \\ -1 & 0 \end{bmatrix} \cdot \begin{bmatrix} u_{n-1} & 1 \\ -1 & 0 \end{bmatrix} \cdots \begin{bmatrix} u_2 & 1 \\ -1 & 0 \end{bmatrix} \cdot \begin{bmatrix} u_1 & 1 \\ -1 & 0 \end{bmatrix}. \tag{7.4.2}$$

*Then $f(q, r) = m$.*

*Proof.* If $g \leftrightarrow_u f$, then $f = g \circ V$, where

$$V = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & u \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & u \end{bmatrix}. \tag{7.4.3}$$

If $g$ is equivalent to $f$ by a sequence of involutions and translations as in equation (7.4.1), then $f = g \circ V$, where $V = V_1 \cdot V_2 \cdots V_{n-1} \cdot V_n$, with each $V_i$ in the form of equation (7.4.3). But then $g = f \circ U$, where

$$U = V^{-1} = V_n^{-1} \cdot V_{n-1}^{-1} \cdots V_2^{-1} \cdot V_1^{-1},$$

which is the product in equation (7.4.2). Our conclusion follows directly from Proposition 7.4.1. □

**Example.** Let $\Delta = -20$ and $\phi(x) = x^2 + 5$, as in the preceding example. Suppose we find that $m = 743$ divides $\phi(348)$, so that $g = (743 : 348)$ is a quadratic form in $\mathcal{Q}_{-20}$. Then we find that

$$(743 : 348) \leftrightarrow_2 (163 : -22) \leftrightarrow_{-7} (3 : 1) \leftrightarrow_1 (2 : 1).$$

(For example, $\phi(348) = 743 \cdot 163$, and we find that $-348 + 163(2) = -22$, the minimum possibility, in absolute value, modulo 163.) Thus 743 is properly represented by the reduced form $f = (2 : 1)$. Specifically, since $g = f \circ U$ for

$$U = \begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix} \cdot \begin{bmatrix} -7 & 1 \\ -1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 2 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} -17 & -8 \\ 15 & 7 \end{bmatrix},$$

then $f(-17, 15) = 2(-17)^2 + 2(-17)(15) + 3(15)^2 = 743$. ◊

**Exercise 7.4.1.** In each part, a quadratic form $g = (m : \ell)$ of the given discriminant $\Delta$ is presented. Use the procedure of Proposition 7.4.2 to find the reduced form $f$ in $\mathcal{Q}_\Delta$ to which $g$ is equivalent, and to find a solution of $f(x, y) = m$.

(a) $g = (187 : 19)$ with $\Delta = -52$.

(b) $g = (187 : 36)$ with $\Delta = -52$.

(c) $g = (171 : 29)$ with $\Delta = -56$.

(d) $g = (171 : 47)$ with $\Delta = -56$.

(e) $g = (185 : 33)$ with $\Delta = -84$.

(f) $g = (185 : 78)$ with $\Delta = -84$.

**Reduction of Ideals.** As an alternative to using quadratic forms and matrix multiplication, as in the preceding results and examples, we can construct a representation of an integer $m$ by some quadratic form of discriminant $\Delta$ via ideals and multiplication of elements in the quadratic domain $D_\Delta$. The following observation, which we will revise as an algorithm, is our starting point.

**Proposition 7.4.3.** *Let $g = (m : \ell)$ and $f = (a : k)$ be quadratic forms of discriminant $\Delta$, and let $M = A_g = [m : \ell]$ and $A = A_f = [a : k]$ be the corresponding ideals of $D = D_\Delta$. If $f$ is equivalent to $g$, then it is possible to write $mA = \upsilon M$ for some element $\upsilon$ of $D$. In this case, $\upsilon$ is an element of $A$, and if we write $\upsilon = q(a) + r(k + z)$ for some integers $q$ and $r$, then $f(q, r) = m$.*

*Proof.* The proof of Theorem 5.1.5 shows that if $g = f \circ U$ for some unimodular matrix $U$, then there is an element $\upsilon$ of $D$ for which $mA = \upsilon M$. Note that $m = N(M)$ is an element of $M$, and so $m\upsilon$ is an element of $\upsilon M = mA$. Since $m \neq 0$, it follows that $\upsilon$ is an element of $A$. So it is possible to write $\upsilon$ as a $\mathbb{Z}$-combination of the ordered basis $S = \{a, k+z\}$ for $A$, that is, $\upsilon = q(a)+r(k+z)$ for some integers $q$ and $r$. Theorem 5.2.4 shows that the quadratic form of $S$ is $f_S = f = (a : k)$, and that $N(\upsilon) = N(A) \cdot f(q, r)$. But notice that with $N(M) = m$ and $N(A) = a$, the equation $\upsilon M = mA$ implies that $N(\upsilon) = am$. We conclude that $f(q, r) = m$. □

Recall from Corollary 5.1.6 that if $A = [a : k]$ is an ideal of $D_\Delta$, and $\phi(k) = ac$, then we have the equation $cA = (k + z)C$, where $C = [c : -k - \varepsilon]$. We can typically rewrite $C$ as $[c : \ell]$, where $\ell$ is minimal in absolute value modulo $c$. (Here $\phi(x)$ is the principal polynomial of discriminant $\Delta$, and $z$ and $\varepsilon$ are defined for $\Delta$ as in equation (2.2.2).) We will write $A \leftrightarrow C$, or $[a : k] \leftrightarrow [c : \ell]$, for this *involution* of ideals. We use this notation in the following algorithm.

**Proposition 7.4.4.** *Let $M = [m : \ell] = [a_0 : k_0]$ be an ideal of $D = D_\Delta$ with $\Delta$ negative. Suppose that there is a sequence of involutions,*

$$[a_0 : k_0] \leftrightarrow [a_1 : k_1] \leftrightarrow \cdots \leftrightarrow [a_{n-1} : k_{n-1}] \leftrightarrow [a_n : k_n], \tag{7.4.4}$$

*with $A = [a_n : k_n] = [a : k]$ a reduced ideal. Let $f = (a : k)$ be the corresponding quadratic form of discriminant $\Delta$. Then we have*

$$a_1 \cdot a_2 \cdots a_{n-1} \cdot a_n \cdot M = (k_0 + z) \cdot (k_1 + z) \cdots (k_{n-1} + z) \cdot A, \tag{7.4.5}$$

*which can be simplified to the form $aM = wA$ for some element $w$ of $D$. If $w = s+tz$, and we let $q = \frac{s+t(k+\varepsilon)}{a}$ and $r = -t$, then $f(q,r) = m$.*

*Proof.* We have previously seen that if $k_i$ is selected so that $\phi(k_i)$ is minimal, then a sequence of involutions as in equation (7.4.4) eventually results in a reduced form. Equation (7.4.5) then results from repeated application of Corollary 5.1.6. We obtain the equation $aM = wA$ for some $w$ by cancellation, and we find that $N(w) = am$ by applying the norm to both sides of this equation. Multiplying both sides of $aM = wA$ by $\overline{w}$, we obtain $a\overline{w}M = N(w)A$, so that $mA = \overline{w}M$. Now Proposition 7.4.3 applies. If $w = s + tz$, then $\overline{w} = s + t\overline{z} = (s + t\varepsilon) - tz$ is an element of $A$, so can be expressed as $q(a) + r(k + z)$ for some integers $q$ and $r$, in which case $f(q,r) = m$. From the equation $(qa + rk) + rz = (s + t\varepsilon) - tz$, we find that $r = -t$ and $q = \frac{s+t\varepsilon-rk}{a} = \frac{s+t(k+\varepsilon)}{a}$. □

To illustrate this procedure, we apply Proposition 7.4.4 to a previous example.

**Example.** Consider $M = [743 : 348]$, an ideal of $D = D_{-20}$. We find that

$$[743 : 348] \leftrightarrow [163 : -22] \leftrightarrow [3 : 1] \leftrightarrow [2 : 1],$$

since with $\phi(x) = x^2 + 5$, we have $\phi(348) = 743 \cdot 163$ with $-348 \equiv -22 \pmod{163}$, and so forth. We then obtain the equation

$$163 \cdot 3 \cdot 2 \cdot M = (348 + z) \cdot (-22 + z) \cdot (1 + z) \cdot A,$$

where $z = \sqrt{-5}$ and $A = [2 : 1]$, as in (7.4.5). Here $(-22 + z)(1 + z) = -22 - 21z + z^2 = -27 - 21z$, so we can cancel 3 from both sides to write

$$163 \cdot 2 \cdot M = (348 + z) \cdot (-9 - 7z) \cdot A.$$

Likewise, $(348 + z)(-9 - 7z) = -3132 - 2445z - 7z^2 = -3097 - 2445z$. Now we can cancel 163 from both sides, obtaining $2M = (-19 - 15z)A$, which is of the form $aM = wA$ as claimed in Proposition 7.4.4. If $s = -19$ and $t = -15$, with $\varepsilon = 0$, $a = 2$, and $k = 1$, then $q = \frac{s+t}{a} = -17$ and $r = -t = 15$. Thus if $f = (2 : 1)$, then $f(-17, 15) = 743$, as we found in a previous example. ◊

**Exercise 7.4.2.** In each part, an ideal $M = [m : \ell]$ of $D_\Delta$ with the given discriminant $\Delta$ is presented. Use the procedure of Proposition 7.4.4 to find the reduced ideal $A = [a : k]$ to which $M$ is equivalent, and to find a solution of $f(x, y) = m$, where $f = (a : k)$. Compare these answers to those of Exercise 7.4.1.

(a) $M = [187 : 19]$ with $\Delta = -52$.

(b) $M = [187 : 36]$ with $\Delta = -52$.

(c) $M = [171 : 29]$ with $\Delta = -56$.

(d) $M = [171 : 47]$ with $\Delta = -56$.

(e) $M = [185 : 33]$ with $\Delta = -84$.

(f) $M = [185 : 78]$ with $\Delta = -84$.

**Example.** Let $\Delta = -47$, so that $\phi(x) = x^2 + x + 12$ and $\varepsilon = 1$. Suppose we find that 53 divides $\phi(17) = \phi(-18)$ and 89 divides $\phi(32) = \phi(-33)$. Then

$$M_1 = [53 : 17], \quad \overline{M_1} = [53 : -18], \quad M_2 = [89 : 32], \quad \overline{M_2} = [89 : -33]$$

are ideals of $D = D_{-47}$. Since $\phi(17) = 53 \cdot 6$ and $-18 \equiv 0 \pmod 6$, we find that

$$[53 : 17] \leftrightarrow [6 : 0] \leftrightarrow [2 : -1] = A_1,$$

a reduced ideal. Here $f_1(x, y) = 2x^2 - xy + 6y^2$ is the corresponding quadratic form. Now we find that $6 \cdot 2 \cdot M_1 = (17 + z)(0 + z)A_1$. With $z = \frac{1+\sqrt{-47}}{2}$, so that $z^2 = -12 + z$, then $(17 + z)z = 17z + z^2 = -12 + 18z$, and it follows that $2M_1 = (-2 + 3z)A_1$. Hence with $q = \frac{s+t(k+\varepsilon)}{a} = \frac{-2+3(0)}{2} = -1$ and $r = -t = -3$, we conclude that $f_1(-1, -3) = 53$, as we can verify. A similar reduction with $\overline{M_1}$ shows that $\overline{f_1}(-1, 3) = 53$ as well.

Similarly,

$$[89 : 32] \leftrightarrow [12 : 3] \leftrightarrow [2 : 0] = A_2,$$

so that 89 is properly represented by the reduced form $f_2(x, y) = 2x^2 + xy + 6y^2$. We find, in fact, that

$$12 \cdot 2 \cdot M_2 = (32 + z)(3 + z)A_2 = (84 + 36z)A_2,$$

and thus $2M_2 = (7 + 3z)$. Now with $q = \frac{s+t(k+\varepsilon)}{a} = \frac{7+3(1+0)}{2} = 5$ and $r = -t = -3$, we can verify that $f_2(5, -3) = 89$. Similarly, we find that $\overline{f_2}(5, 3) = 89$.

Now suppose that we want to find representations of $53 \cdot 89 = 4717$ by reduced forms of discriminant $-47$. We first note that $M_1 \cdot M_2 = [4717 : 388]$ and $\overline{M_1} \cdot M_2 = [4717 : -1926]$ by the method of Theorem 3.4.6, with similar expressions for $M_1 \cdot \overline{M_2}$ and $\overline{M_1} \cdot \overline{M_2}$. Since $M_1 \sim [2 : -1]$ and $M_2 \sim [2 : 0]$, then $M_1 \cdot M_2 \sim [2 : -1] \cdot [2 : 0] \sim 2[1 : 0] \sim [1 : 0]$. Likewise, $\overline{M_1} \cdot M_2 \sim$

$[2 : 0] \cdot [2 : 0] \sim [4 : 0] \sim [3 : -1]$. So we expect that 4717 is represented by $(1 : 0) = x^2 + xy + 12y^2$ and by $(3 : -1) = 3x^2 - xy + 4y^2$, as well as the conjugates of these forms. We will verify the first two claims, using the method of Proposition 7.4.2 for contrast.

We first calculate that

$$(4717 : 388) \leftrightarrow_{12} (32 : -5) \leftrightarrow_{-4} (1 : 0),$$

since $-389 + 32(12) = -5$ and $4 + 1(-4) = 0$. So with

$$\begin{bmatrix} -4 & 1 \\ -1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 12 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} -49 & -4 \\ -12 & -1 \end{bmatrix},$$

we conclude that $f(-49, -12) = 4717$ when $f(x, y) = x^2 + xy + 12y^2$, as we can verify directly. Similarly,

$$(4717 : -1926) \leftrightarrow_{-2} (786 : 353) \leftrightarrow_{2} (159 : -36) \leftrightarrow_{-4} (8 : 3) \leftrightarrow_{1} (3 : -1),$$

and with

$$\begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix} \cdot \begin{bmatrix} -4 & 1 \\ -1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 2 & 1 \\ -1 & 0 \end{bmatrix} \cdot \begin{bmatrix} -2 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 27 & -11 \\ -22 & 9 \end{bmatrix},$$

then $f(27, -22) = 4717$ for $f(x, y) = 3x^2 - xy + 4y^2$. ◊

In summary, if $\phi(x)$ is the principal polynomial of a given discriminant $\Delta$, then every solution $\ell$ of $\phi(x) \equiv 0 \pmod{m}$ yields a quadratic form $g = (m : \ell)$ in $\mathcal{Q}_\Delta$, or likewise an ideal $M = [m : \ell]$ of $D_\Delta$. We have a systematic process whereby this form (or ideal) can be shown equivalent to a reduced form $f = (a : k)$ (or reduced ideal $A_f = [a : k]$). We have seen in this section that this reduction process produces a solution of $f(q, r) = m$. By Theorem 4.3.6, we know that ($f$-equivalence classes of) these solutions are in one-to-one correspondence with solutions $\ell$ of $\phi(x) \equiv 0 \pmod{m}$. Thus the calculation of all proper representations of an integer $m$ by some quadratic form of negative discriminant $\Delta$ is reduced to calculation of all solutions of $\phi(x) \equiv 0 \pmod{m}$.

## Representations by Positive Definite Forms—Review

In this chapter, we presented several applications of our calculations of class groups of negative discriminant from Chapter 6. In particular, we saw how the structure of an ideal class group $\mathcal{C}_\Delta$ provides information about the integers that are properly represented by various quadratic forms of discriminant $\Delta$. We summarize our main results as follows.

(1) If $\phi(x)$ is the principal polynomial of a negative discriminant $\Delta$, then a positive integer $m$ is properly represented by some quadratic form of discriminant $\Delta$ if and only if the congruence $\phi(x) \equiv 0 \pmod{m}$ has a solution.

(2) Every positive definite quadratic form of discriminant $\Delta < 0$ is equivalent to precisely one *reduced* form. Since equivalent forms represent, and properly represent, the same collection of integers, it suffices to describe the integers represented by each reduced quadratic form.

(3) If $\Delta$ is a negative primitive discriminant and $\mathcal{C}_\Delta$ is trivial, then there is precisely one reduced form, the principal form $\phi(x, y)$, and we have a precise criterion for which integers are properly represented by $\phi(x, y)$. We can also describe the number of such representations.

(4) More generally, we can give a complete description of the integers properly represented by all reduced forms of discriminant $\Delta < 0$ if the class group $\mathcal{C}_\Delta$ has invariant factor type $(2, 2, \dots, 2)$, with $\ell$ terms of 2. We call $D = D_\Delta$ a *principal square domain* of type $\ell$ in this case. Here every *genus* of quadratic forms contains exactly one class, and we can use genus symbols of quadratic forms to determine which positive integers are properly represented by each reduced form.

(5) We also demonstrated that the structure of the ideal class group of discriminant $\Delta$ can typically provide useful, although partial, information about the integers represented by quadratic forms of that discriminant in more general cases.

In Chapters 10 and 11, we will see how some of these results can be extended to positive discriminants, and corresponding indefinite quadratic forms.

# 8

# Class Groups of Quadratic Subdomains

Recall that if $d \neq 1$ is squarefree, then $D_\Delta$ is a *complete* quadratic domain if $\Delta = \Delta(d, 1)$, and a *quadratic subdomain* if $\Delta = \Delta(d, \gamma)$ with $\gamma > 1$. In this chapter, we establish connections between the class groups of these discriminants. It will be convenient to state our theorems in terms of quadratic forms, due to the methods required in their proofs. The results apply equally well to ideal class groups. For negative discriminants, we will restrict our attention to positive definite quadratic forms.

We state our main result in §8.1, a method of calculating the class group of discriminant $p^2\Delta$ from that of an arbitrary discriminant $\Delta$ when $p$ is prime. We illustrate with examples that this approach gives us a complete description of class groups of quadratic subdomains of *negative* discriminant, proving these results in §8.2 and §8.3. We extend our results to positive discriminants in §13.3. (Aside from that section, the material in this chapter is not required in any other part of this text.)

## 8.1 Constructing Class Groups of Subdomains

Throughout this section, let $\Delta$ be a discriminant (negative or positive, and not necessarily primitive), and write the form class group of discriminant $\Delta$ as $G = \mathcal{F}_\Delta$. For a fixed prime $p$, let $G_p = \mathcal{F}_{p^2\Delta}$. We will use Propositions 8.1.1 and 8.1.2 to define two subsets of $G_p$, from which we can compute the entire group $G_p$.

**Proposition 8.1.1.** *Let $G$ be the form class group of discriminant $\Delta$ and let $p$ be a prime number. Then every element of $G$ can be written as the class of some form $f = (a : k)$, where $p$ does not divide $a$. In that case, $(a : pk)$ is a primitive quadratic form of discriminant $p^2\Delta$.*

*Proof.* Let $\phi(x)$ be the principal polynomial of discriminant $\Delta$. Write the form $f = (a : k)$ as $f(x, y) = ax^2 + bxy + cy^2$, where $\phi(k) = ac$ and $\phi'(k) = b$. Elements of $G$ are primitive by definition, and so $\gcd(a, b, c) = 1$. We know that $(a : k) \sim (c : -k - \varepsilon)$ by an involution. Since $(a : k) \sim (a : k - a)$ and $\phi(k - a) = a(a - b + c)$, we also find that $(a : k) \sim (a - b + c : a - k - \varepsilon)$. The prime number $p$ cannot divide all three of $a$, $c$, and $a - b + c$, thus we can assume that $p$ does not divide $a$.

Now let $\phi_p(x)$ be the principal polynomial of discriminant $p^2\Delta$. Then $\phi_p(px) = p^2\phi(x)$ and $\phi_p'(px) = p\phi'(x)$ for all $x$. (See Exercise 2.2.7.) In particular, if $a$ divides $\phi(k)$, then $a$ divides $\phi_p(pk)$, hence $f_p = (a : pk)$ is a quadratic form of discriminant $p^2\Delta$, namely $f_p(x, y) = ax^2 + pbxy + p^2cy^2$. Since $\gcd(a, b, c) = 1$ and $p$ does not divide $a$, then $\gcd(a, pb, p^2c) = 1$ as well so that $(a : pk)$ is primitive. □

Proposition 8.1.1 shows that we can write$G = \mathcal{F}_\Delta$ as a set of (classes of) forms $(a : k)$ with $p$ not dividing $a$. Then the set of all classes of $(a : pk)$ is a corresponding subset $S_p$ of $G_p = \mathcal{F}_{p^2\Delta}$. We call $S_p$ a *set of representatives* of $G$ in $G_p$.

**Example.** Let $\Delta = -47$, so that $\phi(x) = x^2 + x + 12$. We leave it to the reader to verify that the reduced quadratic forms of discriminant $\Delta$ are

$$(1 : 0), \qquad (2 : 0), \qquad (2 : -1), \qquad (3 : 0), \qquad (3 : -1).$$

We determine a set of representatives $S_p$ for $G = \mathcal{C}_{-47}$ in $G_p = \mathcal{C}_{-47p^2}$ for small primes $p$ as follows.

(1) If $p = 2$, then we must replace $(2 : 0)$ and $(2 : -1)$ with equivalent forms in which the coefficient of $x^2$ is odd. Here $\phi(0) = 12 = 2 \cdot 6 = \phi(-1)$, so that $c$ is also even. But we find that $(2 : 0) \sim (2 : -2) \sim (7 : 1)$ as in the proof of Proposition 8.1.1, and likewise $(2 : -1) \sim (7 : -2)$. Thus

$$S_2 = \{(1 : 0), (7 : 2), (7 : -4), (3 : 0), (3 : -2)\}$$

is a set of representatives for $G$ in $G_2 = \mathcal{F}_{-188}$.

(2) If $p = 3$, we first note that $(3 : 0) \sim (4 : -1)$ and $(3 : -1) \sim (4 : 0)$. So

$$S_3 = \{(1 : 0), (2 : 0), (2 : -3), (4 : -3), (4 : 0)\}$$

is a set of representatives for $G$ in $G_3 = \mathcal{F}_{-423}$.

(3) If $p = 5$, then

$$S_5 = \{(1 : 0), (2 : 0), (2 : -5), (3 : 0), (3 : -5)\}$$

is a set of representatives for $G$ in $G_5 = \mathcal{F}_{-1175}$. ◊

A few observations are in order. First note that the classes of elements of $S_p$ are not uniquely determined in $\mathcal{F}_{p^2\Delta}$. For instance, when $p = 5$ in the preceding example, we could have replaced $(3 : 0)$ by $(4 : -1)$ in $\mathcal{F}_{-47}$ (as was necessary when $p = 3$). In that case, $(4 : -5)$ is the corresponding element of $S_5$. Here $(3 : 0) \sim (3 : -3)$ and $(4 : -5) \sim (4 : -1)$, with the latter forms both reduced in $\mathcal{Q}_{-1175}$. Thus these potential elements of $S_5$ are not equal as form classes. Notice also that $S_p$ is typically not a subgroup of $G_p$. If $f = (2 : 0)$ in $S_5$, for instance, then $f \cdot f = (4 : 0)$ is not equivalent to any of the listed forms, which shows that the given set $S_5$ is not closed under multiplication. However, no matter how $S_p$ is constructed, it will have the same number of elements as $G$. That is, no two elements of $S_p$, arising from different elements of $G$, can be equivalent to each other in $G_p$. We will assume that claim in this section, and prove that it is true in §8.2.

**Exercise 8.1.1.** For each $\Delta$, list the elements of $G = \mathcal{F}_\Delta$. List a corresponding set of representatives $S_p$ for $G$ in $G_p = \mathcal{F}_{p^2\Delta}$ for $p = 2$, $p = 3$, and $p = 5$. (Each of these $\Delta$ values appears in Exercise 6.3.1.)

(a) $\Delta = -20$.

(b) $\Delta = -40$.

(c) $\Delta = -56$.

(d) $\Delta = -84$.

(e) $\Delta = -116$.

(f) $\Delta = -119$.

**Proposition 8.1.2.** *Let $\phi(x)$ be the principal polynomial of some discriminant $\Delta$ and let $p$ be a prime number. If $k$ is an integer for which $p$ does not divide $\phi(k)$, then $(p^2 : pk)$ is a primitive quadratic form of discriminant $p^2\Delta$.*

*Proof.* Let $\phi_p(x)$ be the principal polynomial of discriminant $p^2\Delta$. Since $\phi_p(pk) = p^2\phi(k)$ and $\gcd(p^2, \phi(k)) = 1$ if $p$ does not divide $\phi(k)$, our claims follow immediately. □

Thus the classes of the forms $(p^2 : pk)$ for which $p$ does not divide $\phi(k)$ can be viewed as elements of $G_p$. We will denote the set of all *distinct* classes of such forms, together with the class of $(1 : 0)$, as $K_p$. We refer to $K_p$ as the *kernel* of $G_p$, explaining that terminology in §8.2. If $k \equiv \ell \pmod{p}$, then $pk \equiv p\ell \pmod{p^2}$ and so $(p^2 : pk) \sim (p^2 : p\ell)$. It follows that $K_p$ has a maximum of $p + 1 - n_p(\phi)$ elements, where $n_p(\phi)$ denotes the number of solutions of $\phi(x) \equiv 0 \pmod{p}$.

In fact, we will establish that $|K_p|$ always divides this maximum number of elements. When $\Delta$ is *negative*, we have the following precise formula for $|K_p|$. We will prove these claims in §8.3.

**Theorem 8.1.3.** *Let $\phi(x)$ be the principal polynomial of some negative discriminant $\Delta$, and let $p$ be prime. Let $K_p$ denote the set of all distinct form classes in $\mathcal{F}_{p^2\Delta}$ of $(1 : 0)$ and of $(p^2 : pk)$ with $\phi(k)$ not divisible by $p$. Let*

$$s = \begin{cases} 3, & \text{if } \Delta = -3, \\ 2, & \text{if } \Delta = -4, \\ 1, & \text{if } \Delta < -4. \end{cases}$$

*Then the number of elements in $K_p$ is given by*

$$|K_p| = \frac{1}{s}\left(p - \left(\frac{\Delta}{p}\right)\right).$$

Here we use the Kronecker symbol, as defined in §0.3, when $p = 2$.

**Exercise 8.1.2.** Show that when $\Delta = -3$ or $\Delta = -4$, then the value of $|K_p|$ given in Theorem 8.1.3 is an integer for every prime $p$.

**Example.** Let $\Delta = -47$ with $\phi(x) = x^2 + x + 12$, and let $p = 5$. Here $\phi(x) \equiv 0 \pmod 5$ has no solutions, and we can write

$$K_5 = \{(1 : 0), (25 : 0), (25 : -5), (25 : 5), (25 : -10), (25 : 10)\},$$

selecting values of $k$ for which $\phi(k)$ is minimal. We can verify that all elements of $K_5$ are distinct in the group $G_5 = \mathcal{F}_{-1175}$ by determining the reduced form of $D_{-1175}$ to which each of these forms is equivalent. With $\phi_5(x) = x^2 + 5x + 300$ and $u_{-1175} = 19$, we find that

$$K_5 = \{(1 : -2), (12 : -5), (12 : 0), (14 : 4), (14 : -9), (18 : 3)\},$$

with each of these reduced forms distinct. ◊

**Exercise 8.1.3.** For each $\Delta$, list the elements of the subset $K_p$ of $G_p = \mathcal{F}_{p^2\Delta}$ for $p = 2$, $p = 3$, and $p = 5$. Verify that all elements listed are distinct in $G_p$.

(a) $\Delta = -20$.

(b) $\Delta = -40$.

(c) $\Delta = -56$.

(d) $\Delta = -84$.

(e) $\Delta = -116$.

(f) $\Delta = -119$.

**Example.** Let $\Delta = -4$, so that $\phi(x) = x^2 + 1$, and let $p = 5$. Here $\phi(x) \equiv 0 \pmod 5$ has two solutions, $x = 2$ and $x = -2$, so that there is a maximum of $p - \left(\frac{\Delta}{p}\right) = 4$ elements in $K_5$, namely

$$(1 : 0), \quad (25 : 0), \quad (25 : 5), \quad (25 : -5).$$

But with $\phi_5(x) = x^2 + 25$, direct calculation shows that

$$(25 : 0) \sim (1 : 0) \quad \text{and} \quad (25 : 5) \sim (2 : 1) \sim (25 : -5).$$

So in fact $K_5 = \{(1 : 0), (2 : 1)\}$ with two distinct elements. ◊

**Exercise 8.1.4.** Let $\Delta = -3$ and $p = 11$. List the twelve potentially distinct elements of $G_p = \mathcal{F}_{p^2\Delta}$ of the form $(1 : 0)$ or $(p^2 : pk)$. Show that these forms belong to only four distinct classes in $G_p$, however.

We now state our main result for §8.1. We will illustrate this claim with examples to conclude this section, and prove Theorem 8.1.4 in §8.2.

**Theorem 8.1.4.** *Let $\Delta$ be a discriminant and let $p$ be a prime number. Let $S_p$ be a set of representatives of $G = \mathcal{F}_\Delta$ in $G_p = \mathcal{F}_{p^2\Delta}$ and let $K_p$ be the kernel of $G_p$, as those sets are defined above. Then each element of the class group $G_p$ can be written as a product $[f] \cdot [g]$ with $[f]$ in $S_p$ and $[g]$ in $K_p$, and all such products are distinct in $G_p$. Thus $|G_p| = |G| \cdot |K_p|$.*

**Example.** Let $\Delta = -47$ and $p = 3$, and let $G = \mathcal{F}_{-47}$ and $G_3 = \mathcal{F}_{-423}$. In a previous example in this section, we saw that

$$S_3 = \{(1 : 0), (2 : 0), (2 : -3), (4 : -3), (4 : 0)\}$$

is a set of representatives for $G$ in $G_3$. With $\phi(x) = x^2 + x + 12$ the principal polynomial of discriminant $\Delta$, we find that $\phi(x) \equiv 0 \pmod 3$ has two solutions, $x = 0$ and $x = -1$, and so $K_3$ has $p - \left(\frac{\Delta}{p}\right) = 2$ elements by Theorem 8.1.3. Specifically, $K_3 = \{(1 : 0), (9 : 3)\}$. Theorem 8.1.4 implies that we can list the elements of $G_3$ in the following array, with elements of $S_3$ as the first row, elements of $K_3$ as the first column (with $(1 : 0)$ a common element of the two subsets), and with products (that is, compositions) of these forms as the remaining entries.

| | | | | |
|---|---|---|---|---|
| $(1 : 0)$ | $(2 : 0)$ | $(2 : -3)$ | $(4 : -3)$ | $(4 : 0)$ |
| $(9 : 3)$ | $(18 : -6)$ | $(18 : 3)$ | $(36 : -15)$ | $(36 : 12)$ |

To test this claim, and to compare methods, we use the approach illustrated in §6.1 to list the reduced quadratic form of discriminant $-423$.

Let $\phi(x) = x^2 + 3x + 108$, the principal polynomial of discriminant $-423$. With $u_{-423} = \left\lfloor \sqrt{423/3} \right\rfloor = 11$, we begin by compiling the following values.

| $x$ | $-1,-2$ | $0,-3$ | $1,-4$ | $2,-5$ | $3,-6$ | $4,-7$ |
|---|---|---|---|---|---|---|
| $\phi(x)$ | 106 | 108 | 112 | 118 | 126 | 136 |

Here we find that there are fifteen reduced forms of discriminant $-423$:

$$\begin{array}{ccccc} (1:-1) & (2:-1) & (2:-2) & (4:0) & (4:-3) \\ (7:1) & (7:-4) & (8:1) & (8:-4) & (9:3) \\ (3:0) & (6:0) & (6:-3) & (9:0) & (9:-3). \end{array}$$

But those in the third row are $(3a : 3k)$, where $(a : k)$ is a reduced form of discriminant $-47$. These forms are not primitive, so are not elements of $G_3$. (See Exercises 6.1.1 and 6.1.2.) We can verify that the remaining ten are the reduced forms equivalent to the products calculated previously. For instance, with $\phi(-15) = 288 = 36 \cdot 8$, we find that $(36 : -15) \sim (8 : 12) \sim (8 : -4)$. ◊

**Example.** Let $\Delta = -47$ and $p = 5$. The sets $S_5$ and $K_5$ have been calculated previously in this section, and appear as the first row and first column, respectively, in the following array. The remaining entries are compositions of the row and column headings.

$$\begin{array}{ccccc} (1:0) & (2:0) & (2:-5) & (3:0) & (3:-5) \\ (25:0) & (50:0) & (50:-25) & (75:0) & (75:25) \\ (25:-5) & (50:20) & (50:-5) & (75:-30) & (75:-5) \\ (25:5) & (50:-20) & (50:5) & (75:30) & (75:-20) \\ (25:-10) & (50:-10) & (50:15) & (75:15) & (75:-35) \\ (25:10) & (50:10) & (50:-15) & (75:-15) & (75:10) \end{array}$$

The claim of Theorem 8.1.4 is that these thirty quadratic forms represent all elements of the form class group $\mathcal{F}_{-1175}$. Note that we could also use the reduced forms of $K_5$, which we calculated earlier, as the entries in the first column. But with $p^2$ relatively prime to $a$ for all elements $(a : pk)$ in $S_5$ by definition, the compositions in the preceding array are easier to calculate as given. ◊

**Exercise 8.1.5.** Verify that the thirty forms in the preceding example are distinct in $\mathcal{F}_{-1175}$ by finding the reduced form in $\mathcal{Q}_{-1175}$ to which each one is equivalent, and noting that they are all different.

**Exercise 8.1.6.** For each discriminant $\Delta$ and prime $p$, use the method of Theorem 8.1.4 to list the elements of the form class group $G_p = \mathcal{F}_{p^2\Delta}$. Verify the results by calculating the reduced forms of discriminant $p^2\Delta$ directly.

(a) $\Delta = -20$ and $p = 2$.

(b) $\Delta = -20$ and $p = 3$.

(c) $\Delta = -20$ and $p = 5$.

(d) $\Delta = -40$ and $p = 2$.

(e) $\Delta = -40$ and $p = 3$.

(f) $\Delta = -56$ and $p = 2$.

(g) $\Delta = -56$ and $p = 3$.

(h) $\Delta = -84$ and $p = 2$.

(i) $\Delta = -116$ and $p = 2$.

(j) $\Delta = -3$ and $p = 7$.

(k) $\Delta = -3$ and $p = 11$.

(l) $\Delta = -3$ and $p = 13$.

(m) $\Delta = -4$ and $p = 7$.

(n) $\Delta = -4$ and $p = 11$.

(o) $\Delta = -4$ and $p = 13$.

As a final example for this section, we illustrate how Theorem 8.1.4 can help us compute the form class group of an arbitrary quadratic subdomain from that of a complete quadratic domain.

**Example.** Consider the form class group of discriminant $\Delta(-1, 12) = -576$. Since Theorem 8.1.4 applies to arbitrary discriminants $\Delta$, we can use that result to build from $\mathcal{F}_{-4}$ to $\mathcal{F}_{-16}$ to $\mathcal{F}_{-64}$ and finally to $\mathcal{F}_{-576}$.

(1) Direct calculation shows that $\mathcal{F}_{-4} = \{(1 : 0)\}$. In the notation of Theorem 8.1.4, we then find that $S_2 = \{(1 : 0)\}$ and $K_2 = \{(1 : 0)\}$, so that $\mathcal{F}_{-16} = \{(1 : 0)\}$. (Note that $(4 : 0)$ is a potential element of $K_2$, but that $(4 : 0) \sim (1 : 0)$. The resulting value of $|K_2|$ is as predicted in Theorem 8.1.3.)

(2) Now we apply Theorem 8.1.4 with $\Delta = -16$ and $p = 2$. We have that $S_2 = \{(1 : 0)\}$, while $K_2 = \{(1 : 0), (4 : 2)\}$, which thus equals $\mathcal{F}_{-64}$. (Here with $\phi(x) = \phi_{-16}(x) = x^2 + 4$, we find that 2 does not divide $\phi(1)$, so that $(p^2 : pk) = (4 : 2)$ is an element of $K$.)

(3) Finally, we apply Theorem 8.1.4 with $\Delta = -64$ and $p = 3$. Now $S_3 = \{(1 : 0), (4 : 6)\}$, and we find that $K_3 = \{(1 : 0), (9 : 0), (9 : 3), (9 : -3)\}$, since $x^2 + 16 \equiv 0 \pmod 3$ has no solutions. The following array of products gives representatives of all form classes in $\mathcal{F}_{-576}$.

$$\begin{array}{cc} (1 : 0) & (4 : 6) \\ (9 : 0) & (36 : 18) \\ (9 : 3) & (36 : -6) \\ (9 : -3) & (36 : 6) \end{array}$$

The following exercise verifies these results. ◊

**Exercise 8.1.7.** Find all reduced forms of discriminant $-576$ by direct calculation. Identify the primitive reduced forms, and verify that each of the forms in the preceding example is equivalent to one of those reduced forms. (Note that the index of a quadratic form of discriminant $\Delta(-1, 12) = -576$ might be any divisor of 12.)

## 8.2 Projection Homomorphisms

In Theorem 8.1.4, we stated that a class group of quadratic forms of discriminant $p^2\Delta$ can be computed in terms of two of its subsets, $S_p$ and $K_p$, which in turn are constructed from the class group and principal polynomial of discriminant $\Delta$. To prove that claim in this section, we will go in the opposite direction, assuming that $\mathcal{F}_{p^2\Delta}$ is known, and projecting it onto the group $\mathcal{F}_\Delta$ with a particular homomorphism. The subsets $S_p$ and $K_p$ are redefined in terms of that function, and our main theorem is then a consequence of general properties of group homomorphisms. We proceed as follows.

If $f(x, y) = ax^2 + bxy + cy^2$ is a quadratic form of discriminant $\Delta$, let

$$f_p(x, y) = ax^2 + pbxy + p^2cy^2.$$

The discriminant of $f_p(x, y)$ is $p^2\Delta$, and $f_p(x, y)$ is primitive if and only if $f(x, y)$ is primitive and $p$ does not divide $a$. In ideal notation, we find that if $f = (a : k)$, then $f_p = (a : pk)$. The following proposition indicates that all elements of $G_p = \mathcal{F}_{p^2\Delta}$ can be represented by quadratic forms of this type.

**Proposition 8.2.1.** *Every primitive quadratic form $g$ of discriminant $p^2\Delta$ is equivalent to some form $f_p = (a : pk)$, where $p$ does not divide $a$.*

*Proof.* Since $g$ is primitive, it properly represents an integer $a$ not divisible by $p$, and we can then assume that $a$ is the coefficient of $x^2$ in $g(x, y)$. In ideal notation, then $g = (a : \ell)$ for some integer $\ell$. If $\gcd(a, p) = 1$, then the congruence $px \equiv \ell \pmod{a}$ has a solution $k$, and so $g$ is norm equivalent to $f_p = (a : pk)$. □

Let $\phi(x)$ and $\phi_p(x)$ be the principal polynomials of discriminant $\Delta$ and $p^2\Delta$, respectively. If $(a : pk)$ is a quadratic form of discriminant $p^2\Delta$, then $a$ divides $\phi_p(pk) = p^2\phi(k)$. Since $\gcd(a, p) = 1$, it follows that $a$ divides $\phi(k)$, and so $(a : k)$ is a quadratic form of discriminant $\Delta$. Thus we can define a function as in the following theorem.

**Theorem 8.2.2.** *Let $\Delta$ be a discriminant, let $p$ be a prime number, and let $G = \mathcal{F}_\Delta$ and $G_p = \mathcal{F}_{p^2\Delta}$. Then the function $\psi : G_p \to G$ given by $\psi([f_p]) = [f]$, where*

*$f_p = (a : pk)$ and $f = (a : k)$ for some $a$ not divisible by $p$, is a well-defined, surjective homomorphism. That is, $\psi([f_p]\cdot[g_p]) = [f]\cdot[g]$ for every pair of elements $[f_p]$ and $[g_p]$ in $G_p$, and every element of $G$ can be written as $\psi([f_p])$ for some $[f_p]$ in $G_p$.*

**Definition.** We refer to $\psi$ as the *projection homomorphism* from $\mathcal{F}_{p^2\Delta}$ onto $\mathcal{F}_\Delta$.

**Example.** Let $\Delta = -40$ and $p = 3$, so that $p^2\Delta = -360$. The reduced quadratic forms of discriminant $\Delta$ are $(1 : 0)$ and $(2 : 0)$. For $p^2\Delta$, the principal polynomial is $\phi_p(x) = x^2 + 90$, with $u_\Delta = \left\lfloor \sqrt{360/3} \right\rfloor = 10$. From the table

| $k$ | 0 | $\pm1$ | $\pm2$ | $\pm3$ | $\pm4$ | $\pm5$ |
|---|---|---|---|---|---|---|
| $\phi_p(k)$ | 90 | 91 | 94 | 99 | 106 | 115 |

we find the following eight *primitive* reduced forms of discriminant $-360$:

$$(1 : 0), \quad (2 : 0), \quad (5 : 0), \quad (7 : 1), \quad (7 : -1), \quad (9 : 0), \quad (9 : 3), \quad (9 : -3).$$

(The forms $(3 : 0)$ and $(6 : 0)$ are also reduced, but not primitive.) To apply the projection homomorphism to $\mathcal{F}_{-360}$, we must replace each $(9 : \ell)$ by an equivalent form $(a : 3k)$ with 3 not dividing $a$. We find, for instance, that since $\phi_p(-3) = 9 \cdot 11$, then $(9 : -3) \sim (11 : 3)$. The forms $(7 : 1)$ and $(7 : -1)$ can be replaced by the equivalent forms $(7 : -6)$ and $(7 : 6)$, respectively. We note the effect of the projection homomorphism from $G_p = \mathcal{F}_{-360}$ to $G = \mathcal{F}_{-40}$ in the following diagram.

$$\begin{array}{cccccc} & & & & \psi & \\ (1 : 0) & (10 : 0) & (11 : 3) & (11 : -3) & \longrightarrow & (1 : 0) \\ (2 : 0) & (5 : 0) & (7 : 6) & (7 : -6) & \longrightarrow & (2 : 0) \end{array}$$

For example, $(7 : 6)$ is sent by $\psi$ to $(7 : 2)$ in $\mathcal{Q}_{-40}$. With $\phi(x) = x^2 + 10$, we find that $(7 : 2) \sim (2 : -2) \sim (2 : 0)$. ◊

**Exercise 8.2.1.** For each discriminant $\Delta$ and prime $p$ below, find all reduced forms of discriminant $\Delta$ and of discriminant $p^2\Delta$ by direct calculation, and describe the projection homomorphism $\psi$ from $\mathcal{F}_{p^2\Delta}$ to $\mathcal{F}_\Delta$.

(a) $\Delta = -4$ and $p = 7$.

(b) $\Delta = -4$ and $p = 13$.

(c) $\Delta = -7$ and $p = 3$.

(d) $\Delta = -7$ and $p = 5$.

(e) $\Delta = -7$ and $p = 11$.

(f) $\Delta = -15$ and $p = 3$.

(g) $\Delta = -15$ and $p = 5$.

(h) $\Delta = -15$ and $p = 7$.

(i) $\Delta = -20$ and $p = 3$.

(j) $\Delta = -20$ and $p = 7$.

(k) $\Delta = -23$ and $p = 3$.

(l) $\Delta = -23$ and $p = 5$.

(m) $\Delta = -24$ and $p = 3$.

(n) $\Delta = -24$ and $p = 5$.

The proof of Theorem 8.2.2 requires the following preliminaries. Recall that $\Gamma$ is the group of all unimodular matrices, that is, $2 \times 2$ matrices having integer entries and determinant 1.

**Definition.** For a fixed prime $p$, let

$$\Gamma_p = \left\{ \begin{bmatrix} q & s \\ r & t \end{bmatrix} \in \Gamma \mid p \text{ divides } r \right\}.$$

We refer to $\Gamma_p$ as the *p-congruence subgroup* of $\Gamma$. If $f$ and $g$ are quadratic forms of some discriminant $\Delta$, we say that $f$ is *p-equivalent* to $g$, and write $f \sim_p g$, if $g = f \circ U$ for some $U$ in $\Gamma_p$.

**Exercise 8.2.2.** Verify that $\Gamma_p$ is a subgroup of $\Gamma$. Explain why it follows that $\sim_p$ is an equivalence relation on $\mathcal{Q}_\Delta$ for every $\Delta$, and that if $f \sim_p g$, then $f \sim g$ is true as well.

**Proposition 8.2.3.** *Let $U$ be a unimodular matrix. If $U$ is not in the subgroup $\Gamma_p$, then there is an integer $k$ so that $U = U_k \cdot V$, where $U_k = \begin{bmatrix} k & -1 \\ 1 & 0 \end{bmatrix}$ and $V$ is in $\Gamma_p$.*

*Proof.* Let $U = \begin{bmatrix} q & s \\ r & t \end{bmatrix}$ be unimodular. If $U$ is not in $\Gamma_p$, so that $p$ does not divide $r$, then the congruence $rx \equiv q \pmod{p}$ has a solution $k$. In this case, we find that

$$U = \begin{bmatrix} q & s \\ r & t \end{bmatrix} = \begin{bmatrix} k & -1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} r & t \\ rk - q & tk - s \end{bmatrix} = U_k \cdot V,$$

with $V$ in $\Gamma_p$ since $p$ divides $rk - q$. □

Since the solution of $rx \equiv q \pmod{p}$ is unique when $p$ does not divide $r$, we find that, in group terminology, the matrices $U_k$ with $k$ in $\mathbb{Z}_p$ together with the identity matrix form a set of representatives for the left cosets of $\Gamma_p$ in $\Gamma$. Thus there are $p + 1$ such cosets.

**Proposition 8.2.4.** *Let $\phi(x)$ be the principal polynomial of some discriminant $\Delta$ and let $f$ be an element of $\mathcal{Q}_\Delta$. Then $f$ is equivalent to the principal form $\phi = (1 : 0)$ if and only if $f$ is $p$-equivalent either to $(1 : 0)$ or to $(\phi(k) : k)$ for some integer $k$.*

*Proof.* We find that $(\phi(k) : k) \circ U = (1 : 0)$ if $U = \begin{bmatrix} 0 & -1 \\ 1 & k+\varepsilon \end{bmatrix}$, with $\varepsilon = \varepsilon_\Delta$, so that $(\phi(k) : k)$ is equivalent to $(1 : 0)$. If $f$ is $p$-equivalent to $(\phi(k) : k)$ for some $k$, then $f$ is equivalent to $(\phi(k) : k)$ and so to $(1 : 0)$.

Conversely, suppose that $f$ is equivalent to $\phi = (1 : 0)$, say with $M_f = U^T M_\phi U$ for some unimodular matrix $U$. If $U$ is in the subgroup $\Gamma_p$, then $f$ is $p$-equivalent to $(1 : 0)$ by definition. If $U$ is not in $\Gamma_p$, then $U = U_k \cdot V$ as in Proposition 8.2.3, so that $M_f = V^T(U_k^T M_\phi U_k)V$, that is, $f$ is $p$-equivalent to $(1 : 0) \circ U_k$. But $(1 : 0) \circ U_k = (\phi(k) : -k - \varepsilon)$ by Proposition 4.2.1. Since $\phi(k) = \phi(-k - \varepsilon)$, we can also say that $f$ is $p$-equivalent to some $(\phi(k) : k)$. □

**Proposition 8.2.5.** *Let $f$ and $g$ be elements of $\mathcal{Q}_\Delta$ for some discriminant $\Delta$, with $f_p$ and $g_p$ the corresponding elements of $\mathcal{Q}_{p^2\Delta}$. Then $f$ is $p$-equivalent to $g$ if and only if $f_p$ is equivalent to $g_p$.*

*Proof.* Note that $M_{f_p} = P^T M_f P$, where $P = \begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix}$. (Recall that if $f(x, y) = ax^2 + bxy + cy^2$, then $f_p(x, y) = ax^2 + pbxy + p^2cy^2$. Here $P$ is not a unimodular matrix since $\det P = p$.) Similarly, $M_{g_p} = P^T M_g P$. Suppose that $f$ is $p$-equivalent to $g$, say with $M_g = U^T M_f U$, where

$$U = \begin{bmatrix} q & s \\ pr & t \end{bmatrix}$$

in $\Gamma_p$. Then we find that $M_{g_p} = (P^{-1}UP)^T M_{f_p}(P^{-1}UP)$, where

$$P^{-1}UP = \begin{bmatrix} 1 & 0 \\ 0 & 1/p \end{bmatrix} \cdot \begin{bmatrix} q & s \\ pr & t \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix} = \begin{bmatrix} q & ps \\ r & t \end{bmatrix}$$

is a unimodular matrix. Thus $f_p$ is equivalent to $g_p$.

Conversely, suppose that $g_p = f_p \circ U$ for some unimodular matrix $U$. With $f_p(x, y) = ax^2 + pbxy + p^2cy^2$ and the coefficient of $y^2$ in $g_p$ divisible by $p^2$, we find that

$$U = \begin{bmatrix} q & ps \\ r & t \end{bmatrix}$$

for some integers $q$, $r$, $s$, and $t$ for which $qt - r \cdot ps = 1$. (If $p$ does not divide $x$, then $p^2$ cannot divide $f_p(x, y)$.) Now $M_{g_p} = U^T M_{f_p} U$ implies that $M_g = (PUP^{-1})^T M_f (PUP^{-1})$, and since

$$PUP^{-1} = \begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix} \cdot \begin{bmatrix} q & ps \\ r & t \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1/p \end{bmatrix} = \begin{bmatrix} q & s \\ pr & t \end{bmatrix}$$

is a unimodular matrix in $\Gamma_p$, then $f$ is $p$-equivalent to $g$. □

*Proof of Theorem* 8.2.2. As we saw in Proposition 8.2.1, every element of $G_p = \mathcal{F}_{p^2\Delta}$ can be written as $[f_p]$, where $f_p = (a : pk)$ with $a$ not divisible by $p$. In that case, $f = (a : k)$ is a primitive form of discriminant $\Delta$, and we let $\psi([f_p]) = [f]$. Proposition 8.2.5 shows that if $[f_p] = [g_p]$, then $f$ is $p$-equivalent to $g$, and so $[f] = [g]$. That is, $\psi$ is well-defined. Every primitive quadratic form of discriminant $\Delta$ properly represents an integer not divisible by $p$, and so each class in $\mathcal{F}_\Delta$ can be written as $[f]$ for some $f = (a : k)$ with $p$ not dividing $a$. In that case, $\psi([f_p]) = [f]$, so that $\psi$ is surjective.

Let $\phi(x)$ and $\phi_p(x)$ be the principal polynomials of discriminant $\Delta$ and $p^2\Delta$, respectively. Let $f_1 = (a : k)$ and $f_2 = (b : \ell)$ in $\mathcal{Q}_\Delta$, with $ab$ not divisible by $p$. Let $t = k + \ell + \phi'(0)$ and let $g = \gcd(a, b, t)$. Then $[f_1] \cdot [f_2]$ is represented by $f = (n : m)$, where $n = ab/g^2$ and $m$ satisfies the congruences

$$\begin{aligned}
\frac{a}{g} \cdot m &\equiv \frac{a}{g} \cdot \ell \pmod{n},\\
\frac{b}{g} \cdot m &\equiv \frac{b}{g} \cdot k \pmod{n},\\
\frac{t}{g} \cdot m &\equiv \frac{1}{g}(k\ell - \phi(0)) \pmod{n}.
\end{aligned}$$

Let $(f_1)_p = (a : pk)$ and $(f_2)_p = (b : p\ell)$, and consider $[(f_1)_p] \cdot [(f_2)_p]$. Note that $pk + p\ell + \phi_p'(0) = pk + p\ell + p\phi'(0) = pt$, and that $\gcd(a, b, pt) = g$, since $p$ divides neither $a$ nor $b$. Thus we find that this class product is represented by $(n : m_p)$, where $n = ab/g^2$ as above, and $m_p$ satisfies

$$\begin{aligned}
\frac{a}{g} \cdot m_p &\equiv \frac{a}{g} \cdot p\ell \pmod{n},\\
\frac{b}{g} \cdot m_p &\equiv \frac{b}{g} \cdot pk \pmod{n},\\
\frac{pt}{g} \cdot m_p &\equiv \frac{1}{g}(pk \cdot p\ell - \phi_p(0)) \equiv \frac{1}{g} \cdot p^2(k\ell - \phi(0)) \pmod{n}.
\end{aligned}$$

We find that $m_p = pm$ satisfies each congruence. It follows that

$$\psi([(f_1)_p] \cdot [(f_2)_p]) = \psi([f_p]) = [f] = [f_1] \cdot [f_2] = \psi([(f_1)_p]) \cdot \psi([(f_2)_p]),$$

so that $\psi$ is a homomorphism. □

We can now prove Theorem 8.1.4 by relating the subsets $S_p$ and $K_p$ of that theorem to groups associated with a projection homomorphism.

**Definition.** If $\psi : \mathcal{F}_{p^2\Delta} \to \mathcal{F}_\Delta$ is a projection homomorphism, then the *kernel* of $\psi$ equals the set of all $[f_p]$ in $\mathcal{F}_{p^2\Delta}$ for which $\psi([f_p]) = [\phi]$, where $\phi = (1 : 0)$ is the principal form of discriminant $\Delta$. We denote this set as $K(\Delta, p)$.

**Proposition 8.2.6.** *Let $\phi(x)$ be the principal polynomial of discriminant $\Delta$, let $p$ be a prime number, and let $K = K(\Delta, p)$ be the kernel of the projection homomorphism*

$\psi : \mathcal{F}_{p^2\Delta} \to \mathcal{F}_\Delta$. *Then $K$ consists of the distinct classes of the quadratic forms* $(1 : 0)$ *and* $(p^2 : pk)$ *in* $\mathcal{Q}_{p^2\Delta}$, *where $k$ is an integer for which $p$ does not divide $\phi(k)$.*

*Proof.* Proposition 8.2.4 states that $f$ in $\mathcal{Q}_\Delta$ is equivalent to $(1 : 0)$ if and only if $f$ is $p$-equivalent either to $(1 : 0)$ or to $(\phi(k) : k)$ for some integer $k$. Proposition 8.2.5 then implies that elements sent to the class of $(1 : 0)$ by a projection homomorphism can all be expressed as the class of $(1 : 0)$ or of $(\phi(k) : pk)$ in $\mathcal{F}_{p^2\Delta}$. Note that the latter forms are primitive, and so are elements of this class group, if and only if $\phi(k)$ is not divisible by $p$. Finally, if $\phi_p(x)$ is the principal polynomial of discriminant $p^2\Delta$, then $\phi_p(pk) = p^2\phi(k)$, so that $(\phi(k) : pk) \sim (p^2 : -pk - p\varepsilon)$, where $\varepsilon = \varepsilon_\Delta$, by an involution. Here $\phi(k) = \phi(-k - \varepsilon)$, so as $k$ varies over all integers for which $p$ does not divide $\phi(k)$, then $-k - \varepsilon$ does as well. □

Proposition 8.2.6 shows that the kernel of a projection homomorphism is the same as $K_p$, the kernel of $G_p$ as defined in §8.1. We can now prove Theorem 8.1.4 using standard facts from group theory, particularly the Fundamental Homomorphism Theorem, which we state and prove in Appendix C.

*Proof of Theorem* 8.1.4. Let $\Delta$ be a discriminant, let $p$ be a prime number, and let $G = \mathcal{F}_\Delta$ and $G_p = \mathcal{F}_{p^2\Delta}$. Let $\psi : G_p \to G$ be the projection homomorphism defined in this section, and write the kernel of $\psi$ as $K = K(\Delta, p)$. The set $G_p/K$ of all distinct cosets $[f] \cdot K$ of $K$ in $G_p$ forms a group under composition of quadratic form classes. Since $\psi$ is surjective, the Fundamental Homomorphism Theorem implies that $G_p/K$ is isomorphic to $G$. Every element of $G$ can be written as the class of some form $(a : k)$ with $p$ not dividing $a$, and so every coset in $G_p/K$ is represented by the corresponding form $(a : pk)$. In particular, the forms of that type must be distinct in $G_p$. We can identify this set of coset representatives with the set $S_p$ as defined in §8.1. So all elements of $G_p$ can be expressed as a product of an element of $S_p$ with an element of $K = K_p$, and all such products are distinct, by properties of cosets. □

## 8.3 The Kernel of a Projection Homomorphism

Let $\phi(x)$ be the principal polynomial of some discriminant $\Delta$ and let $p$ be a prime number. In the proof of Proposition 8.2.6, we found that the kernel $K = K(\Delta, p)$ of a projection homomorphism from $\mathcal{F}_{p^2\Delta}$ onto $\mathcal{F}_\Delta$ consists of the *distinct* classes of quadratic forms $(1 : 0)$ and $(\phi(k) : pk)$, where $k$ is an integer for which $p$ does not divide $\phi(k)$. (This description of the elements of $K$ will be most useful in this section.) To conclude Chapter 8, we determine a criterion for when quadratic forms of this type are equivalent, using automorphs of the principal quadratic form of discriminant $\Delta$. In this way, we can prove Theorem 8.1.3, calculating $|K|$

when $\Delta$ is negative, and we lay the groundwork for a description of $|K|$ when $\Delta$ is positive, which we consider in §13.3.

Throughout this section, let $\phi(x) = x^2 + \varepsilon x + \frac{\varepsilon^2 - \Delta}{4}$ be the principal polynomial of some discriminant $\Delta$. To simplify notation, we will write $\phi(0)$ as $c$ and $\phi'(0)$ as $b$, so that $\phi(x) = x^2 + bx + c$ for all $x$. For the proof of our main result, it will be convenient to introduce a finite group of matrices. This definition assumes properties of matrices with entries in a finite field, and requires the concept of factor groups. (See Appendix C for more details on this terminology.) A concrete description of this group appears in Proposition 8.3.1.

**Definition.** Let $p$ be a prime number, and consider the group $GL_2(\mathbb{Z}_p)$ of nonsingular matrices with entries in $\mathbb{Z}_p$. The set $N = \{aI \mid a \in \mathbb{Z}_p^\times\}$ of nonzero scalar matrices is a normal subgroup of $GL_2(\mathbb{Z}_p)$. We write the typical element of the factor group $GL_2(\mathbb{Z}_p)/N$ as $[A]$, so that $[A] = [B]$ if and only if $A = aB$ for some $a \neq 0$ in $\mathbb{Z}_p$.

**Proposition 8.3.1.** *Let $\phi(x) = x^2 + bx + c$ be the principal polynomial of some discriminant $\Delta$ and let $p$ be a prime number. For each $k$ in $\mathbb{Z}_p$, let*

$$A_k = \begin{bmatrix} k & -c \\ 1 & k+b \end{bmatrix}.$$

*If $I$ is the $2 \times 2$ identity matrix, then the set of classes*

$$G(\Delta, p) = \{[I]\} \cup \{[A_k] \mid k \in \mathbb{Z}_p \text{ and } \phi(k) \neq 0 \text{ in } \mathbb{Z}_p\}$$

*is an abelian subgroup of $GL_2(\mathbb{Z}_p)/N$.*

We call $G(\Delta, p)$ the *$p$-matrix group of discriminant $\Delta$*. Note that the determinant of $A_k$ is $\phi(k)$, so that $A_k$ is in $GL_2(\mathbb{Z}_p)$ if and only if $p$ does not divide $\phi(k)$.

*Proof.* If $k$ and $\ell$ are elements of $\mathbb{Z}_p$ for which $p$ divides neither $\phi(k)$ nor $\phi(\ell)$, then $A_k \cdot A_\ell$ equals

$$\begin{bmatrix} k & -c \\ 1 & k+b \end{bmatrix} \cdot \begin{bmatrix} \ell & -c \\ 1 & \ell+b \end{bmatrix} = \begin{bmatrix} k\ell - c & -c(k+\ell+b) \\ k+\ell+b & (k\ell - c) + b(k+\ell+b) \end{bmatrix}.$$

If $k + \ell + b = 0$, then $[A_k] \cdot [A_\ell] = [I]$. In particular, $[A_k]^{-1} = [A_{-k-b}]$. On the other hand, if $k + \ell + b \neq 0$, then $[A_k] \cdot [A_\ell] = [A_m]$, where $m$ satisfies $(k + \ell + b)m \equiv k\ell - c \pmod{p}$. Thus $G(\Delta, p)$ is a subgroup of $GL_2(\mathbb{Z}_p)/N$, and we see that $[A_k] \cdot [A_\ell] = [A_\ell] \cdot [A_k]$. □

The number of elements in $G(\Delta, p)$ is $p + 1 - n_p(\phi)$, where $n_p(\phi)$ is the number of solutions of $\phi(x) \equiv 0 \pmod{p}$.

**Proposition 8.3.2.** *Let $\phi(x,y) = x^2 + bxy + cy^2$ be the principal form of some discriminant $\Delta$ and let* $\mathrm{Aut}(\phi)$ *be the group of automorphs of $\phi$. Then for every prime $p$, there is a homomorphism $\chi_p : \mathrm{Aut}(\phi) \to G(\Delta, p)$ defined by $\chi_p(U) = [U]$.*

We call $\chi_p$ the *$p$-automorph map* on $\mathrm{Aut}(\phi)$.

*Proof.* If $U = \begin{bmatrix} q & s \\ r & t \end{bmatrix}$ is an automorph of $\phi(x,y) = x^2 + bxy + cy^2$, then Proposition 4.3.4 shows that $s = -cr$ and $t = q + br$. We find that if $p$ divides $r$, then $[U] = [I]$, while if $p$ does not divide $r$, then $[U] = [A_{qr^{-1}}]$, in the notation of Proposition 8.3.1. Note that since $U$ has determinant 1, the class $[U]$ is an element of $G(\Delta, p)$ in every case. In particular, $\phi(U) = [A_k]$ if and only if $rk \equiv q \pmod{p}$. Now

$$\chi_p(UV) = [UV] = [U] \cdot [V] = \chi_p(U)\chi_p(V)$$

for all $U$ and $V$, and so $\chi_p$ is a homomorphism from $\mathrm{Aut}(\phi)$ to $G(\Delta, p)$. □

Notice that the kernel of $\chi_p$ equals $\mathrm{Aut}(\phi) \cap \Gamma_p$. We denote the image of $\mathrm{Aut}(\phi)$ under $\chi_p$ as $H(\Delta, p)$. By general properties of group homomorphisms, $H(\Delta, p)$ is a subgroup of $G(\Delta, p)$, and so $|H(\Delta, p)|$ divides $|G(\Delta, p)|$. When $\Delta$ is negative, we can describe $H(\Delta, p)$ for every prime $p$ as follows.

**Proposition 8.3.3.** *Let $\phi(x,y)$ be the principal form of some negative discriminant $\Delta$ and let $p$ be a prime number. If $H(\Delta, p)$ is the image of* $\mathrm{Aut}(\phi)$ *under $\chi_p$ as above, then*

$$H(\Delta, p) = \begin{cases} \{[I], [A_0], [A_{-1}]\}, & \text{if } \Delta = -3, \\ \{[I], [A_0]\}, & \text{if } \Delta = -4, \\ \{[I]\}, & \text{if } \Delta < -4. \end{cases}$$

*Proof.* If $\Delta = -3$, then $\phi(x,y) = x^2 + xy + y^2$, and so

$$\mathrm{Aut}(\phi) = \left\{ \pm \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \pm \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}, \pm \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix} \right\}$$

by Theorem 6.1.4. Note that $\chi_p(U) = \chi_p(-U)$ for every automorph $U$, since $[U] = [-U]$ in $GL_2(\mathbb{Z}_p)/N$. So we see immediately that $H(-3, p) = \{[I], [A_0], [A_{-1}]\}$. Note that if $\phi(x) = x^2 + x + 1$, then $\phi(0) = 1 = \phi(-1)$, so these three elements are distinct in $G(-3, p)$ for every prime $p$.

Similarly, if $\Delta = -4$, then $\phi(x,y) = x^2 + y^2$, and

$$\mathrm{Aut}(\phi) = \left\{ \pm \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \pm \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \right\}.$$

Here we find immediately that $H(-4, p) = \{[I], [A_0]\}$, with these two elements distinct in $G(-4, p)$ for every prime $p$.

Finally, if $\Delta < -4$, then $\phi(x, y) = x^2 + bxy + cy^2$ with $c \neq 1$. Thus $\mathrm{Aut}(\phi) = \{\pm I\}$, and so $H(\Delta, p) = \{[I]\}$ for all primes $p$. □

We now prove two lemmas that describe all equivalences among the elements of $K(\Delta, p)$, the kernel of a projection homomorphism.

**Lemma 8.3.4.** *Let $\phi(x)$ be the principal polynomial of some discriminant $\Delta$ and let $p$ be a prime number. Let $k$ be an element of $\mathbb{Z}_p$ for which $p$ does not divide $\phi(k)$, so that $(\phi(k) : pk)$ is an element of $K = K(\Delta, p)$, the kernel of the projection homomorphism from $\mathcal{F}_{p^2\Delta}$ onto $\mathcal{F}_\Delta$. Then $(\phi(k) : pk)$ is equivalent to $(1 : 0)$ if and only if $[A_k]$ is an element of $H(\Delta, p)$, the image of a $p$-automorph map.*

*Proof.* Proposition 8.2.5 shows that $(\phi(k) : pk)$ is equivalent to $(1 : 0)$ in $\mathcal{Q}_{p^2\Delta}$ if and only if $\phi_k = (\phi(k) : k)$ is $p$-equivalent to $\phi = (1 : 0)$ in $\mathcal{Q}_\Delta$. If

$$V_k = \begin{bmatrix} -k - b & -1 \\ 1 & 0 \end{bmatrix}, \tag{8.3.1}$$

where $b = \phi'(0)$, then we find that $\phi_k = \phi \circ V_k$. (See Exercise 8.3.1 below.) Proposition 4.3.5 now implies that $\phi_k = \phi \circ W$ if and only if $W = UV_k$, where $U$ is an automorph of $\phi$. But

$$UV_k = \begin{bmatrix} q & -rc \\ r & q + br \end{bmatrix} \cdot \begin{bmatrix} -k - b & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} q(-k - b) - rc & -q \\ q - kr & -r \end{bmatrix}$$

is in the group $\Gamma_p$ if and only if $rk \equiv q \pmod{p}$. That is, $\phi_k$ is $p$-equivalent to $\phi$ if and only if an automorph $U$ of $\phi$ exists so that $\chi_p(U) = [A_{qr^{-1}}] = [A_k]$. This is the case if and only if $[A_k]$ is an element of $H(\Delta, p)$, the image of $\mathrm{Aut}(\phi)$ under $\chi_p$. □

**Exercise 8.3.1.** Verify that $\phi_k = \phi \circ V_k$, where $V_k$ is defined as in (8.3.1).

**Lemma 8.3.5.** *Let $\phi(x)$ be the principal polynomial of some discriminant $\Delta$ and let $p$ be a prime number. Let $k$ and $\ell$ be distinct elements of $\mathbb{Z}_p$ for which $p$ divides neither $\phi(k)$ nor $\phi(\ell)$. Then $(\phi(k) : pk)$ is equivalent to $(\phi(\ell) : p\ell)$ in $K(\Delta, p)$ if and only if $[A_k]^{-1} \cdot [A_\ell]$ is an element of $H(\Delta, p)$.*

*Proof.* Proposition 8.2.5 implies that $(\phi(k) : pk)$ is equivalent to $(\phi(\ell) : p\ell)$ in $\mathcal{Q}_{p^2\Delta}$ if and only if $\phi_k = (\phi(k) : k)$ is $p$-equivalent to $\phi_\ell = (\phi(\ell) : \ell)$ in $\mathcal{Q}_\Delta$. We find that $\phi_\ell = \phi_k \circ V_{\ell,k}$, where

$$V_{\ell,k} = \begin{bmatrix} 1 & 0 \\ \ell - k & 1 \end{bmatrix}. \tag{8.3.2}$$

Now Proposition 4.3.5 implies that $\phi_\ell = \phi_k \circ W$ if and only if $W = VV_{\ell,k}$, where $V$ is an automorph of $\phi_k$. The same proposition shows that every such automorph $V$ has the form $V = V_k^{-1}UV_k$, where $V_k$ is defined as in equation (8.3.1) and $U$ is an automorph of $\phi = (1 : 0)$. Direct calculation shows that if $U$ is written as in the proof of Lemma 8.3.4, then the lower left-hand entry of $(V_k^{-1}UV_k)V_{\ell,k}$ is

$$q(\ell - k) + r(c + (k + b)\ell). \tag{8.3.3}$$

On the other hand,

$$\begin{aligned}[A_k]^{-1} \cdot [A_\ell] &= \begin{bmatrix} -k-b & -c \\ 1 & -k \end{bmatrix} \cdot \begin{bmatrix} \ell & -c \\ 1 & \ell + b \end{bmatrix} \\ &= \begin{bmatrix} -(c + (k+b)\ell) & (-c(\ell - k) \\ \ell - k & -(c + k + b)\ell) + (\ell - k)b \end{bmatrix} = [A_m]\end{aligned}$$

if and only if $(\ell - k)m \equiv -(c + (k + b)\ell) \pmod{p}$. Thus $\phi_k$ is $p$-equivalent to $\phi_\ell$ if and only if there is an automorph $U = \begin{bmatrix} q & -rc \\ r & q + br \end{bmatrix}$ of $\phi$ for which $p$ divides the expression in (8.3.3), which is true if and only if $\chi_p(U) = [A_{qr^{-1}}] = [A_m] = [A_k]^{-1} \cdot [A_\ell]$. □

**Exercise 8.3.2.** If $V_{\ell,k}$ is defined as in (8.3.2), verify that $\phi_\ell = \phi_k \circ V_{\ell,k}$.

**Theorem 8.3.6.** *Let $\Delta$ be a discriminant and let $p$ be a prime number. Let $K(\Delta, p)$ be the kernel of the projection homomorphism $\psi : \mathcal{F}_{p^2\Delta} \to \mathcal{F}_\Delta$. Let $H(\Delta, p)$ be the image of the $p$-automorph map $\chi_p : \mathrm{Aut}(\phi) \to G(\Delta, p)$, where $\phi(x, y)$ is the principal form of discriminant $\Delta$, and $G(\Delta, p)$ is the $p$-matrix group of discriminant $\Delta$. Then*

$$|K(\Delta, p)| = \frac{|G(\Delta, p)|}{|H(\Delta, p)|}. \tag{8.3.4}$$

*Proof.* Taken together, Lemmas 8.3.4 and 8.3.5 imply that two potential elements of the kernel $K(\Delta, p)$ are equal if and only if corresponding elements of $G(\Delta, p)$ are in the same coset of the subgroup $H(\Delta, p)$. Thus the number of elements in $K(\Delta, p)$ equals the number of such cosets, which is the quotient in equation (8.3.4). □

Now the proof of Theorem 8.1.3 is a straightforward observation.

*Proof of Theorem* 8.1.3. Let $\Delta$ be a negative discriminant and let $p$ be a prime number. We have noted above that the number of elements in the group $G(\Delta, p)$ is $p + 1 - n_p(\phi)$, where $\phi(x)$ is the principal polynomial of discriminant $\Delta$. It follows that

$$|G(\Delta, p)| = p - \left(\frac{\Delta}{p}\right)$$

for every prime $p$. From Proposition 8.3.3, we have that

$$s = |H(\Delta, p)| = \begin{cases} 3, & \text{if } \Delta = -3, \\ 2, & \text{if } \Delta = -4, \\ 1, & \text{if } \Delta < -4. \end{cases}$$

The formulas of Theorem 8.1.3 follow immediately from Theorem 8.3.6. □

## Class Groups of Quadratic Subdomains—Review

We demonstrated in this chapter that the form class group of a quadratic subdomain (that is, $\mathcal{F}_{\Delta_1}$, where $\Delta_1 = \Delta(d, \gamma)$ for some $\gamma > 1$) can be constructed from the class group of the corresponding complete quadratic domain ($\mathcal{F}_\Delta$ with $\Delta = \Delta(d, 1)$) in a systematic approach. Specifically, the method allows us to compute $\mathcal{F}_{p^2\Delta}$ from $\mathcal{F}_\Delta$ when $\Delta$ is an arbitrary discriminant and $p$ is prime.

(1) If $\Delta$ is a discriminant and $p$ is prime, then we can compute the form class group $G_p = \mathcal{F}_{p^2\Delta}$ as products of elements of two subsets, $S_p$ and $K_p$, of $G_p$.

(2) The subsets $S_p$ and $K_p$ can be determined explicitly using the principal polynomial $\phi(x)$ of discriminant $\Delta$. The number of elements in $S_p$ is the same as the number of elements in the class group $\mathcal{F}_\Delta$. When $\Delta$ is negative, we have a formula (Theorem 8.1.3) for the number of elements in $K_p$.

(3) When $\Delta$ is a discriminant and $p$ is prime, then the subsets $S_p$ and $K_p$ can also be described in terms of a homomorphism $\psi$ (which we call the *projection homomorphism*) from the form class group $G_p = \mathcal{F}_{p^2\Delta}$ onto $\mathcal{F}_\Delta$. Specifically, $K_p = K(\Delta, p)$ is the kernel of $\psi$, and $S_p$ can be viewed as a collection of representatives for the cosets in $G_p/K_p$. The number of elements in $K_p$ is related to the group of automorphs of $\phi(x, y)$, the principal form of discriminant $\Delta$.

Thus, in theory, we can restrict our attention to constructing class groups (of ideals or quadratic forms) of discriminant $\Delta$ when $\Delta$ is *primitive*.

# Part Four: Indefinite Quadratic Forms

**Overview.** In Part Three, we developed a method of constructing the ideal class group of an arbitrary negative discriminant, and we applied the structure of these groups to representations of integers by positive definite quadratic forms having the same discriminant. We now shift our attention to positive discriminants, with the same goals of describing class groups of ideals and representations of integers by *indefinite* quadratic forms. There are several ways in which this situation is different, and more difficult, than the negative discriminant case.

(1) We have seen that when $\Delta$ is positive, then the quadratic domain $D_\Delta$ may have infinitely many units, making it more difficult to recognize associate elements in this domain. We show in Chapter 11 that this is, in fact, always true for a quadratic domain of positive discriminant, and we will demonstrate a method by which we can construct all units of such a domain.

(2) While it is again possible to place an upper bound on norms of representatives of ideal classes, as we saw was the case for negative discriminants, we will see that quite often there are additional equivalences among ideals satisfying those restrictions. In Chapter 10, we develop a method by which we can test for all such equivalences among potential representatives.

(3) It is typically impossible to test our conclusions on the existence of representations of an integer by an indefinite quadratic form with explicit calculations. For instance, while it is a trivial matter to test whether an equation such as $5x^2 + 7y^2 = 247$ has integer solutions by trial-and-error, there is no immediate upper bound on values of $x$ and $y$ in possible solutions $(x, y)$ of $-5x^2+7y^2 = 247$. We will address this type of situation in Chapter 11.

As a way of approaching each of the problems above, we first study a classical method of approximating real numbers by sequences of rational numbers, called *simple continued fractions*. We develop the basic properties of continued fractions in Chapter 9, proving that every real number has an expression in this form, and conversely that every simple continued fraction converges to some real number.

We will see that every real *quadratic* number has a *periodic* continued fraction expansion, in which there is a repetition of terms after a certain point.

Chapter 10 begins with a definition of potential representatives for classes of quadratic forms of positive discriminant, and an algorithm that determines all possible additional equivalences among those forms. We show that this method is a special case of a more general algorithm by which we can compute the continued fraction expansion of an arbitrary irrational quadratic number. In this way, we find that we can construct the class group of all forms of a given positive discriminant—again genus equivalence provides additional information about the structure of this class group.

In Chapter 11, we apply the results of the preceding two chapters to representations of integers by indefinite quadratic forms. We associate a continued fraction with an arbitrary quadratic form $f(x, y)$ of positive discriminant, and we show how the convergents of that continued fraction provide solutions of $f(x, y) = n$ for small values of $n$. Using this method, we systematically determine all units in a quadratic domain $D_\Delta$ with $\Delta$ positive. We develop criteria for an integer to be represented by an indefinite quadratic form, using the structure of the class group of quadratic forms of a given positive discriminant. We also demonstrate how these representations can be constructed in practice, using the equivalence algorithm on quadratic forms developed in Chapter 10.

**Requirements for Part Four.** In its precise definition, the continued fraction expansion of an irrational real number is the limit of a recursively defined sequence of rational numbers. We assume that the reader is familiar with the concept of convergence of a sequence $\{r_n\}_{n=1}^{\infty}$ to a real number $L$. We require the following key definition and claim, typically proved in a real analysis class.

**Definition.** A sequence $r_1, r_2, r_3, \ldots$ of real numbers is called a *Cauchy sequence* if it satisfies the following condition: for every real number $\epsilon > 0$, there is a positive integer $N$ such that $|r_i - r_j| < \epsilon$ whenever $i$ and $j$ are greater than $N$.

We assume that every Cauchy sequence converges to a real number.

# 9

# Continued Fractions

In this chapter, we introduce a technique of approximating real numbers by sequences of rational numbers, called *continued fractions*. We provide an informal introduction to this topic in §9.1, and motivate its applications to quadratic number theory in §9.2, with the classical arithmetic problem known as Pell's equation. In the remaining sections of Chapter 9, we formally define infinite simple continued fractions and we establish a particular characterization of the continued fractions of irrational quadratic numbers.

## 9.1 Introduction to Continued Fractions

We can view the process of associating a continued fraction to an arbitrary real number as a generalization of the Euclidean algorithm.

**Example.** The following list of equations is a typical application of the Euclidean algorithm, in this case with $a = 345$ and $b = 158$.

$$\begin{array}{rcl} 345 &=& 158 \cdot 2 + 29 \\ 158 &=& 29 \cdot 5 + 13 \\ 29 &=& 13 \cdot 2 + 3 \\ 13 &=& 3 \cdot 4 + 1 \\ 3 &=& 1 \cdot 3 + 0 \end{array} \qquad \begin{array}{rcl} 29 &=& a(1) + b(-2) \\ 13 &=& a(-5) + b(11) \\ 3 &=& a(11) + b(-24) \\ 1 &=& a(-49) + b(107) \\ 0 &=& a(158) + b(-345) \end{array}$$

We can rewrite each equation in the left-hand column in terms of rational numbers, dividing both sides by the appropriate divisor in each equation.

$$\begin{array}{rcl@{\qquad}rcl}
\frac{345}{158} &=& 2+\frac{29}{158} & \frac{29}{158} &=& \frac{a}{b}-2 \\
\frac{158}{29} &=& 5+\frac{13}{29} & -\frac{13}{790} &=& \frac{a}{b}-\frac{11}{5} \\
\frac{29}{13} &=& 2+\frac{3}{13} & \frac{3}{1738} &=& \frac{a}{b}-\frac{24}{11} \\
\frac{13}{3} &=& 4+\frac{1}{3} & -\frac{1}{7742} &=& \frac{a}{b}-\frac{107}{49} \\
\frac{3}{1} &=& 3+\frac{0}{1} & 0 &=& \frac{a}{b}-\frac{345}{158}
\end{array} \tag{9.1.1}$$

In the right-hand column, we obtain a difference expression involving $a/b$ by dividing both sides by $b$ times the multiple of $a$ in each equation. Now by repeated substitution, we obtain the following equation for $a/b$:

$$\frac{345}{158} = 2+\frac{1}{158/29} = 2+\frac{1}{5+\frac{1}{29/13}} = 2+\frac{1}{5+\frac{1}{2+\frac{1}{13/3}}} = 2+\frac{1}{5+\frac{1}{2+\frac{1}{4+\frac{1}{3}}}}.$$

We refer to this expression as a continued fraction expansion for $\upsilon = \frac{345}{158}$. Finally for this example, note that the sequence of continued fractions

$$2, \qquad 2+\frac{1}{5}, \qquad 2+\frac{1}{5+\frac{1}{2}}, \qquad 2+\frac{1}{5+\frac{1}{2+\frac{1}{4}}}, \qquad 2+\frac{1}{5+\frac{1}{2+\frac{1}{4+\frac{1}{3}}}}$$

can be simplified as a corresponding sequence of rational numbers:

$$2, \qquad \frac{11}{5}, \qquad \frac{24}{11}, \qquad \frac{107}{49}, \qquad \frac{345}{158}.$$

The second column of equations in (9.1.1) shows that this sequence provides increasingly accurate rational approximations of $\upsilon = \frac{345}{158}$. ♢

Of course in this example $\upsilon$ is a rational number, so is its own best rational approximation. But we can generalize this approach when $\upsilon$ is an *irrational* number. As in the first column of equations in (9.1.1), we can write $\upsilon$ as an integer plus a "remainder" term, between 0 and 1, then take the reciprocal of that remainder, and continue these steps with the resulting real number. When $\upsilon$ is rational, as in our first example, we eventually obtain 0 as a remainder, and the process terminates at that point. When $\upsilon$ is irrational, this procedure produces (in theory) an infinite sequence of rational numbers, which we claim converges to $\upsilon$. We describe this algorithm more formally in the following definition. In this section, we look at examples that provide numerical evidence of our claim, which we will state and prove more precisely in §9.3 and §9.4.

**Definition.** Let $v$ be a real number. Define a sequence of real numbers $v_i$ and a sequence of integers $q_i$ for $i \geq 0$ in the following way. Let $v_0 = v$, and for $i \geq 0$, let $q_i = \lfloor v_i \rfloor$ and $v_{i+1} = \frac{1}{v_i - q_i}$. (If $v_t = q_t$ for any $t \geq 0$, then both sequences terminate with the $t$-th term.) If

$$r_0 = q_0, \quad r_1 = q_0 + \frac{1}{q_1}, \quad r_2 = q_0 + \frac{1}{q_1 + \frac{1}{q_2}}, \quad r_3 = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{q_3}}}, \quad \ldots,$$

then $r_i$ is called the *i-th convergent* of $v$. We refer to the process that produces these sequences as the *continued fraction algorithm* for $v$.

Note that $q_0$ might be any integer, but that $q_i$ is a positive integer for $i > 0$, when it exists. To simplify notation, we also write $r_i$ as $\langle q_0, q_1, \ldots, q_i \rangle$ for $i \geq 0$.

**Example.** Let $v = \pi$, the ratio of the circumference of a circle to its diameter, known to be an irrational number.

| $i$ | $v_i$ | $q_i$ | $r_i$ | $r_i$ (approx.) |
|---|---|---|---|---|
| 0 | $\pi$ | 3 | 3 | 3.0000000000 |
| 1 | $(\pi - 3)^{-1} = \frac{1}{\pi - 3}$ | 7 | 22/7 | 3.1428571428 |
| 2 | $\left(\frac{1}{\pi-3} - 7\right)^{-1} = \frac{\pi-3}{-7\pi+22}$ | 15 | 333/106 | 3.1415094339 |
| 3 | $\left(\frac{\pi-3}{-7\pi+22} - 15\right)^{-1} = \frac{-7\pi+22}{106\pi-333}$ | 1 | 355/113 | 3.1415929203 |
| 4 | $\left(\frac{-7\pi+22}{106\pi-333} - 1\right)^{-1} = \frac{106\pi-333}{-113\pi+355}$ | 292 | 103993/33102 | 3.1415926530 |

The preceding table lists exact values of $v_i$ for $0 \leq i \leq 4$, along with the corresponding $q_i$ and $r_i$ terms produced by the continued fraction algorithm. We also include a decimal expansion of the convergent $r_i$, to ten decimal places. The procedure continues indefinitely with no discernible pattern to the values of $q_i$. However, the sequence of terms $r_i$ provides increasingly accurate rational approximations of $\pi = 3.1415926535\ldots$. (The reader might recognize two of the convergents, $r_1 = \frac{22}{7}$ and $r_3 = \frac{355}{113}$, as commonly used substitutes for $\pi$.) $\Diamond$

The continued fraction algorithm for $v$ does not terminate when $v$ is irrational. In some cases, however, we may be able to determine a pattern for the infinite sequence of $q_i$ terms, and thus for the convergents of $v$.

**Example.** Let $v = v_0$ equal the *golden ratio*, $\varphi = \frac{1+\sqrt{5}}{2} \approx 1.618$. Here $q_0 = 1$,

and we find that $v_0 - q_0 = \frac{-1+\sqrt{5}}{2}$. But then notice that

$$v_1 = \frac{1}{v_0 - q_0} = \frac{2}{-1+\sqrt{5}} = \frac{2}{-1+\sqrt{5}} \cdot \frac{1+\sqrt{5}}{1+\sqrt{5}} = \frac{1+\sqrt{5}}{2} = v_0.$$

It follows that $v_i = \varphi$ and $q_i = 1$ for all $i \geq 0$. The sequence of convergents of $\varphi$ is

$$1, \quad 1+\frac{1}{1}, \quad 1+\frac{1}{1+\frac{1}{1}}, \quad 1+\frac{1}{1+\frac{1}{1+\frac{1}{1}}}, \quad \ldots \quad = \quad 1, \quad 2, \quad \frac{3}{2}, \quad \frac{5}{3}, \quad \ldots.$$

Notice that

$$r_3 = 1 + \frac{1}{1+\frac{1}{1+\frac{1}{1}}} = 1 + \frac{1}{\left(1+\frac{1}{1+\frac{1}{1}}\right)} = 1 + \frac{1}{r_2} = \frac{r_2+1}{r_2},$$

and in general $r_{n+1} = \frac{r_n+1}{r_n}$ for $n \geq 0$, with $r_0 = 1$. If we define the *Fibonacci sequence*, $F_n$, for $n \geq 0$ by

$$F_0 = 0, \quad F_1 = 1, \quad \text{and} \quad F_n = F_{n-1} + F_{n-2} \quad \text{for } n \geq 2, \tag{9.1.2}$$

it follows by induction that $r_n = \frac{F_{n+2}}{F_{n+1}}$ for all $n \geq 0$. (See Exercise 9.1.1 below.) Numerical evidence suggests that this sequence converges to $\varphi$, a fact that we will verify in §12.1. Assuming that this sequence does in fact converge, we will write the limit of the sequence of convergents as $\langle 1, 1, 1, \ldots \rangle$. ♢

**Exercise 9.1.1.** Let $r_0 = 1$ and $r_{i+1} = \frac{r_i+1}{r_i}$ for $i \geq 0$. Show that if $F_n$ is defined as in equation (9.1.2), then $r_n = \frac{F_{n+2}}{F_{n+1}}$ for all $n \geq 0$.

The pattern exhibited here is due to the special nature of reciprocals of quadratic numbers. The next example illustrates this further.

**Example.** Let $v = v_0 = \sqrt{19}$, so that $q_0 = \left\lfloor \sqrt{19} \right\rfloor = 4$ and $v_1 = \frac{1}{-4+\sqrt{19}}$. Notice that

$$\frac{1}{-4+\sqrt{19}} \cdot \frac{4+\sqrt{19}}{4+\sqrt{19}} = \frac{4+\sqrt{19}}{-16+19} = \frac{4+\sqrt{19}}{3},$$

likewise a quadratic number. Continuing these calculations, we compile the terms of $v_i$, $q_i$, and $r_i$ sequences in the following table.

| $i$ | $v_i$ | $q_i$ | $r_i$ | $r_i$ (approx.) |
|---|---|---|---|---|
| 0 | $\sqrt{19}$ | 4 | 4 | 4.0000000000 |
| 1 | $\frac{1}{-4+\sqrt{19}} = \frac{4+\sqrt{19}}{3}$ | 2 | 9/2 | 4.5000000000 |
| 2 | $\frac{3}{-2+\sqrt{19}} = \frac{2+\sqrt{19}}{5}$ | 1 | 13/3 | 4.3333333333 |
| 3 | $\frac{5}{-3+\sqrt{19}} = \frac{3+\sqrt{19}}{2}$ | 3 | 48/11 | 4.3636363636 |
| 4 | $\frac{2}{-3+\sqrt{19}} = \frac{3+\sqrt{19}}{5}$ | 1 | 61/14 | 4.3571428571 |
| 5 | $\frac{5}{-2+\sqrt{19}} = \frac{2+\sqrt{19}}{3}$ | 2 | 170/39 | 4.3589743589 |
| 6 | $\frac{3}{-4+\sqrt{19}} = 4+\sqrt{19}$ | 8 | 1421/326 | 4.3588957055 |

Notice that $v_7 = (4+\sqrt{19}-8)^{-1}$ is the same as $v_1$. This means that the $q_i$ sequence repeats the terms $q_1$ through $q_6$ indefinitely. As $i$ increases, the $r_i$ sequence appears to more closely approximate $\sqrt{19} = 4.3588989435\ldots$. We may write $\sqrt{19} = \langle 4, 2, 1, 3, 1, 2, 8, 2, 1, 3, 1, 2, 8, \ldots\rangle$, assuming that this sequence does in fact converge to $\sqrt{19}$. ♢

**Exercise 9.1.2.** Use the continued fraction algorithm to find the sequence of convergents, up to $r_5$, of the given real number $v$.

(a) $v = \frac{249}{89}$.

(b) $v = \sqrt{2}$.

(c) $v = \sqrt{3}$.

(d) $v = \sqrt{7}$.

(e) $v = \frac{4+\sqrt{3}}{7}$.

We conclude this introductory section with an example approached from the opposite direction.

**Example.** Consider the expression $\langle 1, 2, 1, 3, 1, 3, \ldots\rangle = \left\langle 1, 2, \overline{1, 3}\right\rangle$, an abbreviation for the limit $v$ of the sequence

$$1,\quad 1+\frac{1}{2},\quad 1+\frac{1}{2+\frac{1}{1}},\quad 1+\frac{1}{2+\frac{1}{1+\frac{1}{3}}},\quad 1+\frac{1}{2+\frac{1}{1+\frac{1}{3+\frac{1}{1}}}},\quad 1+\frac{1}{2+\frac{1}{1+\frac{1}{3+\frac{1}{1+\frac{1}{3}}}}},$$

if that limit exists. (Here we place a line over a sequence of digits to indicate that this pattern continues indefinitely.) Can we calculate this value of $v$?

We can answer this question given certain assumptions about the behavior of infinite continued fraction expansions. We will verify that such steps are allowed in §9.4. First suppose that there is a real number $w$ equal to the limit of the sequence $\langle 1, 3, 1, 3, 1, 3, \ldots\rangle$. If we write

$$w = 1 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{3 + \frac{1}{\ddots}}}}}},$$

then we find by substitution that

$$w = 1 + \frac{1}{3 + \frac{1}{w}} = 1 + \frac{1}{\frac{3w+1}{w}} = 1 + \frac{w}{3w+1} = \frac{4w+1}{3w+1}.$$

So now $w$ satisfies the equation $3w^2 + w = 4w + 1$, that is, $3w^2 - 3w - 1 = 0$. This equation has two real number solutions: $\frac{3+\sqrt{21}}{6}$ and $\frac{3-\sqrt{21}}{6}$. But since we know that $\lfloor w \rfloor = 1$, the only possibility is $w = \frac{3+\sqrt{21}}{6}$. Now in a similar way,

$$v = 1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{3 + \frac{1}{\ddots}}}}}} = 1 + \frac{1}{2 + \frac{1}{w}},$$

so that

$$v = 1 + \frac{w}{2w+1} = \frac{3w+1}{2w+1} = \frac{15 + 3\sqrt{21}}{12 + 2\sqrt{21}} = \frac{9 + \sqrt{21}}{10},$$

multiplying the numerator and denominator by $12 - 2\sqrt{21}$ for the final equation. We can verify this conclusion by applying the continued fraction algorithm to $\frac{9+\sqrt{21}}{10}$. ♢

**Exercise 9.1.3.** Find a real number $v$ that has the given repeating $q_i$ sequence as its continued fraction.

(a) $\langle 1, 2, 1, 2, 1, 2, \ldots\rangle = \langle \overline{1, 2} \rangle$.

(b) $\langle 1, 2, 3, 1, 2, 3, 1, 2, 3, \ldots\rangle = \langle \overline{1, 2, 3} \rangle$.

(c) $\langle 3, 1, 2, 1, 2, 1, 2, \ldots\rangle = \langle 3, \overline{1, 2} \rangle$.

(d) $\langle 3, 2, 1, 1, 1, 1, \ldots\rangle = \langle 3, 2, \overline{1} \rangle$.

(e) $\langle 1, 2, 5, 2, 5, 2, 5, \ldots\rangle = \langle 1, \overline{2, 5} \rangle$.

(f) $\langle 1, 4, 1, 1, 1, 4, 1, 1, 1, 4, \ldots\rangle = \langle 1, 4, \overline{1, 1, 1, 4} \rangle$.

We summarize our observations from these examples as conjectures. It appears that when $v$ is a real number, we have a systematic process of constructing a sequence of rational numbers, namely a sequence of continued fractions

$$q_0, \qquad q_0 + \frac{1}{q_1}, \qquad q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2}}, \qquad q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3}}}, \qquad \ldots,$$

that converges to $v$. When $v$ is an irrational *quadratic* number, our examples suggest that the $q_i$ sequence that determines this sequence eventually follows some repeating pattern. Conversely, given a sequence of integers $q_0, q_1, q_2, \ldots$ that repeats a pattern, perhaps after some initial terms, our final example illustrates a method of computing a real number equal to the limit of that corresponding sequence of continued fractions. In §9.3, §9.4, and §9.5, we will verify that the outcomes illustrated by the examples in this section hold more generally.

## 9.2 Pell's Equation

In §9.1, we defined continued fractions as a method of approximating a given real number by a sequence of rational numbers. Before we develop this concept further, we will, in this section, illustrate an application of continued fractions to a general arithmetic problem, known as Pell's equation.

Equations of the form $x^2 - dy^2 = 1$, where $d$ is a positive integer, have a long history. An example from antiquity is the so-called *Cattle Problem of Archimedes*, a word problem involving types of cattle that can be algebraically manipulated into the equation $x^2 - dy^2 = 1$, where $d = 4729494$. It is not known whether Greek mathematicians knew a solution of this equation, but it is considered unlikely, in that the smallest nontrivial solution requires a $y$ value with more than forty digits. Indian mathematicians studied these equations throughout the Middle Ages, with Brahmagupta (c. 598–668) describing techniques for finding solutions using what we would now call quadratic integers, and Bhāskara (1114–1185) developing a recursive process for constructing general solutions.

The first general treatment of this problem in the West arose in a challenge issued to English mathematicians by Fermat in the seventeenth century. Fermat asked for a method of finding positive integer solutions of $x^2 - dy^2 = 1$ when $d$ is a positive integer, not a square. (Note that $x^2 - dy^2 = (x - ny)(x + ny) = 1$ has only trivial solutions when $d = n^2$.) Fermat's challenge implied that he knew that infinitely many solutions exist in every case, but as was his custom, he did not describe his methods of arriving at this conclusion. The first systematic solution to this problem, using continued fractions, was put forward by Lord Brouncker in 1657, a method described further by Wallis in his book *Algebra*. In the eighteenth century, Euler mistakenly credited John Pell with the Brouncker/Wallis method.

Although Pell apparently had no connection with this question, such was Euler's influence that $x^2 - dy^2 = 1$ has been called *Pell's equation* since then.

If $D$ is a quadratic domain in which $\sqrt{d}$ is an element, and $v = a + b\sqrt{d}$ in $D$, then

$$N(v) = v\overline{v} = \left(a + b\sqrt{d}\right)\left(a - b\sqrt{d}\right) = a^2 - db^2.$$

In general, if $N(v) = n$, it is convenient to refer to the real number $v$ as a solution of $x^2 - dy^2 = n$, that is, identify $v$ with the pair of integers $(a, b)$. In this case, we say that $v$ is *primitive* if $\gcd(a, b) = 1$. Notice that if $v$ is a solution of $x^2 - dy^2 = n$, then so are $-v$, $\overline{v}$, and $-\overline{v}$.

**Proposition 9.2.1.** *Let $d$ be a positive integer, not a square. If the equation $x^2 - dy^2 = 1$ has a solution other than $\pm 1$, then there is a smallest such solution $v > 1$, and in that case, $w$ is a solution of $x^2 - dy^2 = 1$ if and only if $w = \pm v^n$ for some integer $n$.*

If $v = a + b\sqrt{d}$ is the smallest solution of $x^2 - dy^2 = 1$ with $v > 1$, we refer to $(a, b)$, or to $v$ itself, as the *fundamental solution* of $x^2 - dy^2 = 1$.

*Proof.* Suppose that $v = a + b\sqrt{d}$ is a solution of $x^2 - dy^2 = 1$ with $v \neq \pm 1$. If $a$ and $b$ are positive, then $v$ is greater than 1 and, conversely, if $v > 1$, then the following argument shows that $a$ and $b$ must be positive. Since $N(v) = v \cdot \overline{v} = 1$, then $\overline{v} = a - b\sqrt{d} = \frac{1}{v}$. If $v > 1$, then $0 < \frac{1}{v} < 1$, so it follows that $a + b\sqrt{d} > a - b\sqrt{d}$, which implies that $b$ is positive. Likewise, $-1 < -\frac{1}{v} < 0$, so that $a + b\sqrt{d} > -a + b\sqrt{d}$, which implies that $a$ is positive. Now there are finitely many positive integers $s < v$ and finitely many positive integers $t$ with $t\sqrt{d} < v$, so there can be only finitely many solutions $w = s + t\sqrt{d}$ of $x^2 - dy^2$ such that $1 < w < v$. So if $v \neq \pm 1$ exists, there must be a smallest solution of $x^2 - dy^2 = 1$ greater than 1. We will assume that $v$ itself is that solution.

If $w = \pm v^n$ for some integer $n$, then $N(w) = N(\pm v^n) = N(\pm 1) \cdot N(v)^n = 1$, so that $w$ is also a solution of $x^2 - dy^2 = 1$. Conversely, suppose that $w$ is a solution of $x^2 - dy^2 = 1$. If $w = \pm 1$, then $w = \pm v^0$. Otherwise, we may assume that $w > 1$ (replacing $w$ by $\overline{w}$, $-w$, or $-\overline{w}$ if not). Since $v > 1$, the positive powers of $v$ get arbitrarily large, so there is a positive integer $n$ such that $v^n \leq w < v^{n+1}$. But then $1 \leq w \cdot v^{-n} < v$. Note that $N(w \cdot v^{-n}) = N(w) \cdot N(v)^{-n} = 1$, so that $w \cdot v^{-n}$ is a solution of $x^2 - dy^2 = 1$. That solution must equal 1 to avoid contradicting the definition of $v$. So $w = v^n$. □

If $x^2 - dy^2 = 1$ has a solution in positive integers, $(x, y) = (a, b)$, then $\left(\frac{a}{b}\right)^2 - \frac{1}{b^2} = d$. Thus the larger $b$ is, the closer the rational number $\frac{a}{b}$ is to $\sqrt{d}$, as the following example illustrates.

Table 9.1. Solutions of $x^2 - 3y^2 = 1$

| $i$ | $v^i$ | $a/b$ | $i$ | $v^i$ | $a/b$ |
|---|---|---|---|---|---|
| 1 | $2 + \sqrt{3}$ | 2.0000000000 | 6 | $1351 + 780\sqrt{3}$ | 1.7320512820 |
| 2 | $7 + 4\sqrt{3}$ | 1.7500000000 | 7 | $5042 + 2911\sqrt{3}$ | 1.7320508416 |
| 3 | $26 + 15\sqrt{3}$ | 1.7333333333 | 8 | $18817 + 10864\sqrt{3}$ | 1.7320508100 |
| 4 | $97 + 56\sqrt{3}$ | 1.7321428571 | 9 | $70226 + 40545\sqrt{3}$ | 1.7320508077 |
| 5 | $362 + 209\sqrt{3}$ | 1.7320574162 | 10 | $262087 + 151316\sqrt{3}$ | 1.7320508075 |

**Example.** If $d = 3$, then $v = 2 + \sqrt{3}$ is a solution of $x^2 - 3y^2 = 1$. No smaller solution $a + b\sqrt{3}$ exists with $a$ and $b$ both positive, and so $v$ is the fundamental solution. Table 9.1 lists other solutions $v^i = a + b\sqrt{d}$ with $i \leq 10$. All positive integer solutions of $x^2 - 3y^2 = 1$ would appear in this list if it were extended indefinitely. For each solution $a + b\sqrt{d}$ in this list, we calculate the decimal expansion of $a/b$. (The tenth approximation is identical to $\sqrt{3}$ to ten decimal places.) ◊

If $d' = m^2 d$, then every solution $a + b\sqrt{d'}$ of $x^2 - d'y^2 = 1$ yields a corresponding solution $a + mb\sqrt{d}$ of $x^2 - dy^2 = 1$. Conversely, if $a + b\sqrt{d}$ is a solution of $x^2 - dy^2 = 1$ with $b$ divisible by $m$, then $a + \frac{b}{m}\sqrt{d'}$ is a solution of $x^2 - d'y^2 = 1$. Thus we see, from the example above, that $7 + 2\sqrt{12}$ is the fundamental solution of $x^2 - 12y^2 = 1$, that $26 + 5\sqrt{27}$ is the fundamental solution of $x^2 - 27y^2 = 1$, and so forth. We will consider connections between the fundamental solutions of $x^2 - dy^2 = 1$ and $x^2 - (m^2 d)y^2 = 1$ further in §13.2.

**Calculating the Fundamental Solution.** In §9.1, we saw that the continued fraction of an irrational real number $v$ can be viewed as a sequence of rational approximations of $v$. Since a solution of Pell's equation $x^2 - dy^2 = 1$ is a rational approximation of $\sqrt{d}$, it is not surprising that such a solution might arise from the continued fraction algorithm applied to $\sqrt{d}$. In the following theorem, we introduce a revised algorithm for constructing this continued fraction, which also produces the fundamental solution of $x^2 - dy^2 = 1$.

**Theorem 9.2.2** (Pell's Equation Algorithm)**.** *Let $d$ be a positive integer, not a square. Let $a_0 = 1$ and $k_0 = 0$. For all $i \geq 0$, select $k_{i+1}$ to be congruent to $-k_i$ modulo $a_i$, with $k_{i+1} > -\sqrt{d}$ as small as possible. Then let*

$$a_{i+1} = \frac{d - k_{i+1}^2}{a_i}. \tag{9.2.1}$$

*In this case, $a_i$ is an integer satisfying $0 < a_i < 2\sqrt{d}$, and $a_i$ divides $d - k_i^2$ for all $i \geq 0$. There is a smallest integer $\ell > 0$ so that $a_\ell = 1$.*

*Now define $q_i$ for $i \geq 0$ to be*

$$q_i = -\frac{k_i + k_{i+1}}{a_i}, \tag{9.2.2}$$

*and define $m_i$ and $n_i$ for $i \geq -2$ as follows:*

$$m_{-2} = 0, \quad m_{-1} = 1, \quad \text{and} \quad m_i = q_i m_{i-1} + m_{i-2} \quad \text{for } i \geq 0,$$
$$n_{-2} = 1, \quad n_{-1} = 0, \quad \text{and} \quad n_i = q_i n_{i-1} + n_{i-2} \quad \text{for } i \geq 0.$$

*Then $m_{i-1}^2 - d n_{i-1}^2 = (-1)^i a_i$ for all $i \geq 0$. Let $v = m_{\ell-1} + n_{\ell-1}\sqrt{d}$. If $\ell$ is even, then $v$ is the fundamental solution of $x^2 - dy^2 = 1$. If $\ell$ is odd, then $v^2$, which also equals $m_{2\ell-1} + n_{2\ell-1}\sqrt{d}$, is the fundamental solution of $x^2 - dy^2 = 1$.*

This algorithm is a slight variation on the quadratic continued fraction algorithm, which we will state and prove as Theorem 10.3.1. The implications of this continued fraction calculation to Pell's equation require certain results from Theorem 11.1.1. We omit the proof of Theorem 9.2.2 in this section, instead illustrating this procedure with examples.

**Example.** Let $d = 22$. In applying the algorithm of Theorem 9.2.2, it is helpful to calculate $d - x^2$ for $-\sqrt{d} < x < \sqrt{d}$, as in the following table.

| $x$ | $\pm 4$ | $\pm 3$ | $\pm 2$ | $\pm 1$ | $0$ |
|---|---|---|---|---|---|
| $22 - x^2$ | 6 | 13 | 18 | 21 | 22 |

Let $a_0 = 1$ and $k_0 = 0$. We want $k_1$ to be congruent to $-k_0 = 0$ modulo $a_0 = 1$, and as small as possible with $k_1 > -\sqrt{d}$. Hence $k_1 = -4$ and then $a_1 = \frac{d-k_1^2}{a_0} = \frac{22-(-4)^2}{1} = 6$. Now $k_2$ must satisfy $k_2 \equiv -k_1 \equiv 4 \pmod 6$. Thus $k_2 = -2$ is the smallest possibility with $k_2 > -\sqrt{d}$, and then $a_2 = \frac{d-k_2^2}{a_1} = \frac{22-(-2)^2}{6} = 3$. We continue these calculations in the following table, eventually finding that $a_6 = 1$, so that $\ell = 6$. Notice also that since $a_7 = a_1$ and $k_7 = k_1$, the sequences of $a_i$ and $k_i$ values then repeat the pattern of $1 \leq i \leq 6$ indefinitely.

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| $a$ | 1 | 6 | 3 | 2 | 3 | 6 | 1 | 6 |
| $k$ | 0 | $-4$ | $-2$ | $-4$ | $-4$ | $-2$ | $-4$ | $-4$ |
| $q$ | 4 | 1 | 2 | 4 | 2 | 1 | 8 | |
| $m$ | 4 | 5 | 14 | 61 | 136 | 197 | | |
| $n$ | 1 | 1 | 3 | 13 | 29 | 42 | | |

Simultaneously with these calculations, or after we have found $a_\ell = 1$, we can see that $q_0 = -\frac{k_0+k_1}{a_0} = -\frac{0-4}{1} = 4$, then $q_1 = -\frac{-4-2}{6} = 1$, and so forth. With

the repetition of the $a_i$ and $k_i$ sequences, we see that $q_i = q_{i+6}$ for $i \geq 1$. Finally, we calculate the $m_i$ and $n_i$ sequences in the table above, beginning with $m_0 = q_0 m_{-1} + m_{i-2} = q_0 \cdot 1 + 0 = 4$ and $n_0 = q_0 n_{-1} + n_{i-2} = q_0 \cdot 0 + 1 = 1$. We can verify that $m_{i-1}^2 - d n_{i-1}^2 = (-1)^i a_i$ for the values of $i$ listed above. With $\ell$ even, Theorem 9.2.2 implies that the fundamental solution of $x^2 - 22y^2 = 1$ is given by $(x, y) = (m_5, n_5) = (197, 42)$.

Using results from §9.3 and §9.4, we will see that the sequence of $q_i$ values produced by this algorithm shows that

$$\sqrt{22} = 4 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{4 + \ddots}}}. \tag{9.2.3}$$

For now, we will simply note that partial continued fractions from this expression,

$$4, \qquad 4 + \frac{1}{1} = 5, \qquad 4 + \cfrac{1}{1 + \frac{1}{2}} = \frac{14}{3}, \qquad 4 + \cfrac{1}{1 + \cfrac{1}{2 + \frac{1}{4}}} = \frac{61}{13},$$

are given by $\frac{m_i}{n_i}$ for $i \geq 0$, and that these quotients provide progressively more accurate rational approximations of $\sqrt{22}$ as $i$ increases. ♢

**Example.** For $d = 29$, the values of $d - x^2$ for $-\sqrt{d} < x < \sqrt{d}$ are as follows.

| $x$ | $\pm 5$ | $\pm 4$ | $\pm 3$ | $\pm 2$ | $\pm 1$ | $0$ |
|---|---|---|---|---|---|---|
| $29 - x^2$ | 4 | 13 | 20 | 25 | 28 | 29 |

The following table compiles the data of Theorem 9.2.2 for this example.

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| $a$ | 1 | 4 | 5 | 5 | 4 | 1 | 4 |
| $k$ | 0 | $-5$ | $-3$ | $-2$ | $-3$ | $-5$ | $-5$ |
| $q$ | 5 | 2 | 1 | 1 | 2 | 10 | |
| $m$ | 5 | 11 | 16 | 27 | 70 | | |
| $n$ | 1 | 2 | 3 | 5 | 13 | | |

For instance $k_1 = -5$ satisfies $k_1 \equiv -k_0 \pmod{a_0}$ with $k_1 > -\sqrt{d}$ as small as possible, and then $a_1 = \frac{29-(-5)^2}{1} = 4$. Now $k_2 = -3$ is the minimal value satisfying $k_2 \equiv 5 \pmod 4$, and so $a_2 = \frac{29-(-3)^2}{4} = 5$. Additionally, we calculate that $q_0 = -\frac{k_0+k_1}{a_0} = -\frac{0-5}{1} = 5$, and then $q_1 = -\frac{-5-3}{4} = 2$, and so forth.

Here we find that $a_5 = 1$ so that $\ell = 5$. The pair $(x, y) = (m_4, n_4) = (70, 13)$ satisfies the equation $x^2 - 29y^2 = -1$, but the fundamental solution of $x^2 - 29y^2 = 1$ is given by $(m_9, n_9)$ since $\operatorname{lcm}(\ell, 2) = 10$. We could continue the table further, or note more simply that since $\upsilon = 70 + 13\sqrt{29}$ satisfies $N(\upsilon) = -1$, then $N(\upsilon^2) =$

$(-1)^2 = 1$. We calculate that $(70 + 13\sqrt{29})^2 = 9801 + 1820\sqrt{29}$. So $(x, y) = (9801, 1820)$ is a solution of $x^2 - 29y^2 = 1$, and we will see by Theorem 11.1.1 that it must be the fundamental solution. ♢

**Exercise 9.2.1.** For each $d$, use the algorithm of Theorem 9.2.2 to find the fundamental solution of $x^2 - dy^2 = 1$.

(a) $d = 11$.

(b) $d = 13$.

(c) $d = 14$.

(d) $d = 20$.

(e) $d = 23$.

(f) $d = 31$.

(g) $d = 33$.

(h) $d = 41$.

(i) $d = 46$.

(j) $d = 53$.

**Exercise 9.2.2.** Use the algorithm of Theorem 9.2.2 to show that the given pair $(x, y)$ is the fundamental solution of $x^2 - dy^2 = 1$ in the following special cases for $d$.

(a) $(x, y) = (2t^2 + 1, 2t)$, when $d = t^2 + 1$ for some integer $t > 0$.

(b) $(x, y) = (t, 1)$, when $d = t^2 - 1$ for some integer $t > 1$.

(c) $(x, y) = (t^2 + 1, t)$, when $d = t^2 + 2$ for some integer $t > 0$.

(d) $(x, y) = (2t + 1, 2)$, when $d = t^2 + t$ for some integer $t > 0$.

As an application of these results, we conclude this section with a classification of automorphs of $f(x, y) = x^2 - dy^2$.

**Theorem 9.2.3.** *Let $d$ be a positive integer, which is not a square, and let $f(x, y) = x^2 - dy^2$. If $(q, r)$ is a solution of $x^2 - dy^2 = 1$, then $U = \begin{bmatrix} q & dr \\ r & q \end{bmatrix}$ is an automorph of $f$. If $(q, r)$ is the fundamental solution of $x^2 - dy^2 = 1$, then the group of autormorphs of $f$ consists precisely of $\pm U^n$ for every integer $n$.*

*Proof.* Proposition 4.3.4 shows that $U = \begin{bmatrix} q & dr \\ r & q \end{bmatrix}$ is an automorph of $f(x,y) = x^2 - dy^2$ if and only if $f(q,r) = 1$. If $(q,r)$ is the fundamental solution of $x^2 - dy^2 = 1$, and we let $v = q + r\sqrt{d}$, then all solutions are given by $\pm v^n$ with $n$ an integer. One can show, by induction for positive $n$, and using the definition of the inverse of a matrix for negative $n$, that if $v^n$ is written as $q_n + r_n\sqrt{d}$, then $U^n = \begin{bmatrix} q_n & dr_n \\ r_n & q_n \end{bmatrix}$. We leave this verification as the following exercise. □

**Exercise 9.2.3.** Let $(q,r)$ be the fundamental solution of $x^2 - dy^2 = 1$ for some positive $d$, not a square. Let $v = q + r\sqrt{d}$ and for all integers $n$, write $v^n$ as $q_n + r_n\sqrt{d}$. Show that if $U = \begin{bmatrix} q & dr \\ r & q \end{bmatrix}$, then $U^n = \begin{bmatrix} q_n & dr_n \\ r_n & q_n \end{bmatrix}$ for every integer $n$.

**Example.** If $d = 43$, we calculate $d - x^2$ for $-\sqrt{d} < x < \sqrt{d}$ as follows.

| $x$ | $\pm 6$ | $\pm 5$ | $\pm 4$ | $\pm 3$ | $\pm 2$ | $\pm 1$ | $0$ |
|---|---|---|---|---|---|---|---|
| $43 - x^2$ | 7 | 18 | 27 | 34 | 39 | 42 | 43 |

We obtain the following calculations using Theorem 9.2.2.

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $a$ | 1 | 7 | 6 | 3 | 9 | 2 | 9 | 3 | 6 | 7 | 1 | 7 |
| $k$ | 0 | $-6$ | $-1$ | $-5$ | $-4$ | $-5$ | $-5$ | $-4$ | $-5$ | $-1$ | $-6$ | $-6$ |
| $q$ | 6 | 1 | 1 | 3 | 1 | 5 | 1 | 3 | 1 | 1 | 12 | |
| $m$ | 6 | 7 | 13 | 46 | 59 | 341 | 400 | 1541 | 1941 | 3482 | | |
| $n$ | 1 | 1 | 2 | 7 | 9 | 52 | 61 | 235 | 296 | 531 | | |

Since $\ell = 10$ is even, $(3482, 531)$ is the fundamental solution of $x^2 - 43y^2 = 1$. The matrix $U = \begin{bmatrix} 3482 & 22833 \\ 531 & 3482 \end{bmatrix}$ is an automorph of $x^2 - 43y^2$, and the group of all automorphs consists of $\pm U^n$, where $n$ is an integer. ◊

## 9.3 Convergence of Continued Fractions

We now formally define infinite simple continued fractions, and will show that each such object can be viewed as a convergent sequence of rational numbers.

**Definition.** Let $q_0, q_1, \ldots, q_i, w$ be a finite sequence satisfying the following conditions: the first term, $q_0$, is an integer; if there is more than one term, the last term, $w$, is a real number with $w \geq 1$; if there are more than two terms, the intermediate terms, $q_1, q_2, \ldots, q_i$, are positive integers. Then the *finite continued fraction* $\langle q_0, q_1, \ldots, q_i, w \rangle$ is a real number defined recursively as follows.

(1) $\langle q_0 \rangle = q_0$.

(2) $\langle q_0, w \rangle = q_0 + \frac{1}{w}$.

(3) If $i > 0$, then $\langle q_0, q_1, \dots, q_{i-1}, q_i, w \rangle = \left\langle q_0, q_1, \dots, q_{i-1}, q_i + \frac{1}{w} \right\rangle$.

We call $\langle q_0, q_1, \dots, q_i, w \rangle$ a finite *simple* continued fraction if $w$ is an integer. If $q_0, q_1, q_2, \dots$ is an infinite sequence of integers with $q_i > 0$ for $i > 0$, then we define the *infinite simple continued fraction* $\langle q_0, q_1, q_2, \dots \rangle$ to be the limit of the sequence

$$\langle q_0 \rangle, \langle q_0, q_1 \rangle, \langle q_0, q_1, q_2 \rangle, \dots,$$

if that sequence of real numbers converges.

In many texts, a continued fraction is written as $\langle q_0; q_1, q_2, \dots \rangle$ (or with a different type of brackets), with a semicolon separating the $q_0$ from the other terms to indicate the weaker requirement for $q_0$. Our main interest will be in *simple* continued fractions, but by allowing the last term of a finite continued fraction to be real, we can calculate finite continued fractions recursively, as the following example illustrates. When $w$ is rational, we can see inductively that $\langle q_0, q_1, \dots, q_{i-1}, q_i, w \rangle$ is a rational number. In particular, a finite simple continued fraction is always a rational number.

**Example.** We find recursively that

$$\langle 5, 7, 1, 3 \rangle = \left\langle 5, 7, 1 + \frac{1}{3} \right\rangle = \left\langle 5, 7, \frac{4}{3} \right\rangle$$
$$= \left\langle 5, 7 + \frac{3}{4} \right\rangle = \left\langle 5, \frac{31}{4} \right\rangle = 5 + \frac{4}{31} = \frac{159}{31}.$$

Note that $\langle 5, 7, 1, 3 \rangle$ is shorthand for the expression

$$5 + \frac{1}{7 + \frac{1}{1 + \frac{1}{3}}},$$

as we saw in §9.1. ◊

**Example.** The infinite continued fraction $\langle 1, 2, 1, 2, 1, 2, \dots \rangle$ is defined to be the limit of the sequence

$$\langle 1 \rangle, \langle 1, 2 \rangle, \langle 1, 2, 1 \rangle, \langle 1, 2, 1, 2 \rangle, \langle 1, 2, 1, 2, 1 \rangle, \langle 1, 2, 1, 2, 1, 2 \rangle, \dots$$
$$= 1, \frac{3}{2}, \frac{4}{3}, \frac{11}{8}, \frac{15}{11}, \frac{41}{30}, \dots,$$

where each of the finite simple continued fractions is calculated by the recursive process illustrated in the previous example. ◊

**Exercise 9.3.1.** Calculate the following finite simple continued fractions.

(a) $\langle -3, 1, 5, 3\rangle$.

(b) $\langle 0, 2, 2, 2, 4\rangle$.

(c) $\langle 2, 1, 3, 1, 4, 3\rangle$.

In this section, we will show that every infinite simple continued fraction converges to a real number. We begin with the following definition, which we previously saw in the algorithm for Pell's equation.

**Definition.** Let $\langle q_0, q_1, q_2, \dots\rangle$ be an infinite simple continued fraction. Then we define two sequences $m_i$ and $n_i$ of integers, and a sequence of rational numbers $r_i$ as follows. Let $m_{-2} = 0$, $m_{-1} = 1$, $n_{-2} = 1$, and $n_{-1} = 0$. Then for $i \geq 0$, let

$$m_i = m_{i-1} \cdot q_i + m_{i-2}, \quad n_i = n_{i-1} \cdot q_i + n_{i-2}, \quad \text{and} \quad r_i = \frac{m_i}{n_i}. \tag{9.3.1}$$

We call $r_i$ the *$i$-th convergent* of the continued fraction $\langle q_0, q_1, q_2, \dots\rangle$, and call $m_i$ and $n_i$ the *numerator* and *denominator*, respectively, of the $i$-th convergent.

The following lemma ensures that $r_i$ is in fact a rational number for all $i \geq 0$, since $n_i$ cannot equal zero.

**Lemma 9.3.1.** *Let $\langle q_0, q_1, q_2, \dots\rangle$ be an infinite simple continued fraction, with $n_i$ the denominator of its $i$-th convergent. Then $n_i > n_{i-1}$ if $i > 1$, and $n_i \geq i$ for all $i \geq 0$.*

*Proof.* Note that $n_0 = n_{-1} \cdot q_0 + n_{-2} = 1$ and $n_1 = n_0 \cdot q_1 + n_{-1} = q_1 \geq 1$. If $i$ is greater than 1, so that $q_i \geq 1$, and we assume that $n_{i-1}$ and $n_{i-2}$ are both positive, then

$$n_i = n_{i-1} \cdot q_i + n_{i-2} \geq n_{i-1} + n_{i-2} > n_{i-1}.$$

The fact that $n_i$ is strictly larger than $n_{i-1}$ shows that if $n_{i-1} \geq i - 1$, then $n_i \geq i$. Both claims of this lemma then follow by induction. □

**Exercise 9.3.2.** Find the numerator and denominator terms of the sequence of convergents of the following continued fractions, up to the fifth term, $r_5$.

(a) $\langle 2, 1, 2, 1, 2, 1, \dots\rangle$.

(b) $\langle 3, 3, 3, 3, 3, 3, \dots\rangle$.

(c) $\langle 1, 2, 3, 1, 2, 3, \dots\rangle$.

**Lemma 9.3.2.** *Let $\langle q_0, q_1, q_2, \dots\rangle$ be a continued fraction. Let $m_i$ and $n_i$ be defined as in* (9.3.1)*. Then for every integer $i \geq 0$ and real number $w \geq 1$,*

$$\langle q_0, q_1, \dots, q_i, w\rangle = \frac{m_i \cdot w + m_{i-1}}{n_i \cdot w + n_{i-1}}. \tag{9.3.2}$$

*Proof.* We use induction on $i$. If $i = 0$, then by the definition of continued fractions and of the numerator and denominator sequences,

$$\langle q_0, w\rangle = q_0 + \frac{1}{w} = \frac{q_0 w + 1}{w} = \frac{m_0 \cdot w + m_{-1}}{n_0 \cdot w + n_{-1}}$$

for any real number $w \geq 1$.

Now suppose that we have established (9.3.2) for a specific $k \geq 0$ in place of $i$, and for all real numbers $w \geq 1$. Then by definition, $\langle q_0, \dots, q_k, q_{k+1}, w\rangle = \langle q_0, \dots, q_k, z\rangle$, where $z = q_{k+1} + \frac{1}{w}$ is a real number greater than or equal to 1. But now by the inductive hypothesis,

$$\begin{aligned}\langle q_0, \dots, q_k, q_{k+1}, w\rangle = \langle q_0, \dots, q_k, z\rangle &= \frac{m_k \cdot z + m_{k-1}}{n_k \cdot z + n_{k-1}} \\ &= \frac{(m_k \cdot q_{k+1} + m_{k-1}) + m_k \cdot \frac{1}{w}}{(n_k \cdot q_{k+1} + n_{k-1}) + n_k \cdot \frac{1}{w}} = \frac{m_{k+1} \cdot w + m_k}{n_{k+1} \cdot w + n_k},\end{aligned}$$

the last step using (9.3.1) and multiplying the numerator and denominator by $w$. But this is (9.3.2) with $k + 1$ in place of $i$, which shows by induction that (9.3.2) holds for all $i \geq 0$. □

**Exercise 9.3.3.** Express each of the following continued fractions as a rational expression in terms of $w$.

(a) $\langle 1, 2, w\rangle$.

(b) $\langle 2, 3, 5, w\rangle$.

(c) $\langle 2, 1, 3, 1, w\rangle$.

**Corollary 9.3.3.** *Let $q_0, q_1, \dots$ be a sequence of integers, with $q_i > 0$ if $i > 0$. Then $\langle q_0, q_1, \dots, q_i\rangle = r_i$, where $r_i$ is the $i$-th convergent defined as in* (9.3.1).

*Proof.* If $i = 0$, then $\langle q_0\rangle = q_0 = \frac{m_0}{n_0} = r_0$. If $i > 0$, then

$$\langle q_0, q_1, \dots, q_{i-1}, q_i\rangle = \frac{m_{i-1} \cdot q_i + m_{i-2}}{n_{i-1} \cdot q_i + n_{i-2}} = \frac{m_i}{n_i} = r_i,$$

using (9.3.2) and (9.3.1). □

Therefore $\langle q_0, q_1, q_2, \dots\rangle = \lim_{i\to\infty} r_i$, using the definition of infinite continued fractions and the notation of (9.3.1). It remains to show that this limit always exists.

**Lemma 9.3.4.** *Let $\langle q_0, q_1, q_2, \dots\rangle$ be a continued fraction, and let $m_i$ and $n_i$ be defined as in* (9.3.1). *Then $m_i n_{i+1} - m_{i+1} n_i = (-1)^{i+1}$ for all $i \geq 0$. Thus for all $i \geq 0$,*

$$\gcd(m_i, n_i) = \gcd(m_i, m_{i+1}) = \gcd(n_i, n_{i+1}) = 1.$$

*Proof.* When $i = 0$, then $m_0n_1 - m_1n_0 = q_0 \cdot q_1 - (q_0q_1 + 1) \cdot 1 = -1 = (-1)^{0+1}$. Now suppose that $m_kn_{k+1} - m_{k+1}n_k = (-1)^{k+1}$ for some $k \geq 0$. Then by (9.3.1), we have

$$\begin{aligned} m_{k+1}n_{k+2} - m_{k+2}n_{k+1} &= m_{k+1}(n_{k+1}q_{k+2} + n_k) - (m_{k+1}q_{k+2} + m_k)n_{k+1} \\ &= m_{k+1}n_{k+1}q_{k+2} + m_{k+1}n_k - m_{k+1}n_{k+1}q_{k+2} - m_kn_{k+1} \\ &= m_{k+1}n_k - m_kn_{k+1} = -(-1)^{k+1} = (-1)^{k+2}, \end{aligned}$$

using the inductive hypothesis. The first claim follows by induction. But now note that when $i \geq 0$, then 1 can be expressed as a combination of $m_i$ and $n_i$, likewise as a combination of $m_i$ and $m_{i-1}$, and as a combination of $n_i$ and $n_{i-1}$. It follows immediately that these pairs of integers cannot have any common divisors other than 1. □

**Lemma 9.3.5.** *Suppose that $\frac{a}{b} < \frac{c}{d}$, where a, b, c, and d are integers with b and d positive. Then*

$$\frac{a}{b} < \frac{aq + cr}{bq + dr} < \frac{c}{d}$$

*for every pair of positive integers q and r.*

*Proof.* Multiplying the inequality $\frac{a}{b} < \frac{c}{d}$ by the positive integer $bd$, we have that $ad < bc$. Since $r$ is positive, it follows that $adr < bcr$, so that $adr + abq < bcr + abq$, or $a(bq + dr) < b(aq + cr)$. Now dividing both sides by the positive integer $b(bq + dr)$, we see that $\frac{a}{b} < \frac{aq+cr}{bq+dr}$. Likewise $ad < bc$ implies that $d(aq + cr) < c(bq + dr)$, so that $\frac{aq+cr}{bq+dr} < \frac{c}{d}$. □

**Example.** Let $q = 11$ and $r = 17$. Since $\frac{3}{4} < \frac{4}{5}$, we know that $\frac{3}{4} < \frac{3(11)+4(17)}{4(11)+5(17)} < \frac{4}{5}$, that is, $\frac{3}{4} < \frac{101}{129} < \frac{4}{5}$. ◊

**Lemma 9.3.6.** *Let $r_i$ be the i-th convergent of $\langle q_0, q_1, q_2, \ldots \rangle$. Then the following inequalities are true:*

$$r_0 < r_2 < r_4 < \cdots < r_{2i} < \cdots < r_{2i+1} < \cdots < r_5 < r_3 < r_1.$$

*In other words, the sequence of even-indexed convergents is strictly increasing, the sequence of odd-indexed convergents is strictly decreasing, but every even-indexed convergent is strictly smaller than every odd-indexed convergent.*

*Proof.* We know that $r_0 = \frac{m_0}{n_0} = q_0$, while $r_1 = \frac{m_1}{n_1} = \frac{q_0q_1+1}{q_1} = q_0 + \frac{1}{q_1}$. Since $q_1$ is positive, then $r_0 < r_1$. Now since $q_i$ is a positive integer for every $n > 0$, Lemma 9.3.5 implies that

$$r_i = \frac{m_i}{n_i} = \frac{m_{i-1} \cdot q_i + m_{i-2} \cdot 1}{n_{i-1} \cdot q_i + n_{i-2} \cdot 1}$$

is strictly between $r_{i-1} = \frac{m_{i-1}}{n_{i-1}}$ and $r_{i-2} = \frac{m_{i-2}}{n_{i-2}}$ for all $i \geq 2$. So $r_2$ satisfies $r_0 < r_2 < r_1$, and then $r_2 < r_3 < r_1$. The result follows by continuing this process inductively. □

Now we can prove our main result of this section.

**Theorem 9.3.7.** *If $\langle q_0, q_1, q_2, \dots \rangle$ is an infinite simple continued fraction, then its sequence of convergents, $r_i$, is a Cauchy sequence. Thus*

$$\langle q_0, q_1, q_2, \dots \rangle = \lim_{i \to \infty} r_i$$

*is a real number, $v$, satisfying $q_0 < v < q_0 + 1$.*

*Proof.* We want to show that for every real number $\epsilon > 0$, there is a positive integer $N$ such that $|r_i - r_j| < \epsilon$ whenever $i$ and $j$ are greater than $N$. So suppose that $\epsilon > 0$ is given. Let $N$ be a positive integer for which $N^2 > \frac{1}{\epsilon}$.

If $m_i$ and $n_i$ are the numerator and denominator of the $i$-th convergent $r_i$, we know that

$$m_N n_{N+1} - m_{N+1} n_N = (-1)^{N+1} \tag{9.3.3}$$

by Lemma 9.3.4. Lemma 9.3.1 shows that $n_i$ is a strictly increasing sequence for $i \geq 1$, with $n_i \geq i$. Dividing both sides of equation (9.3.3) by the positive integer $n_N n_{N+1}$, we find that

$$|r_N - r_{N+1}| = \frac{1}{n_N n_{N+1}} < \frac{1}{n_N^2} \leq \frac{1}{N^2} < \epsilon.$$

But now if $i$ and $j$ exceed $N$, Lemma 9.3.6 shows that $|r_i - r_j| \leq |r_N - r_{N+1}| < \epsilon$. So $r_i$ is a Cauchy sequence, and must converge to some real number $v$, which equals $\langle q_0, q_1, q_2, \dots \rangle$ by Corollary 9.3.3. For the final statement, note that

$$q_0 = r_0 < v < r_1 = q_0 + \frac{1}{q_1} \leq q_0 + 1$$

by Lemma 9.3.6. □

**Exercise 9.3.4.** In each part, calculate the two continued fractions and indicate which one is larger (in the usual order on real numbers).

(a) $v = \langle 1, 2 \rangle$ or $w = \langle 1, 3 \rangle$.

(b) $v = \langle 1, 2, 3 \rangle$ or $w = \langle 1, 2, 4 \rangle$.

(c) $v = \langle 1, 2 \rangle$ or $w = \langle 1, 2, 3 \rangle$.

(d) $v = \langle 1, 1, 1, 1, 1, 2 \rangle$ or $w = \langle 1, 1, 1, 1, 1, 1, 2 \rangle$.

**Exercise 9.3.5.** Let $q_0, q_1, q_2, \dots, q_i$ be integers with $q_i > 0$ if $i > 0$. Let $x$ and $y$ be real numbers with $x > y \geq 1$. Let $v = \langle q_0, q_1, q_2, \dots, q_i \rangle$, $w = \langle q_0, q_1, q_2, \dots, q_i, x \rangle$, and $z = \langle q_0, q_1, q_2, \dots, q_i, y \rangle$. Show that $v < w < z$ if $i$ is even and $v > w > z$ if $i$ is odd.

## 9.4 Continued Fraction Expansions of Real Numbers

In §9.1, we outlined a method, called the *continued fraction algorithm*, of associating a particular sequence of rational numbers to a given real number $v$. Numerical evidence suggested that this sequence converges to $v$. We now verify that this is always the case. That is, we show that every real number $v$ can be expressed in some way as a simple continued fraction. We will find that this expression is unique, and infinite, if $v$ is irrational. On the other hand, if $v$ is rational, there are always two distinct finite continued fraction expressions for $v$.

**Lemma 9.4.1.** *Let $v = v_0$ be a real number, and for $i \geq 0$, let $q_i = \lfloor v_i \rfloor$ and let $v_{i+1} = \frac{1}{v_i - q_i}$ if $q_i \neq v_i$, as in the continued fraction algorithm. Then*

$$\langle q_0, q_1, q_2, \dots, q_{i-1}, v_i \rangle = v$$

*for all $i \geq 1$ for which $v_i$ is defined.*

*Proof.* If $i = 1$, then $\langle q_0, v_1 \rangle = q_0 + \frac{1}{v_1} = q_0 + (v_0 - q_0) = v_0 = v$. Now suppose that $\langle q_0, q_1, q_2, \dots, q_{k-1}, v_k \rangle = v$ for some $k \geq 1$, and that $v_{k+1}$ exists. Then

$$\begin{aligned}\langle q_0, q_1, q_2, \dots, q_k, v_{k+1} \rangle &= \left\langle q_0, q_1, q_2, \dots, q_{k-1}, q_k + \frac{1}{v_{k+1}} \right\rangle \\ &= \langle q_0, q_1, q_2, \dots, q_{k-1}, v_k \rangle = v,\end{aligned}$$

by definition and the inductive hypothesis, as we wanted to show. □

**Theorem 9.4.2.** *Let $v = v_0$ be a real number, and for $i \geq 0$, let $q_i = \lfloor v_i \rfloor$ and let $v_{i+1} = \frac{1}{v_i - q_i}$ if $q_i \neq v_i$. Then the (finite or infinite) continued fraction $\langle q_0, q_1, q_2, \dots \rangle$ is equal to $v$.*

*Proof.* Suppose first that $v_i = q_i$ for some $i \geq 0$, so that $v_{i+1}$ is undefined. If $i = 0$, then $v = v_0 = q_0 = \langle q_0 \rangle$ by definition, while if $i > 0$, then

$$v = \langle q_0, q_1, q_2, \dots, q_{i-1}, v_i \rangle = \langle q_0, q_1, q_2, \dots, q_{i-1}, q_i \rangle$$

by Lemma 9.4.1.

Now suppose that $v_i \neq q_i$ for all $i \geq 0$, and let $r_i = \frac{m_i}{n_i}$ be the $i$-th convergent of the infinite continued fraction $\langle q_0, q_1, q_2, \dots \rangle$, as in (9.3.1). Then by Lemmas 9.4.1 and 9.3.2,

$$v = \langle q_0, q_1, q_2, \dots, q_i, v_{i+1} \rangle = \frac{m_i \cdot v_{i+1} + m_{i-1}}{n_i \cdot v_{i+1} + n_{i-1}}$$

for all $i \geq 0$. It follows that

$$|v - r_i| = \left| \frac{m_i \cdot v_{i+1} + m_{i-1}}{n_i \cdot v_{i+1} + n_{i-1}} - \frac{m_i}{n_i} \right| = \frac{|m_{i-1} n_i - m_i n_{i-1}|}{n_i (n_i v_{i+1} + n_{i-1})} = \frac{1}{n_i (n_i v_{i+1} + n_{i-1})}$$

by Lemma 9.3.4. Notice that $v_{i+1} > q_{i+1}$ by definition, so that

$$\frac{1}{n_i(n_i v_{i+1} + n_{i-1})} < \frac{1}{n_i(n_i q_{i+1} + n_{i-1})} = \frac{1}{n_i n_{i+1}} \leq \frac{1}{n_i^2} \leq \frac{1}{i^2},$$

using facts about the $n_i$ sequence from Lemma 9.3.1. Since $0 \leq |v - r_i| < \frac{1}{i^2}$ for all $i$, then $\lim_{i\to\infty} r_i = v$, by basic facts about convergence of sequences. But we know that this limit also equals $\langle q_0, q_1, q_2, ...\rangle$. □

**Example.** In an example in §9.1, we applied the continued fraction algorithm to $v = \sqrt{19}$, and found a repeating sequence of $q$-values. We are now justified in writing

$$\sqrt{19} = \langle 4, 2, 1, 3, 1, 2, 8, 2, 1, 3, 1, 2, 8, ...\rangle,$$

that is, $v$ is equal to the continued fraction produced by this algorithm. ◊

**Uniqueness of Continued Fractions.** We established in §9.3 that every simple continued fraction is a real number, and we have now seen that every real number has some expression as a continued fraction. In this subsection, we consider whether such expressions are unique. We begin with a useful lemma for computational purposes.

**Lemma 9.4.3.** *Let $q_0, q_1, q_2, ...$ be integers, with $q_i > 0$ if $i > 0$. Then the following statements are true.*

(1) $\langle q_0, q_1, ..., q_i, w\rangle = \langle q_0, \langle q_1, ..., q_i, w\rangle\rangle$ *for all integers $i > 0$ and all real numbers $w \geq 1$.*

(2) $\langle q_0, q_1, q_2, ...\rangle = \langle q_0, \langle q_1, q_2, ...\rangle\rangle$.

Note that $\langle q_1, ..., q_i, w\rangle$ and $\langle q_1, q_2, ...\rangle$ are real numbers greater than or equal to $q_1$ by Theorem 9.3.7. Since $q_1 \geq 1$, it follows that $\langle q_0, \langle q_1, ..., q_i, w\rangle\rangle$ and $\langle q_0, \langle q_1, q_2, ...\rangle\rangle$ are well-defined continued fractions.

*Proof.* For statement (1), we use induction on $i$. If $i = 1$, then

$$\langle q_0, q_1, w\rangle = \left\langle q_0, q_1 + \frac{1}{w}\right\rangle = \langle q_0, \langle q_1, w\rangle\rangle$$

by the definition of continued fractions. So suppose that for some integer $k > 0$, we have established that $\langle q_0, q_1, ..., q_k, w\rangle = \langle q_0, \langle q_1, ..., q_k, w\rangle\rangle$ for all $w \geq 1$. Then

$$\begin{aligned}\langle q_0, q_1, ..., q_k, q_{k+1}, w\rangle &= \left\langle q_0, q_1, ..., q_k, q_{k+1} + \frac{1}{w}\right\rangle \\ &= \left\langle q_0, \left\langle q_1, ..., q_k, q_{k+1} + \frac{1}{w}\right\rangle\right\rangle = \langle q_0, \langle q_1, ..., q_k, q_{k+1}, w\rangle\rangle,\end{aligned}$$

using the definition of continued fractions and the inductive hypothesis. The result follows by induction.

Now let $v = \langle q_0, q_1, q_2, \ldots \rangle$ and $w = \langle q_1, q_2, \ldots \rangle$. By definition, $v$ is the limit of the sequence

$$\langle q_0 \rangle, \langle q_0, q_1 \rangle, \langle q_0, q_1, q_2 \rangle, \ldots, \langle q_0, q_1, q_2, \ldots, q_i \rangle, \ldots$$

as $i$ goes to infinity. But by statement (1) and the definition of continued fractions, this sequence is the same as

$$q_0, \quad q_0 + \frac{1}{\langle q_1 \rangle}, \quad q_0 + \frac{1}{\langle q_1, q_2 \rangle}, \quad \ldots, \quad q_0 + \frac{1}{\langle q_1, q_2, \ldots, q_i \rangle}, \quad \ldots.$$

Since $w$ is the limit of the sequence $\langle q_1 \rangle, \langle q_1, q_2 \rangle, \ldots, \langle q_1, q_2, \ldots, q_i \rangle, \ldots$ as $i$ goes to infinity, it follows that $v = q_0 + \frac{1}{w} = \langle q_0, w \rangle = \langle q_0, \langle q_1, q_2, \ldots \rangle \rangle$, as we wanted to show. □

**Exercise 9.4.1.** Show that $\langle q_0, q_1, \ldots \rangle = \langle q_0, q_1, \ldots, q_k, \langle q_{k+1}, q_{k+2}, \ldots \rangle \rangle$ if each $q_i$ is an integer, and $q_i > 0$ when $i > 0$.

The following example illustrates how we might use the preceding lemma and exercise for computational purposes. (We saw a similar example at the end of §9.1, based on assumptions about continued fraction expansions.)

**Example.** Let $v = \langle 5, 1, 3, 5, 1, 3, 5, 1, 3, \ldots \rangle$, where we assume that the pattern 5, 1, 3 continues indefinitely. By Exercise 9.4.1, we can write

$$v = \langle 5, 1, 3, 5, 1, 3, 5, 1, 3, \ldots \rangle = \langle 5, 1, 3, \langle 5, 1, 3, 5, 1, 3, \ldots \rangle \rangle = \langle 5, 1, 3, v \rangle.$$

Now by definition,

$$\langle 5, 1, 3, v \rangle = \left\langle 5, 1, 3 + \frac{1}{v} \right\rangle = \left\langle 5, 1 + \frac{v}{3v+1} \right\rangle = \left\langle 5 + \frac{3v+1}{4v+1} \right\rangle = \frac{23v+6}{4v+1}.$$

Then $4v^2 + v = 23v + 6$, and so $v$ satisfies the equation $2x^2 - 11x - 3 = 0$. This quadratic polynomial has two roots, $\frac{11 \pm \sqrt{145}}{4}$, but since $v$ is larger than its first convergent, $q_0 = 5$, we know that $v = \frac{11+\sqrt{145}}{4}$. ◊

**Exercise 9.4.2.** Find the value of $v$ that satisfies the following equations.

(a) $v = \langle 1, 2, v \rangle$.

(b) $v = \langle 2, 3, 5, v \rangle$.

(c) $v = \langle 2, 1, 3, 1, v \rangle$.

We have seen that a rational number can be expressed as a finite simple continued fraction. In fact, every rational number has two such expressions. For example, $\langle 1, 2, 2, 1 \rangle = \left\langle 1, 2, 2 + \frac{1}{1} \right\rangle = \langle 1, 2, 3 \rangle$ by definition, and similarly, $\langle 2, 1, 7 \rangle$

can also be written as $\langle 2, 1, 6, 1\rangle$. The following theorem asserts that, aside from this exception, continued fraction expansions of real numbers are unique.

**Theorem 9.4.4.** *Let $q_0, q_1, q_2, \ldots$ and $r_0, r_1, r_2, \ldots$ be sequences of integers with $q_i$ and $r_i$ positive if $i > 0$. Then the following statements are true.*

(1) *If $\langle q_0, q_1, q_2, \ldots\rangle = \langle r_0, r_1, r_2, \ldots\rangle$, then $q_i = r_i$ for all $i \geq 0$.*

(2) *Suppose that $\langle q_0, q_1, \ldots, q_k\rangle = \langle r_0, r_1, \ldots, r_\ell\rangle$ with $k \leq \ell$. Then $q_i = r_i$ for $0 \leq i \leq k-1$, and either $k = \ell$ and $q_k = r_k$, or $k+1 = \ell$ with $q_k = r_k + 1$ and $r_{k+1} = 1$.*

*Proof.* If $a$ is a positive integer, then a finite or infinite continued fraction with first term $a$ must be greater than or equal to 1, with equality holding only for $\langle a\rangle = \langle 1\rangle$.

(1) Suppose that $\langle q_0, q_1, q_2, \ldots\rangle = \langle r_0, r_1, r_2, \ldots\rangle$. Then by Lemma 9.4.3, we have $\langle q_0, w\rangle = \langle r_0, z\rangle$, where $w = \langle q_1, q_2, \ldots\rangle$ and $z = \langle r_1, r_2, \ldots\rangle$. So $q_0 + \frac{1}{w} = r_0 + \frac{1}{z}$ by definition, so that $q_0 - r_0 = \frac{1}{z} - \frac{1}{w}$. But $w > 1$ and $z > 1$, as noted above, which implies that $-1 < \frac{1}{z} - \frac{1}{w} < 1$. Since $q_0 - r_0$ is an integer, it follows that $q_0 = r_0$, and thus $w = z$. Now the same argument applied to $\langle q_1, q_2, \ldots\rangle = \langle r_1, r_2, \ldots\rangle$ implies that $q_1 = r_1$ and $\langle q_2, q_3, \ldots\rangle = \langle r_2, r_3, \ldots\rangle$. By induction, we find that the two continued fraction expressions must have $q_i = r_i$ for all $i \geq 0$.

(2) Suppose that $\langle q_0, q_1, \ldots, q_k\rangle = \langle r_0, r_1, \ldots, r_\ell\rangle$, with $0 \leq k \leq \ell$. Applying the same argument as in part (1), we find that $q_i = r_i$ for $0 \leq i \leq k-1$, and that $\langle q_k\rangle = \langle r_k, \ldots, r_\ell\rangle$. If $\ell = k$, then $q_k = r_k$. If $\ell > k$, then $q_k = r_k + \frac{1}{w}$, where $w = \langle r_{k+1}, \ldots, r_\ell\rangle$ and $r_{k+1} > 0$. If $r_{k+1} > 1$ or if $r_{k+2}$ is defined, then $w > 1$, making the equation $q_k - r_k = \frac{1}{w}$ impossible. Thus in this case $k+1 = \ell$ and $r_{k+1} = 1$. The result of statement (2) follows. □

**Exercise 9.4.3.** Show that a finite simple continued fraction cannot be equal to an infinite simple continued fraction.

The final three exercises will be needed in later sections.

**Exercise 9.4.4.** Suppose that $v = \langle q_0, q_1, q_2, \ldots\rangle$ is the continued fraction expansion of a real number $v$. If $n$ is an integer, what is the continued fraction of $v + n$?

**Exercise 9.4.5.** Let $v > 1$ be a real number with continued fraction expansion $\langle q_0, q_1, q_2, \ldots\rangle$. Show that $1/v = \langle 0, q_0, q_1, q_2, \ldots\rangle$.

**Exercise 9.4.6.** Let $v > 1$ be a real number. Let $r_i$ be the $i$-th convergent of $v$ and let $s_i$ be the $i$-th convergent of $1/v$. Show that $s_0 = 0$ and that $s_{i+1} = 1/r_i$ for all $i \geq 0$.

## 9.5 Purely Periodic Continued Fractions

Numerical evidence from examples in the preceding sections of Chapter 9 leads us to conjecture that when $v$ is an irrational quadratic number, then the continued fraction expansion of $v$ follows some repeating pattern, perhaps after some initial terms. Examples in §9.1 and in §9.4 similarly suggest that when the continued fraction expansion of $v$ repeats a pattern, then $v$ satisfies some quadratic polynomial equation. In this section, we verify that these conjectures are correct. We begin by introducing the following terminology and notation for this situation.

**Definition.** We say that the simple continued fraction $\langle q_0, q_1, q_2, \dots \rangle$ is *periodic* if there is an integer $k \geq 0$ and an integer $\ell > 0$ so that $q_i = q_{i+\ell}$ for all $i \geq k$. We write $\langle q_0, q_1, q_2, \dots \rangle$ as $\langle q_0, q_1, \dots, q_{k-1}, \overline{q_k, \dots, q_{k+\ell-1}} \rangle$ in this case. A periodic continued fraction is *purely periodic* if $k = 0$, that is, if $q_i = q_{i+\ell}$ for all $i \geq 0$. If $\ell$ is the smallest positive integer for which $q_i = q_{i+\ell}$ for all $i \geq k$, we call $\ell$ the *period length* of the periodic continued fraction.

**Example.** We have seen in previous examples that the continued fraction expansion of $\sqrt{19}$ repeats the pattern of $q_1$ through $q_6$ indefinitely, that is, $q_i = q_{i+6}$ for all $i \geq 1$. Specifically, we can write $\sqrt{19} = \langle 4, \overline{2, 1, 3, 1, 2, 8} \rangle$. This expansion is not purely periodic. ◊

Recall that $v$ is called a *quadratic number* if $f(v) = 0$ for some polynomial $f(x) = ax^2 + bx + c$ with integer coefficients and $a \neq 0$. When $v$ is not a rational number, then $f(x)$ is uniquely determined by $v$, under the assumption that $\gcd(a, b, c) = 1$ and that $a$ is positive. We call $f(x)$ the *minimum polynomial* of $v$, and define the *discriminant* of $v$ to equal $b^2 - 4ac$, the discriminant of $f(x)$. The second root of $f(x)$ is called the *conjugate* of $v$, written as $\overline{v}$.

In this section, we investigate *purely* periodic continued fractions. There is a simple characterization, due to Galois, of the numbers represented by these expressions.

**Theorem 9.5.1.** *Let $v = \langle \overline{q_0, q_1, \dots, q_{\ell-1}} \rangle$ be a real number expressed by a purely periodic continued fraction. Then $v$ is an irrational quadratic number with $v > 1$, and its conjugate satisfies $-1 < \overline{v} < 0$.*

**Example.** In an example in §9.4, we found that $\langle \overline{5, 1, 3} \rangle$ represents $v = \frac{11+\sqrt{145}}{4}$ $\approx 5.76$. Here $\overline{v} = \frac{11-\sqrt{145}}{4} \approx -0.26$. ◊

*Proof.* Let $v = \langle \overline{q_0, q_1, \dots, q_{\ell-1}} \rangle$. Notice that $q_0 = q_\ell$ must be a *positive* integer, and since $v$ is greater than its first convergent, $q_0$, then $v > 1$. Now because $v$ is

purely periodic, we have, using Lemma 9.3.2,

$$\upsilon = \langle q_0, q_1, \dots, q_{\ell-1}, \upsilon \rangle = \frac{m_{\ell-1}\upsilon + m_{\ell-2}}{n_{\ell-1}\upsilon + n_{\ell-2}},$$

where $m_i$ and $n_i$ are the numerator and denominator of the $i$-th convergent of $\langle q_0, q_1, \dots \rangle$. Thus $n_{\ell-1}\upsilon^2 + n_{\ell-2}\upsilon = m_{\ell-1}\upsilon + m_{\ell-2}$, and $\upsilon$ is a root of $f(x) = ax^2 + bx + c$, where

$$a = n_{\ell-1}, \qquad b = n_{\ell-2} - m_{\ell-1}, \qquad c = -m_{\ell-2}.$$

Here $\upsilon$ is not rational, since its continued fraction expansion is infinite.

Now with all $q_i$ terms positive, we find that

$$m_0 = q_0 \geq 1 = m_{-1} \quad \text{and} \quad m_i = m_{i-1}q_i + m_{i-2} > m_{i-1}$$

for $i$ positive. Likewise,

$$n_0 = 1 > 0 = n_{-1}, \quad n_1 = q_1 \geq n_0, \quad \text{and} \quad n_i = n_{i-1}q_i + n_{i-2} > n_{i-1}$$

for $i > 1$. The period length $\ell$ of the continued fraction of $\upsilon$ is at least 1, so $f(0) = -m_{\ell-2}$ is negative. On the other hand,

$$f(-1) = (n_{\ell-1} - n_{\ell-2}) + (m_{\ell-1} - m_{\ell-2})$$

is positive since, as we see above, $n_i \geq n_{i-1}$ and $m_i \geq m_{i-1}$ for all $i \geq 0$, with at least one of these a strict inequality. Therefore $f(x)$ has a root $w$ between $-1$ and 0. With $\upsilon > 1$ and a quadratic polynomial having at most two roots, $w$ must be the conjugate of $\upsilon$. □

**Reduced Quadratic Numbers.** We introduce the following terminology for a quadratic number with the property of Theorem 9.5.1.

**Definition.** If $\upsilon$ is an irrational quadratic number, we say that $\upsilon$ is *reduced* if $\upsilon > 1$ and $-1 < \overline{\upsilon} < 0$.

**Exercise 9.5.1.** Find the quadratic number $\upsilon$ represented by each of the following purely periodic continued fraction expressions. Verify in each case that $\upsilon$ is reduced.

(a) $\langle\overline{2, 5}\rangle$.

(b) $\langle\overline{2, 1, 2}\rangle$.

(c) $\langle\overline{4, 3, 1, 3}\rangle$.

Theorem 9.5.1 implies that a purely periodic continued fraction represents a reduced quadratic irrational. The converse of this statement is also true, giving us a precise criterion for which quadratic numbers are purely periodic. We prove this after some preliminary results. Recall that we say that $\Delta$ is a *discriminant* if $\Delta \equiv 0$ or $1 \pmod 4$ and $\Delta$ is not a square.

**Lemma 9.5.2.** *Let $\Delta$ be a positive discriminant. Then there are finitely many reduced quadratic numbers having discriminant $\Delta$.*

*Proof.* Let $\Delta$ be a positive discriminant, and suppose that $v$ is a reduced quadratic irrational of discriminant $\Delta$. If $f(x) = ax^2 + bx + c$ is the minimum polynomial of $v$, then

$$v = \frac{-b + \sqrt{\Delta}}{2a} > 1 \quad \text{and} \quad 0 > \overline{v} = \frac{-b - \sqrt{\Delta}}{2a} > -1. \tag{9.5.1}$$

Notice that then $v + \overline{v} = \frac{-b}{a} > 0$, so that $b < 0$. Also, multiplying the first inequality in (9.5.1) by the positive number $2a$ and the second pair by the negative number $-2a$ yields

$$-b + \sqrt{\Delta} > 2a > b + \sqrt{\Delta} > 0.$$

With $0 > b > -\sqrt{\Delta}$ and $0 < 2a < -b + \sqrt{\Delta} < 2\sqrt{\Delta}$, there are only finitely many possibilities for $v = \frac{-b+\sqrt{\Delta}}{2a}$ when $\Delta$ is fixed. □

We can be more precise about the possibilities for $v$. If $\Delta$ is given, then $b$ must have the same parity as $\Delta = b^2 - 4ac$, and $b$ is between 0 and $-\sqrt{\Delta}$ as above. For each $b$, then $a$ must satisfy $\frac{b+\sqrt{\Delta}}{2} < a < \frac{-b+\sqrt{\Delta}}{2}$. Now for each $a$ and $b$, if $a$ divides $\frac{b^2-\Delta}{4}$ (so that $c = \frac{b^2-\Delta}{4a}$ is an integer), and $\gcd(a, b, c) = 1$, then $v = \frac{-b+\sqrt{\Delta}}{2a}$ is a reduced quadratic number of discriminant $\Delta$.

**Example.** We will find all reduced quadratic numbers of discriminant $\Delta = 28$. Here $b$ must be an even number with $-\sqrt{28} \approx -5.3 < b < 0$. For each possibility, we consider integers $a$ with $\frac{b+\sqrt{28}}{2} < a < \frac{-b+\sqrt{28}}{2}$ and test whether $a$ divides $\frac{b^2-28}{4}$. If $b = -2$, then $\frac{b^2-28}{4} = -6$. We have $\frac{-2+\sqrt{28}}{2} \approx 1.65 < a < 3.65 \approx \frac{2+\sqrt{28}}{2}$. Both $a = 2$ and $a = 3$ divide $-6$, and in each case, $a$, $b$, and $c = \frac{-6}{a}$ are relatively prime. If $b = -4$, then $\frac{b^2-28}{4} = -3$. There are four possibilities for $a$ with $\frac{-4+\sqrt{28}}{2} \approx 0.65 < a < 4.65 \approx \frac{4+\sqrt{28}}{2}$, but only $a = 1$ and $a = 3$ divide $-3$. Again, $a$, $b$, and $c = \frac{-3}{a}$ are relatively prime in each case. We summarize the results in

the following table, with $v = \frac{-b+\sqrt{b^2-4ac}}{2a}$ and $\overline{v} = \frac{-b-\sqrt{b^2-4ac}}{2a}$.

| $a$ | $b$ | $c$ | $v$ | $\overline{v}$ |
|---|---|---|---|---|
| 1 | $-4$ | $-3$ | $2+\sqrt{7} \approx 4.65$ | $2-\sqrt{7} \approx -0.65$ |
| 2 | $-2$ | $-3$ | $\frac{1+\sqrt{7}}{2} \approx 1.82$ | $\frac{1-\sqrt{7}}{2} \approx -0.82$ |
| 3 | $-2$ | $-2$ | $\frac{1+\sqrt{7}}{3} \approx 1.22$ | $\frac{1-\sqrt{7}}{3} \approx -0.55$ |
| 3 | $-4$ | $-1$ | $\frac{2+\sqrt{7}}{3} \approx 1.55$ | $\frac{2-\sqrt{7}}{3} \approx -0.22$ |

The approximations in the final two columns verify that each $v$ is reduced. ◊

**Exercise 9.5.2.** For each of the following values of $\Delta$, find all reduced quadratic numbers of discriminant $\Delta$.

(a) $\Delta = 5$.

(b) $\Delta = 12$.

(c) $\Delta = 21$.

(d) $\Delta = 76$.

(e) $\Delta = 145$.

**Lemma 9.5.3.** *Let $v$ be an irrational quadratic number with discriminant $\Delta$. Let $q = \lfloor v \rfloor$ and let $v = q + \frac{1}{w}$. Then $w$ is also an irrational quadratic number with discriminant $\Delta$. Furthermore, if $v$ is reduced, then $w$ is reduced.*

*Proof.* We assume that $v$ is a root of $f(x) = ax^2 + bx + c$, where $a$, $b$, and $c$ are relatively prime integers, $a > 0$, and $\Delta = b^2 - 4ac$ is a positive integer, not a square. If $v = q + \frac{1}{w}$, then $w$ is irrational, since otherwise $v$ would be rational. Now

$$f(v) = f\left(q + \tfrac{1}{w}\right) = a\left(q + \tfrac{1}{w}\right)^2 + b\left(q + \tfrac{1}{w}\right) + c$$
$$= (aq^2 + bq + c) + (2aq + b)\tfrac{1}{w} + a \cdot \tfrac{1}{w^2} = 0$$

implies, multiplying both sides by $w^2$, that $w$ is a root of $g(x) = a'x^2 + b'x + c'$, where

$$a' = aq^2 + bq + c, \qquad b' = 2aq + b, \qquad c' = a.$$

Here $\gcd(a', b', c') = 1$, since a common divisor of $a'$, $b'$, and $c'$ would divide $a = c'$, $b = b' - 2qc'$, and $c = a' - qb' + q^2c'$, but $\gcd(a, b, c) = 1$. The

discriminant of $g$ is

$$\Delta' = (b')^2 - 4a'c' = (2aq+b)^2 - 4a(aq^2+bq+c)$$
$$= 4a^2q^2 + 4abq + b^2 - 4a^2q^2 - 4abq - 4ac = b^2 - 4ac = \Delta.$$

In general, $a' = f(q)$ is negative, since $\overline{v} < q < v$ and $a$ is positive. So $-g(x)$, which has the same discriminant as $g(x)$, is the minimum polynomial of $w$, and $w$ has discriminant $\Delta$.

Now suppose that $v$ is reduced, that is, $v > 1$ and $-1 < \overline{v} < 0$. Since $\frac{1}{w} = v - \lfloor v \rfloor$ is between 0 and 1, then $w > 1$. Notice that $g(0) = a > 0$, while

$$g(-1) = aq^2 + bq + c - 2aq - b + a = a(q^2 - 2q + 1) + b(q-1) + c = f(q-1).$$

Since $\overline{v} < 0 \leq q - 1 < v$, we know that $f(q-1)$ is negative. So $g$ changes sign between $-1$ and 0, which implies that $\overline{w}$, the second root of $g$, must satisfy $-1 < \overline{w} < 0$. So $w$ is also reduced. □

**Example.** Consider the reduced quadratic irrationals of discriminant 28, which we compiled in a previous example. If $v = \frac{1+\sqrt{7}}{2}$, then $v - \lfloor v \rfloor = \frac{-1+\sqrt{7}}{2}$, so that $w = \frac{2}{-1+\sqrt{7}} = \frac{1+\sqrt{7}}{3}$. Now $w = 1 + \frac{1}{x}$, where $x = \frac{3}{-2+\sqrt{7}} = 2 + \sqrt{7}$. Then $x = 4 + \frac{1}{y}$, where $y = \frac{1}{-2+\sqrt{7}} = \frac{2+\sqrt{7}}{3}$. Finally, $y = 1 + \frac{1}{z}$, where $z = \frac{3}{-1+\sqrt{7}} = \frac{1+\sqrt{7}}{2}$, the value of $v$ with which we began. The four values that we obtain this way are all reduced quadratic numbers of discriminant 28, as we found above. It is instructive for the next theorem to note that the process we followed in this example is exactly that of the continued fraction algorithm, which in this case shows that $\frac{1+\sqrt{7}}{2} = \langle \overline{1,1,4,1} \rangle$. ♢

**Exercise 9.5.3.** For each reduced quadratic number $v$ found in Exercise 9.5.2, show that $w = (v - \lfloor v \rfloor)^{-1}$ is also a reduced quadratic number of discriminant $\Delta$. Find the continued fraction expansion of each $v$.

**Theorem 9.5.4.** *Let $v$ be a reduced quadratic number. Then the continued fraction expansion of $v$ is purely periodic.*

*Proof.* Apply the continued fraction algorithm to $v$. Lemma 9.5.3 implies that each term in the sequence $v_0, v_1, v_2, \ldots$ is a reduced quadratic number with the same discriminant, $\Delta$, as $v$. (Because $v$ is irrational, this sequence does not terminate.) But Lemma 9.5.2 says that the number of *different* terms in this sequence must be finite. So there must be some $k \geq 0$ and $\ell > 0$ so that $v_k = v_{k+\ell}$. Assume that $k$ is as small as possible so that this is true. In this case, the continued fraction algorithm implies that $v_i = v_{i+\ell}$ and $q_i = q_{i+\ell}$ for all $i \geq k$. So the continued fraction expansion of $v$ is periodic.

To show that the expansion of $\upsilon$ is *purely* periodic, we want to show that $k = 0$. Suppose instead that $k > 0$, so that $\upsilon_{k-1}$ is a term of the $\upsilon$-sequence that is not equal to any of its successors. If $i = k + \ell$, then $\upsilon_{k-1} = q_{k-1} + \frac{1}{\upsilon_k}$ and $\upsilon_{i-1} = q_{i-1} + \frac{1}{\upsilon_i}$ with $\upsilon_k = \upsilon_i$, so that $\upsilon_{k-1} - \upsilon_{i-1}$ is an integer. Since $\upsilon_{k-1}$ and $\upsilon_{i-1}$ are quadratic numbers of discriminant $\Delta$, we can write $\upsilon_{k-1} = \frac{-b+\sqrt{\Delta}}{2a}$ and $\upsilon_{i-1} = \frac{-b'+\sqrt{\Delta}}{2a'}$ for some integers $a$, $b$, $a'$, and $b'$. Furthermore, with $\upsilon_{k-1}$ and $\upsilon_{i-1}$ reduced, so that $\upsilon_{k-1} > \overline{\upsilon_{k-1}}$ and $\upsilon_{i-1} > \overline{\upsilon_{i-1}}$, we find that $a$ and $a'$ are positive. But then with

$$\upsilon_{k-1} - \upsilon_{i-1} = \frac{(ab' - a'b) + (a' - a)\sqrt{\Delta}}{2aa'}$$

an integer, we conclude that $a = a'$. (Otherwise we could express $\sqrt{\Delta}$ as a ratio of integers.) We can rewrite $\upsilon_{k-1} - \upsilon_{i-1}$ as $\frac{b'-b}{2a}$, still given that this value is an integer.

Now $-1 < \overline{\upsilon_{k-1}} < 0$ and $-1 < \overline{\upsilon_{i-1}} < 0$ since $\upsilon_{k-1}$ and $\upsilon_{i-1}$ are reduced, that is,

$$-1 < \frac{-b - \sqrt{\Delta}}{2a} < 0 \quad \text{and} \quad -1 < \frac{-b' - \sqrt{\Delta}}{2a} < 0. \tag{9.5.2}$$

Multiplying the first pair of inequalities in (9.5.2) by the positive number $2a$ and the second pair by the negative number $-2a$, we find that $-2a < -b - \sqrt{\Delta} < 0$ and $0 < b' + \sqrt{\Delta} < 2a$, implying that $-2a < b' - b < 2a$. But then with $\frac{b'-b}{2a}$ an integer, it follows that $b' - b = 0$. So in fact, $\upsilon_{k-1} = \upsilon_{i-1}$, contradicting the assumption that $\upsilon_{k-1}$ is not equal to any successive term in the $\upsilon$-sequence. We must conclude that $k = 0$ and that the continued fraction expansion of $\upsilon$ is purely periodic. □

## 9.6 Continued Fractions of Irrational Quadratic Numbers

We can now extend the results about reduced quadratic numbers from §9.5 to arbitrary irrational quadratic numbers with the following theorem due to Lagrange.

**Theorem 9.6.1.** *The continued fraction expansion of a real number $\upsilon$ is periodic if and only if $\upsilon$ is an irrational quadratic number.*

*Proof.* Suppose first that $\upsilon = \langle q_0, q_1, \ldots, q_{k-1}, \overline{q_k, \ldots, q_{k+\ell-1}} \rangle$ is a real number with a periodic continued fraction expansion. If $w = \langle \overline{q_k, \ldots, q_{k+\ell-1}} \rangle$, then $w$ is a reduced quadratic irrational and we have that

$$\upsilon = \langle q_0, q_1, \ldots, q_{k-1}, w \rangle = \frac{m_{k-1}w + m_{k-2}}{n_{k-1}w + n_{k-2}}$$

by Lemma 9.3.2. We can show that $v$ is a quadratic number by multiplying the numerator and denominator of this quotient by $n_{k-1}\overline{w} + n_{k-2}$. Since the continued fraction expansion of $v$ does not terminate, $v$ is irrational.

Now suppose that $v$ is an irrational quadratic number. Applying the continued fraction algorithm to $v$ yields an infinite sequence, $v_0, v_1, v_2, \ldots$, of irrational quadratic numbers, all with the same discriminant as $v$, by Lemma 9.5.3. If we can show that some term in this sequence is *reduced*, then by Theorem 9.5.4 the sequences $v_i$ and $q_i$ repeat a pattern at that point, and the continued fraction expansion of $v$ is periodic. From the continued fraction algorithm, we know that $v_i > 1$ for all $i \geq 1$. If we can show that $-1 < \overline{v_i} < 0$ for *some* $i \geq 1$, then $v_i$ is reduced. We will show that this must be the case.

By Lemmas 9.4.1 and 9.3.2, we know that

$$v = \langle q_0, q_1, \ldots, q_{i-1}, v_i \rangle = \frac{v_i \cdot m_{i-1} + m_{i-2}}{v_i \cdot n_{i-1} + n_{i-2}}$$

for all positive $i$, where $m_i$ and $n_i$ are the numerator and denominator of the $i$-th convergent $r_i$ of $v$. Thus $v \cdot (v_i \cdot n_{i-1} + n_{i-2}) = v_i \cdot m_{i-1} + m_{i-2}$, and so $\overline{v} \cdot (\overline{v_i} \cdot n_{i-1} + n_{i-2}) = \overline{v_i} \cdot m_{i-1} + m_{i-2}$, by taking conjugates of both sides. Solving this equation for $\overline{v_i}$, we obtain

$$\overline{v_i} = -\frac{m_{i-2} - \overline{v} \cdot n_{i-2}}{m_{i-1} - \overline{v} \cdot n_{i-1}} = -\frac{n_{i-2}}{n_{i-1}} \left( \frac{r_{i-2} - \overline{v}}{r_{i-1} - \overline{v}} \right).$$

By Lemma 9.3.1, $n_i$ is an increasing sequence of positive integers for $i \geq 1$, so that $-1 < -\frac{n_{i-2}}{n_{i-1}} < 0$. We know that $\lim_{i \to \infty} r_i = v$, and since $v \neq \overline{v}$, it follows that

$$\lim_{i \to \infty} \frac{r_{i-2} - \overline{v}}{r_{i-1} - \overline{v}} = \lim_{i \to \infty} \frac{v - \overline{v}}{v - \overline{v}} = 1.$$

We can select $i$ large enough so that $r_{i-1} - \overline{v}$ and $r_{i-2} - \overline{v}$ are both the same sign as $v - \overline{v}$, which implies that $\frac{r_{i-2} - \overline{v}}{r_{i-1} - \overline{v}} > 0$. If $v > \overline{v}$, select $i$ also to be even. In this case we know that $r_{i-2} < v < r_{i-1}$, so that $0 < r_{i-2} - \overline{v} < r_{i-1} - \overline{v}$. Therefore, $\frac{r_{i-2} - \overline{v}}{r_{i-1} - \overline{v}} < 1$. If $v < \overline{v}$, we draw the same conclusion if we select $i$ to be odd. In any case, with $-1 < -\frac{n_{i-2}}{n_{i-1}} < 0$ and $0 < \frac{r_{i-2} - \overline{v}}{r_{i-1} - \overline{v}} < 1$, it follows that $-1 < \overline{v_i} < 0$. Thus $v_i$ is reduced for some positive integer $n$, and so the continued fraction expansion of $v$ is periodic. □

**Example.** We use $v = \left\langle 1, 3, 1, 2, 3, \overline{1, 4} \right\rangle$ to illustrate both parts of this theorem. If $w = \left\langle \overline{1, 4} \right\rangle = \langle 1, 4, w \rangle = \left\langle 1, 4 + \frac{1}{w} \right\rangle = \frac{5w+1}{4w+1}$, then $w$ satisfies the quadratic equation $4x^2 - 4x - 1 = 0$. With $w > 1$, we find that $w = \frac{1+\sqrt{2}}{2}$. Now $v = \langle 1, 3, 1, 2, 3, w \rangle$, and by calculating the third and fourth convergents of this

continued fraction (see the table below), we find that

$$v = \frac{47w + 14}{37w + 11} = \frac{75 + 47\sqrt{2}}{59 + 37\sqrt{2}} \cdot \frac{59 - 37\sqrt{2}}{59 - 37\sqrt{2}} = \frac{947 - 2\sqrt{2}}{743},$$

an irrational quadratic number.

In the following table, we verify this result by applying the continued fraction algorithm to $\frac{947-2\sqrt{2}}{743}$.

| $i$ | $v_i$ | $q_i$ | $m_i$ | $n_i$ | $r_i$ |
|---|---|---|---|---|---|
| 0 | $\frac{947-2\sqrt{2}}{743}$ | 1 | 1 | 1 | 1.0000000000 |
| 1 | $\frac{743}{204-2\sqrt{2}} = \frac{102+\sqrt{2}}{28}$ | 3 | 4 | 3 | 1.3333333333 |
| 2 | $\frac{28}{18+\sqrt{2}} = \frac{36-2\sqrt{2}}{23}$ | 1 | 5 | 4 | 1.2500000000 |
| 3 | $\frac{23}{13-2\sqrt{2}} = \frac{13+2\sqrt{2}}{7}$ | 2 | 14 | 11 | 1.2727272727 |
| 4 | $\frac{7}{-1+2\sqrt{2}} = 1 + 2\sqrt{2}$ | 3 | 47 | 37 | 1.2702702703 |
| 5 | $\frac{1}{-2+2\sqrt{2}} = \frac{1+\sqrt{2}}{2}$ | 1 | 61 | 48 | 1.2708333333 |
| 6 | $\frac{2}{-1+\sqrt{2}} = 2 + 2\sqrt{2}$ | 4 | 291 | 229 | 1.2707423581 |
| 7 | $\frac{1}{-2+2\sqrt{2}} = \frac{1+\sqrt{2}}{2}$ | 1 | 352 | 277 | 1.2707581227 |

Since $v_7 = v_5$, the continued fraction is periodic, as expected. Notice that with $v = \frac{947-2\sqrt{2}}{743} = 1.2707558181\ldots$ and $\overline{v} = \frac{947+2\sqrt{2}}{743} = 1.2783693501\ldots$, we must have $n \geq 4$ to ensure that $r_{i-1} - \overline{v}$ and $r_{i-2} - \overline{v}$ are the same sign as $v - \overline{v}$. Since $v - \overline{v} < 0$, taking $n = 5$ (the next *odd* value of $n$) is required so that $v_i$ is reduced. ♢

**Exercise 9.6.1.** Find the quadratic numbers represented by each of the following continued fraction expansions.

(a) $\langle\overline{1, 1, 2}\rangle$.

(b) $\langle 4, 3, \overline{1, 1, 2}\rangle$.

(c) $\langle 3, 7, 6, \overline{2, 5}\rangle$.

(d) $\langle 2, 1, \overline{3, 1, 5}\rangle$.

(e) $\langle 1, 2, 1, \overline{1, 2, 3}\rangle$.

**Exercise 9.6.2.** For each of the following quadratic numbers $v$, find the minimum polynomial $f(x)$ and the discriminant $\Delta$ of $v$, and find the continued fraction expansion of $v$.

(a) $v = \frac{1+\sqrt{5}}{2}$.

(b) $v = \frac{11+5\sqrt{7}}{3}$.

(c) $v = \frac{7-\sqrt{11}}{4}$.

**Exercise 9.6.3.** In each part, show that $\sqrt{d}$ has the given continued fraction expansion, when $d$ is expressed in terms of an integer $t$ as noted.

(a) $\sqrt{d} = \langle t, \overline{2t} \rangle$ when $d = t^2 + 1$ for some $t > 0$.

(b) $\sqrt{d} = \langle t-1, \overline{1, 2t-2} \rangle$ when $d = t^2 - 1$ for some $t > 1$.

(c) $\sqrt{d} = \langle t, \overline{t, 2t} \rangle$ when $d = t^2 + 2$ for some $t > 0$.

(d) $\sqrt{d} = \langle t, \overline{2, 2t} \rangle$ when $d = t^2 + t$ for some $t > 0$.

**Semi-reduced and Palindromic Quadratic Numbers.** To conclude this chapter, we define two properties that an irrational quadratic number $v$ might possess, and we describe the effect of these properties on the continued fraction expansion of $v$. In §9.5, we showed that the continued fraction expansion of a real number is purely periodic if and only if $v$ is a *reduced* irrational quadratic number, that is, a root of a quadratic polynomial, with $v$ larger than 1, and with $\overline{v}$ (the second root of the minimum polynomial of $v$) between $-1$ and 0.

**Definition.** An irrational quadratic number $v$ is said to be *semi-reduced* if there is an integer $g$ such that $g + v$ is reduced. (We allow the possibility that $g = 0$, so that a reduced irrational quadratic number is also semi-reduced.)

**Proposition 9.6.2.** *An irrational quadratic number $v$ is semi-reduced if and only if $v + \lfloor -\overline{v} \rfloor > 1$.*

*Proof.* Note that if $w = g + v$ for some integer $g$, then $\overline{w} = g + \overline{v}$. If $v$ is a fixed irrational quadratic number, there is a unique integer $g$ with $-1 < g + \overline{v} < 0$, namely $g = \lfloor -\overline{v} \rfloor$. For that integer $g$, then $w = g + v$ is reduced if and only if $w > 1$, that is, $v + \lfloor -\overline{v} \rfloor > 1$. □

**Example.** If $d > 0$ is not a square, then $v = \sqrt{d}$ is semi-reduced. Here $-\overline{v} = \sqrt{d}$, so that $v + \lfloor -\overline{v} \rfloor = \sqrt{d} + \lfloor \sqrt{d} \rfloor > 1$. ◊

Notice that if $v$ is semi-reduced, then $v > \overline{v}$. Thus if $v$ has minimum polynomial $f(x) = ax^2 + bx + c$, we can assume that $v = \frac{-b+\sqrt{\Delta}}{2a}$, where $\Delta = b^2 - 4ac$. The following proposition provides some additional criteria to ensure that a quadratic number is semi-reduced.

**Proposition 9.6.3.** *Let $\upsilon$ be an irrational quadratic number with minimum polynomial $f(x) = ax^2 + bx + c$ and suppose that $\upsilon$ is larger than $\overline{\upsilon}$. Let $\Delta = b^2 - 4ac$, the discriminant of $f(x)$ and of $\upsilon$. Then the following statements are true.*

(1) *If $2a < \sqrt{\Delta}$, then $\upsilon$ is semi-reduced.*

(2) *If $a < -c$, then $\upsilon$ is semi-reduced.*

(3) *If $a = 1$, then $\upsilon$ is semi-reduced.*

*Proof.* As noted above, we can write $\upsilon = \frac{-b+\sqrt{\Delta}}{2a}$ and then $-\overline{\upsilon} = \frac{b+\sqrt{\Delta}}{2a}$.

(1) Suppose that $2a < \sqrt{\Delta}$. Then $b + 2a < b + \sqrt{\Delta}$, and since $a$ is positive by the definition of the minimum polynomial of $\upsilon$, it follows that $\frac{b}{2a} + 1 < \frac{b+\sqrt{\Delta}}{2a} = -\overline{\upsilon}$. But in this case, $\lfloor -\overline{\upsilon} \rfloor > \frac{b}{2a}$. On the other hand, $-b + \sqrt{\Delta} > 2a - b$, and then $\upsilon > 1 - \frac{b}{2a}$. Therefore $\upsilon + \lfloor -\overline{\upsilon} \rfloor > 1 - \frac{b}{2a} + \frac{b}{2a} = 1$, and $\upsilon$ is semi-reduced by Proposition 9.6.2.

(2) Suppose that $a < -c$. Then $4a^2 < -4ac \leq b^2 - 4ac = \Delta$, again using the fact that $a$ is positive, from which it follows that $2a < \sqrt{\Delta}$. Thus $\upsilon$ is semi-reduced by statement (1).

(3) If $\upsilon$ is an irrational quadratic number, then its discriminant satisfies $\Delta \geq 5$. So if $a = 1$, then $2a < \sqrt{\Delta}$ and again we conclude that $\upsilon$ is semi-reduced by statement (1). □

The continued fraction expansion of a semi-reduced quadratic number is characterized as follows.

**Proposition 9.6.4.** *An irrational quadratic number $\upsilon$ is semi-reduced if and only if its continued fraction can be written as $\langle q_0, \overline{q_1, \dots, q_\ell} \rangle$ for some $\ell > 0$.*

*Proof.* If $\upsilon = \langle q_0, \overline{q_1, \dots, q_{\ell-1}, q_\ell} \rangle$ and $g = q_\ell - q_0$, then $g + \upsilon = \langle q_\ell, \overline{q_1, \dots, q_{\ell-1}, q_\ell} \rangle$ by Exercise 9.4.4. But then $g + \upsilon = \langle \overline{q_\ell, q_1, \dots, q_{\ell-1}} \rangle$ has a purely periodic continued fraction, so is reduced. Conversely, if $\upsilon$ is semi-reduced, then there is an integer $g$ so that $w = g + \upsilon$ is reduced. In that case, the continued fraction of $w$ is purely periodic, say of period length $\ell$, and we can write $w = \langle \overline{q_\ell, q_1, \dots, q_{\ell-1}} \rangle$. But then we find that $\upsilon = w - g = \langle q_0, \overline{q_1, \dots, q_{\ell-1}, q_\ell} \rangle$, where $q_0 = q_\ell - g$. □

**Definition.** If $\upsilon$ is a semi-reduced irrational quadratic number, we say that $\upsilon$ is *palindromic* if $\upsilon + \overline{\upsilon}$ is a rational integer.

**Example.** We saw above that if $d > 0$ is not a square, then $\upsilon = \sqrt{d}$ is semi-reduced. Here $\upsilon + \overline{\upsilon} = \sqrt{d} - \sqrt{d} = 0$, so that $\sqrt{d}$ is also palindromic. ◊

We will describe the continued fraction expansions of palindromic numbers, explaining the terminology of this definition, after some preliminary results.

**Lemma 9.6.5.** *Let $\langle q_0, q_1, q_2, \dots \rangle$ be a continued fraction, with $m_i$ and $n_i$ the numerator and denominator, respectively, of its $i$-th convergent. Then the following equations are true.*

(1) *If $q_0 > 0$, then $\langle q_i, q_{i-1}, \dots, q_2, q_1, q_0 \rangle = \frac{m_i}{m_{i-1}}$ for every $i \geq 0$.*

(2) $\langle q_i, q_{i-1}, \dots, q_2, q_1 \rangle = \frac{n_i}{n_{i-1}}$ *for every $i \geq 1$.*

*Proof.* We prove statement (1) by induction on $i$. Suppose that $q_0 > 0$. For $i = 0$, we need to show that $\langle q_0 \rangle = \frac{m_0}{m_{-1}}$. But this is true since $m_0 = q_0$ and $m_{-1} = 1$.

So now suppose we know that $\langle q_k, q_{k-1}, \dots, q_1, q_0 \rangle = \frac{m_k}{m_{k-1}}$ for some $k \geq 0$. Then

$$\begin{aligned}\langle q_{k+1}, q_k, q_{k-1}, \dots, q_1, q_0 \rangle &= \langle q_{k+1}, \langle q_k, q_{k-1}, \dots, q_1, q_0 \rangle \rangle \\ &= \left\langle q_{k+1}, \frac{m_k}{m_{k-1}} \right\rangle = q_{k+1} + \frac{m_{k-1}}{m_k} = \frac{m_{k+1}}{m_k},\end{aligned}$$

since $m_{k+1} = m_{k-1} + m_k q_{k+1}$ by equation (9.3.1). Statement (1) follows by induction. Statement (2) is similar, and is left as the following exercise. □

**Exercise 9.6.4.** Let $\langle q_0, q_1, q_2, \dots \rangle$ be a continued fraction, with $n_i$ the denominator of its $i$-th convergent. Show that $\langle q_i, q_{i-1}, \dots, q_2, q_1 \rangle = \frac{n_i}{n_{i-1}}$ for every $i \geq 1$.

**Lemma 9.6.6.** *Let $v = \langle \overline{q_0, q_1, \dots, q_{\ell-1}, q_\ell} \rangle$ be a purely periodic continued fraction and let $w = \langle \overline{q_\ell, q_{\ell-1}, \dots, q_1, q_0} \rangle$ be the continued fraction obtained by reversing the period in the first expression. Then $w = -1/\overline{v}$.*

Notice that $v$ is a reduced quadratic irrational, so that $-1 < \overline{v} < 0$. Then $w = -1/\overline{v} > 1$ and $\overline{w} = -1/v$ satisfies $-1 < \overline{w} < 0$, as should be the case since $w$ has a purely periodic continued fraction expansion.

*Proof.* For $i \geq 0$, let $m_i$, $n_i$, $m'_i$, and $n'_i$ be the numerator and denominator of the $i$-th convergents of $v$ and $w$, respectively. Then we have

$$v = \frac{m_\ell \cdot v + m_{\ell-1}}{n_\ell \cdot v + n_{\ell-1}} \quad \text{and} \quad w = \frac{m'_\ell \cdot w + m'_{\ell-1}}{n'_\ell \cdot w + n'_{\ell-1}} \tag{9.6.1}$$

as in the proof of Theorem 9.5.1. But by Corollary 9.3.3 and Lemma 9.6.5,

$$\langle q_\ell, q_{\ell-1}, \dots, q_1, q_0 \rangle = \frac{m'_\ell}{n'_\ell} = \frac{m_\ell}{m_{\ell-1}} \quad \text{and} \quad \langle q_\ell, q_{\ell-1}, \dots, q_1 \rangle = \frac{m'_{\ell-1}}{n'_{\ell-1}} = \frac{n_\ell}{n_{\ell-1}}.$$

Since

$$\gcd(m'_\ell, n'_\ell) = 1 = \gcd(m_\ell, m_{\ell-1})$$

and

$$\gcd(m'_{\ell-1}, n'_{\ell-1}) = 1 = \gcd(n_\ell, n_{\ell-1})$$

by Lemma 9.3.4, and all of these terms are positive, it follows that

$$m'_\ell = m_\ell, \qquad n'_\ell = m_{\ell-1}, \qquad m'_{\ell-1} = n_\ell, \qquad n'_{\ell-1} = n_{\ell-1}.$$

Making these substitutions and rewriting the equations in (9.6.1), we find that $v$ and $w$ are roots, respectively, of

$$f(x) = n_\ell x^2 + (n_{\ell-1} - m_\ell)x - m_{\ell-1}$$

and

$$g(x) = m_{\ell-1}x^2 + (n_{\ell-1} - m_\ell)x - n_\ell.$$

But then notice that

$$\begin{aligned} f\left(-\frac{1}{w}\right) &= n_\ell \cdot \frac{1}{w^2} - (n_{\ell-1} - m_\ell) \cdot \frac{1}{w} - m_{\ell-1} \\ &= -\frac{1}{w^2} \cdot (m_{\ell-1} \cdot w^2 + (n_{\ell-1} - m_\ell) \cdot w - n_\ell) = -\frac{1}{w^2} \cdot g(w) = 0. \end{aligned}$$

Since $-1/w < 0 < v$, and $f(x)$ has only two roots, it follows that $-1/w = \overline{v}$, that is, $w = -1/\overline{v}$, as we wanted to show. □

**Example.** Let $v = \langle \overline{1, 1, 2, 3} \rangle$ and $w = \langle \overline{3, 2, 1, 1} \rangle$. The first four convergents of $v$ are $r_0 = \frac{1}{1}$, $r_1 = \frac{2}{1}$, $r_2 = \frac{5}{3}$, and $r_3 = \frac{17}{10}$. The first four convergents of $w$ are $r'_0 = \frac{3}{1}$, $r'_1 = \frac{7}{2}$, $r'_2 = \frac{10}{3}$, and $r'_3 = \frac{17}{5}$. (Notice that $m'_3 = m_3$, $m'_2 = n_3$, $n'_3 = m_2$, and $n'_2 = n_2$, as predicted in the proof of Lemma 9.6.6.) We find that $v = \frac{17v+5}{10v+3}$ is the positive root of $f(x) = 10x^2 - 14x - 5$, while $w = \frac{17w+10}{5w+3}$ is the positive root of $g(x) = 5x^2 - 14x - 10$. So $v = \frac{7+3\sqrt{11}}{10}$ and $w = \frac{7+3\sqrt{11}}{5}$, and we can verify that $w = -1/\overline{v}$. ◊

**Example.** If $v = \langle \overline{1, 2, 1} \rangle$, then $w = \langle \overline{1, 2, 1} \rangle = v$ (following the notation of Lemma 9.6.6). So in this case, $v = -1/\overline{v}$. We leave it to the reader to verify that $v = \frac{1+\sqrt{10}}{3}$, and that this value of $v$ satisfies the equation $v = -1/\overline{v}$. ◊

**Proposition 9.6.7.** *If $v = \langle q_0, \overline{q_1, \ldots, q_\ell} \rangle$ is a semi-reduced irrational quadratic number, then $v$ is palindromic if and only if $q_i = q_{\ell-i}$ for $1 \le i \le \ell - 1$.*

In other words, the repeating pattern in the continued fraction of a palindromic irrational quadratic number, aside from the last number, forms a "palindrome," that is, reads the same forward and backward.

**Exercise 9.6.5.** Calculate $\upsilon = \left\langle \overline{1,1,3,1} \right\rangle$ as a quadratic number. (Use the fact that $\upsilon = \langle 1,1,3,1,\upsilon \rangle$.) Show that $\upsilon$ is a palindromic number without assuming Proposition 9.6.7. (Note that $\upsilon = \left\langle 1, \overline{1,3,1,1} \right\rangle$.)

**Exercise 9.6.6.** Show that $\upsilon = \left\langle \overline{1,2,1} \right\rangle$ is not a palindromic number. (Here $\upsilon = \left\langle 1, \overline{2,1,1} \right\rangle$.)

*Proof.* Let $g = q_\ell - q_0$, so that $g + \upsilon = \langle \overline{q_\ell, q_1, \ldots, q_{\ell-1}} \rangle$. Then $\frac{1}{-g-\overline{\upsilon}} = \langle \overline{q_{\ell-1}, \ldots, q_1, q_\ell} \rangle$ by Lemma 9.6.6. On the other hand, notice that $\upsilon - q_0 = \langle 0, \overline{q_1, \ldots, q_{\ell-1}, q_\ell} \rangle$, so that $\frac{1}{\upsilon - q_0} = \langle \overline{q_1, \ldots, q_{\ell-1}, q_\ell} \rangle$ by Exercise 9.4.5. If $q_i = q_{\ell-i}$ for $1 \le i \le \ell - 1$, then these continued fraction expansions are identical, so that $\frac{1}{\upsilon - q_0} = \frac{1}{-g-\overline{\upsilon}}$. But then $\upsilon + \overline{\upsilon} = q_0 - g$ is an integer, and $\upsilon$ is palindromic by definition.

Conversely, if $\upsilon + \overline{\upsilon}$ is an integer, then $-\overline{\upsilon} - g$ differs from $\upsilon$ by an integer. But $0 < -\overline{\upsilon} - g < 1$, since $g + \upsilon$ is reduced. It follows that $-\overline{\upsilon} - g = \langle 0, \overline{q_1, \ldots, q_\ell} \rangle$, and so $\frac{1}{-g-\overline{\upsilon}} = \langle \overline{q_1, \ldots, q_\ell} \rangle$. Since $\frac{1}{-g-\overline{\upsilon}} = \langle \overline{q_{\ell-1}, \ldots, q_1, q_\ell} \rangle$ as above, and the continued fraction expansion of an irrational number is unique, we conclude that $q_i = q_{\ell-i}$ for $1 \le i \le \ell - i$. □

**Exercise 9.6.7.** Let $\upsilon$ be a reduced quadratic number, with purely periodic continued fraction $\upsilon = \langle \overline{q_0, q_1, \ldots, q_{\ell-1}} \rangle$. Show that $\upsilon$ is a palindromic number if and only if the string of integers $q_1, \ldots, q_{\ell-1}$ forms a palindrome. (Allow the possibility that $\ell = 1$ so that this string is empty.)

**Exercise 9.6.8.** Let $\upsilon$ be a semi-reduced quadratic number, with minimum polynomial $f(x) = ax^2 + bx + c$. Show that $\upsilon$ is palindromic if and only if $a$ divides $b$. Show that, in this case, then $g = \lfloor \upsilon \rfloor + \frac{b}{a}$ is the integer for which $\upsilon + g$ is reduced.

**Exercise 9.6.9.** Let $\upsilon$ be the larger root of $f(x) = 3x^2 - 6x - 7$. Calculate the continued fraction of $\upsilon$, and verify that $\upsilon$ is semi-reduced and palindromic.

**Exercise 9.6.10.** Find the quadratic number $\upsilon$ with continued fraction expansion $\left\langle -2, \overline{1,2,3,2,1,4} \right\rangle$. Verify that $\upsilon$ has the properties that make it semi-reduced and palindromic.

## Continued Fractions—Review

If $q_0, q_1, q_2, \ldots$ is a sequence of integers with $q_i > 0$ for $i > 0$, then we define a *simple continued fraction* $\langle q_0, q_1, q_2, \ldots \rangle$ in terms of a sequence of rational numbers. Specifically, a finite continued fraction, such as $\langle q_0, q_1, q_2, q_3 \rangle$, is an expression

of the form

$$q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \frac{1}{q_3}}},$$

which is calculated recursively in practice. An infinite continued fraction $\langle q_0, q_1, q_2, ... \rangle$ is then defined as the limit of the sequence

$$\langle q_0 \rangle, \langle q_0, q_1 \rangle, \langle q_0, q_1, q_2 \rangle, \langle q_0, q_1, q_2, q_3 \rangle, \ldots,$$

if that limit exists. In this chapter, we established the following facts about these expressions.

(1) Every infinite simple continued fraction $\langle q_0, q_1, q_2, ... \rangle$ does in fact converge to a real number.

(2) Conversely, if $v$ is a real number, then $v$ can be expressed as a continued fraction, and there is a recursive process for constructing the $q_i$ terms from $v$. The continued fraction of $v$ is infinite, and unique, if $v$ is irrational. If $v$ is rational, then there are two distinct finite continued fractions equal to $v$.

(3) The *convergents*, $r_0 = \langle q_0 \rangle$, $r_1 = \langle q_0, q_1 \rangle$, $r_2 = \langle q_0, q_1, q_2 \rangle$, and so forth, for the continued fraction of a real number $v$ can be calculated as $r_i = m_i/n_i$ using recursive formulas for $m_i$ and $n_i$ in terms of the $q_i$ values.

(4) When $v$ is a root of a quadratic polynomial with integer coefficients, $f(x) = ax^2 + bx + c$, having positive discriminant $\Delta$ not a square, then the algorithm that produces the continued fraction of $v$ begins to repeat a pattern after a certain number of steps.

(5) The continued fraction expansion of an irrational quadratic number $v$ is *periodic*, written as $v = \langle q_0, q_1, \ldots, q_{k-1}, \overline{q_k, \ldots, q_{k+\ell-1}} \rangle$ for some nonnegative $k$ and positive $\ell$. By definition, this means that $q_{m+\ell} = q_m$ for all $m \geq k$. Furthermore, a periodic continued fraction always converges to an irrational quadratic number.

(6) The continued fraction expansion of $v$ is *purely periodic* (that is, with $k = 0$) if and only if $v$ is an irrational quadratic number for which $v > 1$ and $-1 < \overline{v} < 0$. (Here $\overline{v}$ is the second root of the minimum polynomial of $v$.) We say that $v$ is *reduced* in this situation. There are finitely many reduced irrational quadratic numbers of a fixed positive discriminant, and these can be constructed systematically.

(7) A quadratic number $v$ is *semi-reduced* if there is an integer $g$ so that $g+v$ is reduced. A semi-reduced quadratic number $v$ is *palindromic* if $v+\overline{v}$ is an integer. These properties can be determined from the continued fraction expansion of $v$.

(8) The convergents in the continued fraction expansion of a real number $v$ provide increasingly accurate rational approximations of $v$. If $d$ is a positive integer, not a square, then the convergents of $\sqrt{d}$ eventually produce a solution $(a, b)$ of *Pell's equation*, $x^2 - dy^2 = 1$. We can identify this solution with the real

number $v = a + b\sqrt{d}$. All solutions of $x^2 - dy^2 = 1$ are obtained as integer powers of the *fundamental solution*, that is, the smallest such solution $v > 1$.

In the following two chapters, we will see that this concept of continued fractions, particularly of irrational quadratic numbers, can be applied to answer questions about quadratic domains of positive discriminant, analogous to those we addressed for negative discriminants in Chapters 6 and 7. In particular, we will see that this method allows us to describe equivalences among quadratic forms or ideals of a fixed positive discriminant, and thus determine the class groups of those discriminants. We will also find that continued fractions help us construct representations of integers by indefinite quadratic forms.

# 10

# Class Groups of Positive Discriminant

In this chapter, we apply the results about continued fractions compiled in Chapter 9 to compute the class groups of ideals or of quadratic forms of positive discriminant. When $\Delta$ is negative, we saw that there is a particular collection of equivalence class representatives that we can construct in practice, the reduced ideals of discriminant $\Delta$. For positive values of $\Delta$, we can likewise select a finite list of potential class representatives, but in this case there are typically other equivalences among these candidates. We introduce an algorithm in §10.1 by which we can discover all of these equivalences, and thus obtain the class group of a positive discriminant. Using genus equivalence, we can typically determine the structure of those groups, as we will see in §10.2. We describe a broader algorithm in §10.3 for calculating the continued fraction of any irrational quadratic number. Finally, we see in §10.4 that our results establishing equivalences of indefinite quadratic forms can be viewed as applications of these continued fractions.

## 10.1 Class Groups of Indefinite Quadratic Forms

We now develop a systematic method of determining a collection of class representatives for quadratic forms or ideals of a particular positive discriminant. We will state our main results in terms of quadratic forms, with corresponding statements about ideals noted as their consequences. We begin with a restriction that

we can place on class representatives for these quadratic forms, similar to one we found for negative discriminants.

**Proposition 10.1.1.** *Let $\phi(x)$ be the principal polynomial of some positive discriminant $\Delta$, and let $w$ be the smaller root of $\phi(x)$. Then every element of $\mathcal{Q}_\Delta$ is equivalent to a quadratic form $f = (a : k)$ with $|a| \leq \sqrt{\Delta/4}$ and $w < k < w + |a|$.*

*Proof.* Let $f(x, y) = ax^2 + bxy + cy^2$ be a quadratic form of discriminant $\Delta = b^2 - 4ac > 0$, and assume that $|a|$ is as small as possible among forms that are equivalent to $f$. In particular, then $|a| \leq |c|$ since $f$ is equivalent to its involution, $cx^2 - bxy + ay^2$, by Proposition 4.2.2. Using a translation, as in Proposition 4.2.3, we can further assume that $|b| \leq |a|$. In this case, we find that $a$ and $c$ must have opposite sign, since otherwise

$$4a^2 \leq 4ac = b^2 - \Delta \leq a^2 - \Delta,$$

so that $3a^2 \leq -\Delta$, impossible if $\Delta$ is positive. So instead,

$$4a^2 \leq -4ac = \Delta - b^2 \leq \Delta,$$

from which we conclude that $|a| < \sqrt{\Delta/4}$, since $\Delta$ is not a square. Now rewrite $f$ in ideal notation as $(a : k)$. Using a translation, we may replace $k$ by any number to which it is congruent modulo $|a|$, and so assume that $w < k < w + |a|$. □

**Definition.** We refer to $u_\Delta = \left\lfloor \sqrt{\Delta/4} \right\rfloor$ as the *upper bound* of a positive discriminant $\Delta$. We will say that a quadratic form of discriminant $\Delta > 0$ is a *candidate form* if it satisfies the conditions of Proposition 10.1.1.

As our terminology suggests, the forms defined in the preceding proposition are "candidates" for representatives of the form class group of a positive discriminant. But there are generally other equivalences among these forms, as we see in the following example, which also illustrates a procedure for listing all candidate forms.

**Example.** Let $\Delta = 73$, so that $u_\Delta = \left\lfloor \sqrt{73/4} \right\rfloor = 4$. The principal polynomial of discriminant $\Delta$ is $\phi(x) = x^2 + x - 18$, and $w = \frac{-1-\sqrt{73}}{2} \approx -4.8$. To compile the candidate forms of discriminant 73, it suffices to calculate $\phi(x)$ for $-4 \leq x \leq -1$. For later results, we note that $\phi(x) = \phi(-x - \varepsilon)$, and we pair these "conjugate" values in the following table, which consists precisely of all negative values taken on by $\phi(x)$ at integers $x$.

| $x$ | $-4, 3$ | $-3, 2$ | $-2, 1$ | $-1, 0$ |
|---|---|---|---|---|
| $\phi(x)$ | $-6$ | $-12$ | $-16$ | $-18$ |

Now for $1 \leq a \leq 4$, we test which values of $\phi(k)$ with $-4.8 < k < -4.8 + a$ are divisible by $\pm a$. We obtain the following list of candidate forms of discriminant 73.

(We write $(\pm a : k)$ for the distinct quadratic forms $(a : k)$ and $(-a : k)$ in lists of this type.)

$$(\pm 1 : -4), (\pm 2 : -4), (\pm 2 : -3), (\pm 3 : -4), (\pm 3 : -3), (\pm 4 : -3), (\pm 4 : -2).$$

Proposition 10.1.1 implies that every element of $\mathcal{Q}_{73}$ is equivalent to (at least) one of these forms. But there may well be equivalences among these forms. Here, for instance, we find that $(3 : -3) \sim (-4 : 2) \sim (-4 : -2)$ by an involution and translation. ◊

**Exercise 10.1.1.** Find all candidate forms of each discriminant $\Delta$ below.

(a) $\Delta = 17$.

(b) $\Delta = 28$.

(c) $\Delta = 33$.

(d) $\Delta = 37$.

(e) $\Delta = 57$.

(f) $\Delta = 65$.

(g) $\Delta = 88$.

(h) $\Delta = 93$.

(i) $\Delta = 104$.

(j) $\Delta = 152$.

**The Equivalence Algorithm on Candidate Forms.** We now state our main theorem for this section, describing a method by which we can determine all possible equivalences among the candidate forms of positive discriminant produced by Proposition 10.1.1. We will delay the proof of this claim until the final section of Chapter 10, where we will see that this method is an application of a broader algorithm to construct the continued fraction expansion of an arbitrary irrational quadratic number.

**Theorem 10.1.2.** *Let $\phi(x) = x^2 + \varepsilon x + \frac{\varepsilon^2 - \Delta}{4}$ be the principal polynomial of some positive discriminant $\Delta$, let $w$ be the smaller root of $\phi(x)$, and let $u_\Delta$ be the upper bound of $\Delta$. Let $f = (a : k)$ be an element of $\mathcal{Q}_\Delta$ for which $0 < a < u_\Delta$ and $w < k < w + a$. Let $a_0 = a$ and $k_0 = k$, and for $i \geq 0$, let $k_{i+1}$ be congruent to $-k_i - \varepsilon$ modulo $a_i$ with $k_{i+1} > w$ as small as possible, and let*

$$a_{i+1} = -\frac{\phi(k_{i+1})}{a_i}.$$

*Then each $a_i$ is an integer dividing $\phi(k_i)$, and*

$$(a_i : k_i) \sim (-a_{i+1} : k_{i+1}) \quad \textit{and} \quad (-a_i : k_i) \sim (a_{i+1} : k_{i+1})$$

*for all $i \geq 0$. In this situation, there is a smallest even positive integer $m$ so that $a_m = a$ and $k_m = k$. If $g = (a' : k')$ is a candidate quadratic form of discriminant $\Delta$, then $g$ is equivalent to $f$ if and only if either $a' = a_i$ and $k' = k_i$ for some even $i$, or $a' = -a_i$ and $k' = k_i$ for some odd $i$, with $0 < i \leq m$.*

Theorem 10.1.2 implies that given a candidate form $f$ of positive discriminant $\Delta$, we can determine precisely the other candidates to which $f$ is equivalent. Thus we can construct the form class group of discriminant $\Delta$. We refer to the procedure described in this theorem as the *equivalence algorithm* applied to a candidate form $f = (a : k)$ of positive discriminant. We demonstrate its application with examples in the remainder of this section.

**Example.** The following table compiles data produced by applying the equivalence algorithm to $f = (1 : -4)$, a candidate form of discriminant $\Delta = 73$, as we saw previously.

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| $a$ | 1 | 6 | 2 | 3 | 4 | 4 | 3 | 2 | 6 | 1 |
| $k$ | $-4$ | $-4$ | $-3$ | $-4$ | $-3$ | $-2$ | $-3$ | $-4$ | $-3$ | $-4$ |

Here we use calculations of $\phi(x)$ from a table in the preceding example.

(1) To calculate $k_1$, we begin with $-k_0 - \varepsilon = 3$, the conjugate value of $k_0$. With $a_0 = 1$, we select the smallest $k_1 > w$ for which $k_1 \equiv 3 \pmod 1$, that is, $k_1 = -4$. Now $a_1 = -\frac{\phi(-4)}{a_0} = 6$. (Notice that $a_1$ divides $\phi(k_1)$ as claimed in Theorem 10.1.2.)

(2) Now $-k_1 - \varepsilon = 3$, and we select the minimal $k_2 \equiv 3 \pmod 6$, that is, $k_2 = -3$. So then $a_2 = -\frac{\phi(-3)}{a_1} = 2$.

(3) Then $-k_2 - \varepsilon = 2$, and $k_3 = -4$ is the minimal possibility for which $k_3 \equiv 2 \pmod 2$. Thus $a_3 = \frac{\phi(-4)}{a_2} = 3$.

Continuing these steps, we find in this example that $a_9 = 1$ and $k_9 = -4$. Since $a_{i+1}$ and $k_{i+1}$ are determined purely from the values of $a_i$ and $k_i$, we now see that the sequence of $a_i$ and $k_i$ values will repeat the pattern of this table indefinitely, and we can terminate the algorithm when this occurs. Note that $m = 18$ is the smallest positive *even* integer for which $a_m = a$ and $k_m = k$. Theorem 10.1.2 now implies that we have the following sequence of equivalences:

$$\begin{aligned}(1 : -4) &\sim (-6 : -4) \sim (2 : -3) \sim (-3 : -4) \sim (4 : -3) \sim (-4 : -2) \\ &\sim (3 : -3) \sim (-2 : -4) \sim (6 : -3) \sim (-1 : -4) \sim (6 : -4) \sim (-2 : -3) \\ &\sim (3 : -4) \sim (-4 : -3) \sim (4 : -2) \sim (-3 : -3) \sim (2 : -4) \sim (-6 : -3).\end{aligned}$$

Every candidate form of discriminant $\Delta = 73$ appears in this list (as well as some forms that do not fit the criterion that $|a| < u_\Delta$). Our conclusion is that all elements of $\mathcal{Q}_{73}$ are in the same class, and we can draw the same conclusion for ideals of the quadratic domain $D_{73}$. ◊

**Example.** Let $\Delta = 221$, with $\phi(x) = x^2 + x - 55$ having smaller root $w = \frac{-1-\sqrt{221}}{2} \approx -7.9$, and with $u_\Delta = \left\lfloor \sqrt{221/4} \right\rfloor = 7$. To find candidate forms, we list all values of $x$ for which $\phi(x)$ is negative, pairing each $x$ with its conjugate $-x - \varepsilon = -x - 1$.

| $x$ | $-7,6$ | $-6,5$ | $-5,4$ | $-4,3$ | $-3,2$ | $-2,1$ | $-1,0$ |
|---|---|---|---|---|---|---|---|
| $\phi(x)$ | $-13$ | $-25$ | $-35$ | $-43$ | $-49$ | $-53$ | $-55$ |

We find the following list of potential representatives for all quadratic forms in $\mathcal{Q}_{221}$:

$$(\pm 1 : -7), \quad (\pm 5 : -6), \quad (\pm 5 : -5), \quad (\pm 7 : -5), \quad (\pm 7 : -3).$$

To determine whether there are equivalences among these forms, we apply the equivalence algorithm to pairs $a$ and $k$ listed here, as in the tables below.

| $i$ | 0 | 1 | 2 |
|---|---|---|---|
| $a$ | 1 | 13 | 1 |
| $k$ | $-7$ | $-7$ | $-7$ |

| $i$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| $a$ | 5 | 7 | 7 | 5 | 5 |
| $k$ | $-6$ | $-5$ | $-3$ | $-5$ | $-6$ |

Note that in both tables, our form recurs the first time after an even number of steps. From the first table, we find that

$$(1 : -7) \sim (-13 : -7) \quad \text{and} \quad (-1 : -7) \sim (13 : -7),$$

but this does not establish any equivalences with other candidate forms. From the second table, however, we see that

$$(5 : -6) \sim (-7 : -5) \sim (7 : -3) \sim (-5 : -5)$$

and

$$(-5 : -6) \sim (7 : -5) \sim (-7 : -3) \sim (5 : -5).$$

This accounts for all candidate forms, and so every quadratic form in $\mathcal{Q}_{221}$ is equivalent to $(1 : -7)$, $(-1 : -7)$, $(5 : -6)$, or $(-5 : -6)$. The final statement in Theorem 10.1.2 ensures that no two of these forms can be equivalent. So there are precisely four classes of quadratic forms of discriminant 221. Note however that the ideals $[1 : -7]$ and $[-1 : -7]$ are equal, and thus equivalent, as are $[5 : -6]$ and $[-5 : -6]$. Hence there are two distinct classes of ideals of discriminant 221. ◊

**Example.** If $\Delta = \Delta(74, 1) = 296$, then $\phi(x) = x^2 - 74$, with smaller root $w = -\sqrt{74} \approx -8.6$, and $u_\Delta = 8$. The table

| $x$ | $\pm 8$ | $\pm 7$ | $\pm 6$ | $\pm 5$ | $\pm 4$ | $\pm 3$ | $\pm 2$ | $\pm 1$ | $0$ |
|---|---|---|---|---|---|---|---|---|---|
| $\phi(x)$ | $-10$ | $-25$ | $-38$ | $-49$ | $-58$ | $-65$ | $-70$ | $-73$ | $-74$ |

yields this collection of candidate forms $(a : k)$ in $\mathcal{Q}_{296}$:

$$(\pm 1 : -8), \quad (\pm 2 : -8), \quad (\pm 5 : -8), \quad (\pm 5 : -7), \quad (\pm 7 : -5), \quad (\pm 7 : -2).$$

The next tables compile data from the equivalence algorithm applied to two of these forms.

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| $a$ | 1 | 10 | 7 | 7 | 10 | 1 |
| $k$ | $-8$ | $-8$ | $-2$ | $-5$ | $-2$ | $-8$ |

| $i$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| $a$ | 2 | 5 | 5 | 2 |
| $k$ | $-8$ | $-8$ | $-7$ | $-8$ |

We conclude that

$$(1 : -8) \sim (-10 : -8) \sim (7 : -2) \sim (-7 : -5) \sim (10 : -2) \sim (-1 : -8) \sim \cdots,$$

returning to $(1 : -8)$ after $m = 10$ steps. Likewise,

$$(2 : -8) \sim (-5 : -8) \sim (5 : -7) \sim (-2 : -8) \sim (5 : -8) \sim (-5 : -7).$$

Thus there are two distinct classes of quadratic forms in $\mathcal{Q}_{296}$, which are represented by $(1 : -8)$ and $(2 : -8)$. There are likewise two distinct classes of ideals of $D_{296}$. $\Diamond$

**Exercise 10.1.2.** For each discriminant $\Delta$, find all distinct classes of quadratic forms in $\mathcal{Q}_\Delta$ and all distinct classes of ideals of the quadratic domain $D_\Delta$. (Note that these values of $\Delta$ are the same as in Exercise 10.1.1.)

(a) $\Delta = 17$.

(b) $\Delta = 28$.

(c) $\Delta = 33$.

(d) $\Delta = 37$.

(e) $\Delta = 57$.

(f) $\Delta = 65$.

(g) $\Delta = 88$.

(h) $\Delta = 93$.

(i) $\Delta = 104$.

(j) $\Delta = 152$.

## 10.2 Genera of Quadratic Forms and Ideals

In §10.1, we developed a practical method for listing all distinct classes of indefinite quadratic forms of discriminant $\Delta$, and likewise all distinct classes of ideals of the real quadratic domain $D_\Delta$. In this section, we look more closely at the structure of the ideal class group $\mathcal{C}_\Delta$ and form class group $\mathcal{F}_\Delta$ when $\Delta$ is positive, using genera of quadratic forms and ideals, as we did in §6.3. The situation is somewhat more complicated when $\Delta$ is positive because of the necessary distinction between equivalence of ideals and equivalence of quadratic forms.

Recall that if $f = (a : k)$ is a primitive quadratic form of discriminant $\Delta$, we define a collection of *genus symbols* for $f$, based on the prime numbers that divide $\Delta$. (See §4.4 for details.) We say that $f$ and $g$ are in the same *genus*, or are *genus equivalent*, if they have the same collection of genus symbols. Equivalent quadratic forms are always genus equivalent. For the ideal class group $G = \mathcal{C}_\Delta$, the principal genus $H = \mathcal{G}_\Delta$ is made up of all classes of ideals for which every defined genus symbol equals 1. We found in §6.3 that $H = G^2$, the subgroup of $G$ consisting of the squares of all ideal classes. The genus of an ideal class $[A]$ is $[A] \cdot H$, the coset of $H$ in $G$ determined by $[A]$. The number of genera of classes equals $2^\ell$, where $\ell$ is the number of even terms in the invariant factor type of $G$. When $D_\Delta$ is a *complete* quadratic domain with $\Delta$ positive, we have the following formula for the number of genera of quadratic forms in $\mathcal{Q}_\Delta$, and the number of genera in the ideal class group $\mathcal{C}_\Delta$.

**Theorem 10.2.1.** *Let $D$ be a complete quadratic domain of positive discriminant $\Delta$, let $t$ be the number of distinct prime factors of $\Delta$, and let $s$ be the number of those factors that are congruent to 3 modulo 4. Then the number of genera of quadratic forms of discriminant $\Delta$ is $2^{t-1}$. The number of genera of ideal classes of $D$ is $2^{t-1}$ if $s = 0$, and is $2^{t-2}$ if $s > 0$.*

Notice that if $s$ is positive, then $\Delta$ must have at least two prime divisors. So the number of genera asserted in this theorem is an integer in every case. We illustrate Theorem 10.2.1 with several examples before looking at its proof.

**Example.** Let $\Delta = \Delta(65, 1) = 65 = 5 \cdot 13$, with $\phi(x) = x^2 + x - 16$. From the following table, we see that candidate forms $(a : k)$ exist with $a = \pm 1, \pm 2$, and $\pm 4$.

| $x$ | $-4, 3$ | $-3, 2$ | $-2, 1$ | $-1, 0$ |
|---|---|---|---|---|
| $\phi(x)$ | $-4$ | $-10$ | $-14$ | $-16$ |

We apply the equivalence algorithm of Theorem 10.1.2 to two of them.

| $i$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| $a$ | 1 | 4 | 4 | 1 |
| $k$ | $-4$ | $-4$ | $-1$ | $-4$ |

| $i$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| $a$ | 2 | 5 | 2 | 2 |
| $k$ | $-4$ | $-3$ | $-3$ | $-4$ |

We conclude that

$$(1 : -4) \sim (-4 : -4) \sim (4 : -1) \sim (-1 : -4) \sim (4 : -4) \sim (-4 : -1)$$

and

$$(2 : -4) \sim (-5 : -3) \sim (2 : -3) \sim (-2 : -4) \sim (5 : -3) \sim (-2 : -3).$$

Thus there are two distinct classes of forms in $\mathcal{Q}_{65}$, represented by $(1 : -4)$ and $(2 : -4)$, for example. Notice that if $f = (1 : -4)$, then $\left(\frac{f}{5}\right) = 1 = \left(\frac{f}{13}\right)$, while if $f = (2 : -4)$, then $\left(\frac{f}{5}\right) = -1 = \left(\frac{f}{13}\right)$. The same is true of any representatives we might select.

In this example, there are two distinct classes of ideals in $D = D_{65}$, with $D = [1 : -4]$ and $P = [2 : -4]$ as possible representatives. The ideal class group $\mathcal{C}_{65}$ must have invariant factor type (2), as we can confirm by noting that $P^2 = [4 : -4] \sim D$. Since there is one even invariant factor, there are $2^1 = 2$ genera of ideal classes in $\mathcal{C}_{65}$, each containing one class. In the terminology of Theorem 10.2.1, $\Delta$ has $t = 2$ prime divisors, with $s = 0$ of them congruent to 3 modulo 4. So we expect $2^{2-1} = 2$ genera, both of quadratic forms and ideals, as we see here. ◊

**Example.** Let $\Delta = \Delta(57, 1) = 57 = 3 \cdot 19$, with $\phi(x) = x^2 + x - 14$. The table

| $x$ | $-4, 3$ | $-3, 2$ | $-2, 1$ | $-1, 0$ |
|---|---|---|---|---|
| $\phi(x)$ | $-2$ | $-8$ | $-12$ | $-14$ |

shows that candidate forms $(a : k)$ exist with $a = \pm 1, \pm 2$, and $\pm 3$. Applying the equivalence algorithm to $(1 : -4)$, for example,

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| $a$ | 1 | 2 | 4 | 3 | 4 | 2 | 1 |
| $k$ | $-4$ | $-4$ | $-3$ | $-2$ | $-2$ | $-3$ | $-4$ |

we find that in $\mathcal{Q}_{57}$,

$$(1 : -4) \sim (-2 : -4) \sim (4 : -3) \sim (-3 : -2) \sim (4 : -2) \sim (-2 : -3)$$

and

$$(-1 : -4) \sim (2 : -4) \sim (-4 : -3) \sim (3 : -2) \sim (-4 : -2) \sim (2 : -3).$$

Here $\left(\frac{f}{3}\right) = 1 = \left(\frac{f}{19}\right)$ for each form $f$ in the first list, while $\left(\frac{f}{3}\right) = -1 = \left(\frac{f}{19}\right)$ in the second list. So there are two distinct classes of quadratic forms in $\mathcal{Q}_{57}$, each in a separate genus. On the other hand, all ideals of $D = D_{57}$ are equivalent, so that $\mathcal{C}_{57}$ is the trivial group. Here $t = 2$ and $s = 2$, so we expect to see $2^{2-1} = 2$ genera of quadratic forms, but only $2^{2-2} = 1$ genus of ideals. ◊

**Example.** Let $\Delta = \Delta(79,1) = 316 = 2^2 \cdot 79$, with $\phi(x) = x^2 - 79$. From the table

| $x$ | $\pm 8$ | $\pm 7$ | $\pm 6$ | $\pm 5$ | $\pm 4$ | $\pm 3$ | $\pm 2$ | $\pm 1$ | $0$ |
|---|---|---|---|---|---|---|---|---|---|
| $\phi(x)$ | $-15$ | $-30$ | $-43$ | $-54$ | $-63$ | $-70$ | $-75$ | $-78$ | $-79$ |

we find candidate forms $(a : k)$ with $a = \pm 1, \pm 2, \pm 3, \pm 5, \pm 6$, and $\pm 7$. Applying the equivalence algorithm in the tables

| $i$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| $a$ | 1 | 15 | 2 | 15 | 1 |
| $k$ | $-8$ | $-8$ | $-7$ | $-7$ | $-8$ |

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| $a$ | 3 | 10 | 7 | 9 | 6 | 5 | 3 |
| $k$ | $-8$ | $-7$ | $-3$ | $-4$ | $-5$ | $-7$ | $-8$ |

and

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| $a$ | 3 | 5 | 6 | 9 | 7 | 10 | 3 |
| $k$ | $-7$ | $-8$ | $-7$ | $-5$ | $-4$ | $-3$ | $-7$ |

we find that there are six distinct classes of quadratic forms, with representatives

$$(1 : -8), \quad (-1 : -8), \quad (3 : -8), \quad (-3 : -8), \quad (3 : -7), \quad (-3 : -7).$$

Here $\left(\frac{-1}{f}\right) = 1 = \left(\frac{f}{79}\right)$ for $(1 : -8)$, $(-3 : -8)$, and $(-3 : -7)$, while $\left(\frac{-1}{f}\right) = -1 = \left(\frac{f}{79}\right)$ for $(-1 : -8)$, $(3 : -8)$, and $(3 : -7)$, so there are two distinct genera of quadratic forms. For ideals, we find three distinct classes ($[1 : -8]$, $[3 : -8]$, and $[3 : -7]$), each in the same genus. The ideal class group has invariant factor type (3). Here $\Delta = 316$ has $t = 2$ prime divisors, with $s = 1$ of them congruent to 3 modulo 4. So we expect to have $2^{2-1} = 2$ genera of quadratic forms, and $2^{2-2} = 1$ genus of ideals, as seen here. ◊

**Example.** Let $\Delta = \Delta(130,1) = 520 = 2^3 \cdot 5 \cdot 13$, so that $\Delta$ has $t = 3$ prime divisors, with $s = 0$ of them congruent to 3 modulo 4. We expect that there are $2^{3-1} = 4$ genera of quadratic forms, and the same number of genera of ideals in $D = D_{520}$. (Here the genus symbols $\left(\frac{2}{f}\right)$, $\left(\frac{f}{5}\right)$, and $\left(\frac{f}{13}\right)$ are defined, and are written in that order in lists below.) We compile the following (partial) table of values taken on by the principal polynomial $\phi(x) = x^2 - 130$.

| $x$ | $\pm 11$ | $\pm 10$ | $\pm 9$ | $\pm 8$ | $\pm 7$ | $\pm 6$ | $\pm 5$ | $\pm 4$ | $\pm 3$ | $\cdots$ |
|---|---|---|---|---|---|---|---|---|---|---|
| $\phi(x)$ | $-9$ | $-30$ | $-49$ | $-66$ | $-81$ | $-94$ | $-105$ | $-114$ | $-121$ | $\cdots$ |

Applying the equivalence algorithm to various candidtate forms, we find four disjoint cycles, each of odd length.

| $i$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| $a$ | 1 | 9 | 9 | 1 |
| $k$ | $-11$ | $-11$ | $-7$ | $-11$ |

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| $a$ | 2 | 15 | 7 | 7 | 15 | 2 |
| $k$ | $-10$ | $-10$ | $-5$ | $-9$ | $-5$ | $-10$ |

| $i$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| $a$ | 3 | 10 | 3 | 3 |
| $k$ | $-11$ | $-10$ | $-10$ | $-11$ |

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| $a$ | 5 | 6 | 11 | 11 | 6 | 5 |
| $k$ | $-10$ | $-10$ | $-8$ | $-3$ | $-8$ | $-10$ |

For example, the first table indicates that

$$(1 : -11) \sim (-9 : -11) \sim (9 : -7) \sim (-1 : -11) \sim (9 : -11) \sim (-9 : -7).$$

We conclude that there are four distinct classes of quadratic forms, each in a separate genus:

$$+++ : (1 : -11), \quad +-- : (2 : -10), \quad --+ : (3 : -11), \quad -+- : (5 : -10).$$

There are likewise four classes of ideals, and the class group $\mathcal{C}_{520}$ has invariant factor type $(2, 2)$. ◊

**Exercise 10.2.1.** For each of the following discriminant values, list all elements in the form class group $\mathcal{F}_\Delta$, indicate how these elements are partitioned into distinct genera, and determine the invariant factor type of this group. Do the same for the ideal class group $\mathcal{C}_\Delta$.

(a) $\Delta = 37$.

(b) $\Delta = 40$.

(c) $\Delta = 61$.

(d) $\Delta = 92$.

(e) $\Delta = 93$.

(f) $\Delta = 105$.

(g) $\Delta = 156$.

(h) $\Delta = 328$.

(i) $\Delta = 440$.

(j) $\Delta = 568$.

*Proof of Theorem* 10.2.1. As we saw in the proof of Proposition 6.3.4, if $\Delta$ has $t$ distinct prime divisors, then there are $t$ genus symbols defined for quadratic forms $f$ of discriminant $\Delta$. But the product of these symbols must equal 1, so there are $2^{t-1}$ possible collections of genus symbols of forms.

Suppose now that $f = (a : k)$ is a quadratic form of discriminant $\Delta$. Then $g = (-a : k)$ is also in $\mathcal{Q}_\Delta$, since $a$ and $-a$ both divide $\phi(k)$. If $\Delta$ has any prime divisor $p \equiv 3 \pmod 4$, then $\left(\frac{f}{p}\right) \neq \left(\frac{g}{p}\right)$, so that $f$ and $g$ are in different genera. But the ideals $A_f$ and $A_g$ are identical, so are in the same genus. Thus we see that

the number of genera of ideals is half the number of genera of quadratic forms, that is, $2^{t-2}$. On the other hand, if $\Delta$ has no prime divisor congruent to 3 modulo 4, then $\left(\frac{f}{p}\right) = \left(\frac{g}{p}\right)$ for every odd prime divisor $p$ of $\Delta$, and so $f$ and $g$ are in the same genus. (Notice that $\Delta$ must be congruent to 1 modulo 4, so that none of the symbols $\left(\frac{-1}{f}\right)$, $\left(\frac{2}{f}\right)$, or $\left(\frac{-2}{f}\right)$ is defined in this case.) Thus there are $2^{t-1}$ genera, both of quadratic forms and of ideals, in this situation. □

We conclude this section with one more example to illustrate the complications that arise when the quadratic domain $D_\Delta$ is not complete.

**Example.** Let $\Delta = \Delta(65, 3) = 585 = 3^2 \cdot 5 \cdot 13$. Here $\phi(x) = x^2 + 3x - 144$, with $\phi(-x-3) = \phi(x)$, and $\phi(x)$ is negative for the values partially presented below.

| $-x-3$ | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | $\cdots$ |
|---|---|---|---|---|---|---|---|---|---|
| $x$ | $-13$ | $-12$ | $-11$ | $-10$ | $-9$ | $-8$ | $-7$ | $-6$ | $\cdots$ |
| $\phi(x)$ | $-14$ | $-36$ | $-56$ | $-74$ | $-90$ | $-104$ | $-116$ | $-126$ | $\cdots$ |

For $a < \sqrt{\Delta/4}$, we find that quadratic forms $(a : k)$ exist for $\pm1$, $\pm2$, $\pm3$, $\pm4$, $\pm5$, $\pm6$, $\pm7$, $\pm8$, $\pm9$, $\pm10$, and $\pm12$, but those with $a = \pm3$, $\pm6$, and $\pm12$ are not primitive. (These correspond to the forms listed in the previous example of $\Delta = 65$ in this section, each multiplied by 3.) For the other forms, we find the following data when we apply the equivalence algorithm on $(1 : -13)$ and on $(2 : -13)$. (Here $a_{12} = 1$ and $k_{12} = -13$ for the first collection of data.)

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $a$ | 1 | 14 | 10 | 9 | 4 | 14 | 9 | 14 | 4 | 9 | 10 | 14 |
| $k$ | $-13$ | $-13$ | $-4$ | $-9$ | $-12$ | $-11$ | $-6$ | $-6$ | $-11$ | $-12$ | $-9$ | $-4$ |

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $a$ | 2 | 18 | 5 | 18 | 2 | 7 | 8 | 13 | 8 | 7 | 2 |
| $k$ | $-13$ | $-12$ | $-9$ | $-9$ | $-12$ | $-13$ | $-11$ | $-8$ | $-8$ | $-11$ | $-13$ |

With the period length of both expansions even, we conclude that there are four separate classes of primitive quadratic forms. Each is in a distinct genus, determined by the genus symbols $\left(\frac{f}{3}\right)$, $\left(\frac{f}{5}\right)$, and $\left(\frac{f}{13}\right)$ as follows:

$$+++ : (1 : -13), \quad -++ : (-1 : -13),$$
$$--- : (2 : -13), \quad +-- : (-2 : -13).$$

On the other hand, the ideals of $D_{585}$ are in two genera, each containing one class, and $\mathcal{C}_{585}$ has invariant factor type (2). ◊

If $\Delta = 65$ and $p = 3$, then there is a homomorphism $\psi : \mathcal{F}_{p^2\Delta} \to \mathcal{F}_\Delta$ as defined in §8.1. Here $\phi(x) \equiv 0 \pmod 3$ has no solutions, and so the kernel of

$\psi$ might have as many as $p+1=4$ elements. But in fact, since $|\mathcal{F}_\Delta|=2$ and $|\mathcal{F}_{p^2\Delta}|=4$, there are two elements in the kernel. We will address the question of the connection between $\mathcal{F}_\Delta$ and $\mathcal{F}_{p^2\Delta}$ when $\Delta$ is positive in §13.3.

## 10.3 Continued Fractions of Irrational Quadratic Numbers

In §9.2, we introduced an algorithm for computing the continued fraction of a square root, $\sqrt{d}$ with $d>0$ not a square, and we applied this procedure to the construction of the fundamental solution of Pell's equation, $x^2-dy^2=1$. We can extend this approach to a more general algorithm for the continued fraction of an arbitrary irrational quadratic number. The reader will likely recognize a similarity between the method described in the following theorem and the equivalence algorithm that we have applied to candidate forms of positive discriminant throughout §10.1 and §10.2. We will make that connection more apparent in the final section of this chapter.

**Theorem 10.3.1** (Quadratic Continued Fraction Algorithm)**.** *Let $v$ be a quadratic number, written as $v=q+r\sqrt{d}$, where $d>1$ is a squarefree integer, and $q$ and $r$ are rational numbers with $r\neq 0$. Let $ax^2+bx+c$ be a polynomial having $v$ as a root, with $\gcd(a,b,c)=1$ and with $a$ the same sign as $r$. Let $\phi(x)$ be the principal polynomial of discriminant $\Delta=b^2-4ac$, and let $w$ be the smaller root of $\phi(x)$. Let $a_0=a$ and $k_0=\frac{b-\varepsilon}{2}$, where $\varepsilon=\varepsilon_\Delta$. For $i\geq 0$, select $k_{i+1}$ to be congruent to $-k_i-\varepsilon$ modulo $|a_i|$, with $k_{i+1}>w$ as small as possible if $a_i$ is positive, and $k_{i+1}<w$ as large as possible if $a_i$ is negative, and let*

$$a_{i+1}=-\frac{\phi(k_{i+1})}{a_i}. \tag{10.3.1}$$

*Then each $a_i$ is an integer dividing $\phi(k_i)$. Finally, let*

$$q_i=-\frac{k_i+k_{i+1}+\varepsilon}{a_i} \tag{10.3.2}$$

*for $i\geq 0$. Then $\langle q_0,q_1,q_2,\dots\rangle$ is the continued fraction of $v$.*

Note that $f(x)$ is the minimum polynomial of $v$ if $r$ is positive, and is the negative of that minimum polynomial if $r$ is negative. We will prove Theorem 10.3.1 at the end of this section, after several examples to illustrate its application. In practice, this algorithm terminates when we find values $0\leq m<n$ for which $a_m=a_n$ and $k_m=k_n$, in which case the continued fraction of $v$ has the form

$$v=\langle q_0,q_1,\dots,q_{m-1},\overline{q_m,q_{m+1},\dots,q_{n-1}}\rangle.$$

This must eventually occur, as the continued fraction of an irrational quadratic number is periodic.

When $v = \sqrt{d}$, the algorithm of Theorem 10.3.1 is essentially the same as that of Theorem 9.2.2, but our first example illustrates that there may be a change in the data that we compile in this case.

**Example.** Let $v = \sqrt{29} = 0 + 1 \cdot \sqrt{29}$, so that $ax^2 + bx + c = x^2 - 29$. The discriminant of $v$ is $\Delta = 116 = \Delta(29, 2)$, hence $\phi(x) = x^2 + 2x - 28$ is the principal polynomial of discriminant $\Delta$. The roots of $\phi(x)$ are $w = \frac{-2-\sqrt{116}}{2} = -1-\sqrt{29} \approx -6.4$ and $\overline{w} = \frac{-2+\sqrt{116}}{2} = -1+\sqrt{29} \approx 4.4$. To apply Theorem 10.3.1, it is helpful to calculate $\phi(x)$ for $w < x < \overline{w}$ as in the following table, here using the fact that $\phi(x) = \phi(-x - \varepsilon)$.

| $x$ | $-6,4$ | $-5,3$ | $-4,2$ | $-3,1$ | $-2,0$ | $-1$ |
|---|---|---|---|---|---|---|
| $\phi(x)$ | $-4$ | $-13$ | $-20$ | $-25$ | $-28$ | $-29$ |

We begin the algorithm with $a_0 = a = 1$ and $k_0 = \frac{b-\varepsilon}{2} = -1$. We then compute that $k_1 = -6$, the smallest integer larger than $w$ for which $k_1 \equiv -k_0 - \varepsilon \equiv -1 \pmod 1$, so that $a_1 = -\frac{\phi(-6)}{1} = 4$. Now we need $k_2$ congruent to $-k_1 - \varepsilon = 4$ modulo 4, and find that the smallest possibility larger than $w$ is $k_2 = -4$. Thus $a_2 = -\frac{\phi(-4)}{4} = 5$. The following table continues these calculations.

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| $a$ | 1 | 4 | 5 | 5 | 4 | 1 | 4 |
| $k$ | $-1$ | $-6$ | $-4$ | $-3$ | $-4$ | $-6$ | $-6$ |
| $q$ | 5 | 2 | 1 | 1 | 2 | 10 | |

We find that $a_6 = a_1$ and $k_6 = k_1$, so can terminate the algorithm at that point. We can then calculate that $q_0 = -\frac{k_0+k_1+\varepsilon}{a_0} = -\frac{-1-6+2}{1} = 5$, and then $q_1 = -\frac{-6-4+2}{4} = 2$, and so forth. As in an example in §9.2, we find that $\sqrt{29} = \langle 5, \overline{2, 1, 1, 2, 10} \rangle$. (The numerator and denominator sequences of a continued fraction depend only on these $q_i$ values, so are unchanged from that previous calculation.) ◊

**Exercise 10.3.1.** Use Theorem 10.3.1 to find the continued fraction expansion of each of the following square roots.

(a) $v = \sqrt{41}$.

(b) $v = \sqrt{43}$.

(c) $v = \sqrt{53}$.

(d) $v = \sqrt{89}$.

(e) $\upsilon = \sqrt{97}$.

(f) $\upsilon = \sqrt{111}$.

**Example.** Let $\upsilon = \frac{5-2\sqrt{7}}{3}$, which has the conjugate $\overline{\upsilon} = \frac{5+2\sqrt{7}}{3}$. Since $\upsilon + \overline{\upsilon} = \frac{10}{3}$ and $\upsilon\overline{\upsilon} = \frac{-3}{9} = -\frac{1}{3}$, we find that $\upsilon$ has minimum polynomial $3x^2 - 10x - 1$. With the coefficient in $\upsilon$ of $\sqrt{7}$ negative or, equivalently, with $\upsilon < \overline{\upsilon}$, we let $ax^2 + bx + c = -3x^2 + 10x + 1$, the negative of this minimum polynomial. The discriminant of $\upsilon$ is $\Delta = 112 = \Delta(7, 2)$, and the principal polynomial of that discriminant is $\phi(x) = x^2 - 28$, so that $w = -\sqrt{28}$. We calculate the following values of $\phi(x)$.

| $x$ | $\pm5$ | $\pm4$ | $\pm3$ | $\pm2$ | $\pm1$ | $0$ |
|---|---|---|---|---|---|---|
| $\phi(x)$ | $-3$ | $-12$ | $-19$ | $-24$ | $-27$ | $-28$ |

With $a_0 = a = -3$ and $k_0 = \frac{b-\varepsilon}{2} = 5$, we select $k_1$ to be congruent to $-k_0 - \varepsilon = -5$ modulo 3 and as large as possible with $k_1 < w$ (since $a_0$ is negative). So $k_1 = -8$, from which we calculate that $a_1 = -\frac{\phi(k_1)}{a_0} = -\frac{36}{-3} = 12$. So now we want $k_2 \equiv 8 \pmod{12}$ and $k_2 > w$ as small as possible (since $a_1$ is positive). Thus $k_2 = -4$, and then $a_2 = -\frac{\phi(k_2)}{a_1} = -\frac{-12}{12} = 1$. The following table continues this process.

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| $a$ | $-3$ | 12 | 1 | 3 | 4 | 3 | 1 | 3 |
| $k$ | 5 | $-8$ | $-4$ | $-5$ | $-4$ | $-4$ | $-5$ | $-5$ |
| $q$ | $-1$ | 1 | 9 | 3 | 2 | 3 | 10 | |

Now $q_0 = -\frac{k_0+k_1+\varepsilon}{-3} = -\frac{-3}{-3} = -1$, and then $q_1 = -\frac{k_1+k_2+\varepsilon}{12} = -\frac{-12}{12} = 1$, and so forth. Here we find that $a_7 = a_3$ and $k_7 = k_3$, and conclude that $\frac{5-2\sqrt{7}}{3} = \left\langle -1, 1, 9, \overline{3, 2, 3, 10} \right\rangle$. ◊

**Exercise 10.3.2.** In each part, apply Theorem 10.3.1 to find the continued fraction expansion of $\upsilon$ and of its conjugate, $\overline{\upsilon}$.

(a) $\upsilon = 3 + \sqrt{23}$ and $\overline{\upsilon} = 3 - \sqrt{23}$.

(b) $\upsilon = \frac{3+\sqrt{17}}{5}$ and $\overline{\upsilon} = \frac{3-\sqrt{17}}{5}$.

(c) $\upsilon = \frac{-5+2\sqrt{13}}{3}$ and $\overline{\upsilon} = \frac{-5-2\sqrt{13}}{3}$.

(d) $\upsilon = 13 + 4\sqrt{11}$ and $\overline{\upsilon} = 13 - 4\sqrt{11}$.

**Example.** If $v = \frac{2+\sqrt{17}}{3}$, then $v$ is the larger root of $f(x) = 9x^2 - 12x - 13$, which has discriminant $\Delta = 612 = \Delta(17, 6)$. Here $\phi(x) = x^2 + 6x - 144$ is the principal polynomial of discriminant $\Delta$, with $w = -3 - 3\sqrt{17} \approx -15.4$ the smaller root of $\phi(x)$. In the following table, we list, in part, the values of $\phi(x)$ for $w < x < \overline{w}$. (In this case, $\phi(x) = \phi(-x - 6)$ for all $x$, so we pair those values.)

| $-x-6$ | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | $\cdots$ |
|---|---|---|---|---|---|---|---|---|---|---|
| $x$ | $-15$ | $-14$ | $-13$ | $-12$ | $-11$ | $-10$ | $-9$ | $-8$ | $-7$ | $\cdots$ |
| $\phi(x)$ | $-9$ | $-32$ | $-53$ | $-72$ | $-89$ | $-104$ | $-117$ | $-128$ | $-137$ | $\cdots$ |

We apply the quadratic continued fraction algorithm with $a_0 = a = 9$ and $k_0 = \frac{b-\varepsilon}{2} = \frac{-12-6}{2} = -9$. We select $k_1 \equiv 3 \pmod 9$ with $k_1 > w$ as small as possible, that is, $k_1 = -15$, so that $a_1 = -\frac{\phi(k_1)}{a_0} = -\frac{-9}{9} = 1$. Now $k_2 \equiv 9 \pmod 1$ with $k_2 > w$ as small as possible is $k_2 = -15$, and we find that $a_2 = -\frac{\phi(k_2)}{a_1} = -\frac{-9}{1} = 9$. Continuing these calculations, we find that $a_8 = a_0$ and $k_8 = k_0$, as in the following table.

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| $a$ | 9 | 1 | 9 | 13 | 8 | 9 | 8 | 13 | 9 |
| $k$ | $-9$ | $-15$ | $-15$ | $-9$ | $-10$ | $-12$ | $-12$ | $-10$ | $-9$ |
| $q$ | 2 | 24 | 2 | 1 | 2 | 2 | 2 | 1 | |

Here $q_0 = -\frac{k_0+k_1+\varepsilon}{a_0} = -\frac{-9-15+6}{9} = 2$, and $q_1 = -\frac{k_1+k_2+\varepsilon}{a_1} = -\frac{-15-15+6}{1} = 24$, and so forth. We conclude that $\frac{2+\sqrt{17}}{3} = \langle \overline{2, 24, 2, 1, 2, 2, 2, 1} \rangle$. ◊

**Exercise 10.3.3.** In each part, apply Theorem 10.3.1 to find the continued fraction expansion of $v$.

(a) $v = 1 + \sqrt{94}$.

(b) $v = \frac{5-\sqrt{114}}{3}$.

(c) $v = \frac{-4+\sqrt{65}}{2}$.

(d) $v = \frac{3+\sqrt{67}}{2}$.

(e) $v = \frac{4-\sqrt{83}}{7}$.

(f) $v = \frac{-7+\sqrt{113}}{4}$.

*Proof of Theorem* 10.3.1. Let $v = q + r\sqrt{d}$ be a root of $ax^2 + bx + c$, where $\gcd(a, b, c) = 1$ and the sign of $a$ is chosen to be the same as the sign of $r$. Let $\Delta = b^2 - 4ac$ and let $\phi(x) = x^2 + \varepsilon x + \frac{\varepsilon^2 - \Delta}{4}$ be the principal polynomial of discriminant $\Delta$. Define the sequences $a_i$, $k_i$, and $q_i$ as in the statement of Theorem 10.3.1. We first show by induction that $a_i$ is an integer and that $a_i$ divides $\phi(k_i)$ for every $i \geq 0$. For $i = 0$, we find that

$$\phi(k_0) = \phi\left(\frac{b - \varepsilon}{2}\right) = \frac{b^2 - 2\varepsilon b + \varepsilon^2 + 2\varepsilon b - 2\varepsilon^2 + \varepsilon^2 - \Delta}{4} = \frac{b^2 - \Delta}{4} = ac,$$

so that the integer $a_0 = a$ divides $\phi(k_0)$. Assume then that $a_i$ is an integer that divides $\phi(k_i)$ for some $i \geq 0$. Note that $q_i$ is also an integer, from the way in which $k_{i+1}$ is defined. Since $k_{i+1} = -a_i q_i - k_i - \varepsilon$ by equation (10.3.2), we find that

$$\phi(k_{i+1}) = k_{i+1}^2 + \varepsilon k_{i+1} + \frac{\varepsilon^2 - \Delta}{4} = a_i^2 q_i^2 + a_i q_i (2k_i + \varepsilon) + \phi(k_i). \tag{10.3.3}$$

If $a_i$ divides $\phi(k_i)$, then $a_i$ divides $\phi(k_{i+1})$, and so $a_{i+1} = -\frac{\phi(k_{i+1})}{a_i}$ is an integer. Furthermore, since $\phi(k_{i+1}) = -a_i a_{i+1}$, we have that $a_{i+1}$ divides $\phi(k_{i+1})$. This establishes our first claim by induction.

To show that this algorithm produces the continued fraction expansion of $v$, let $b_i = 2k_i + \varepsilon$ and let $v_i = \frac{-b_i + \sqrt{\Delta}}{2a_i}$ for all $i \geq 0$. Notice that $v_0 = v$, from the way in which the sign of $a_0 = a$ is selected. If we can show that $q_i = \lfloor v_i \rfloor$ and that $v_{i+1} = \frac{1}{v_i - q_i}$ for all $i \geq 0$, then $\langle q_0, q_1, q_2, \ldots \rangle$ is the continued fraction of $v$ by Theorem 9.4.2.

Let $w = \frac{-\varepsilon - \sqrt{\Delta}}{2}$ be the smaller root of $\phi(x)$. Note that as $k_{i+1}$ is defined, we have

$$w < -a_i q_i - k_i - \varepsilon < w + a_i \quad \text{or} \quad w + a_i < -a_i q_i - k_i - \varepsilon < w, \tag{10.3.4}$$

depending on whether $a_i$ is positive or negative. In either case, solving (10.3.4) for $q_i$, using the definition of $w$, we find that

$$\frac{-b_i + \sqrt{\Delta}}{2a_i} > q_i > \frac{-b_i + \sqrt{\Delta}}{2a_i} - 1, \quad \text{so that} \quad q_i = \left\lfloor \frac{-b_i + \sqrt{\Delta}}{2a_i} \right\rfloor = \lfloor v_i \rfloor.$$

Now with $-b_i - 2a_i q_i = -2a_i q_i - 2k_i - \varepsilon = 2k_{i+1} + \varepsilon = b_{i+1}$, using (10.3.2), we find that

$$v_i - q_i = \frac{(-b_i - 2a_i q_i) + \sqrt{\Delta}}{2a_i} = \frac{b_{i+1} + \sqrt{\Delta}}{2a_i}. \tag{10.3.5}$$

But then

$$\frac{1}{v_i - q_i} = \frac{2a_i}{b_{i+1} + \sqrt{\Delta}} \cdot \frac{-b_{i+1} + \sqrt{\Delta}}{-b_{i+1} + \sqrt{\Delta}} = \frac{2a_i(-b_{i+1} + \sqrt{\Delta})}{\Delta - b_{i+1}^2} = \frac{-b_{i+1} + \sqrt{\Delta}}{2a_{i+1}},$$

since

$$\Delta - b_{i+1}^2 = \Delta - (2k_{i+1} + \varepsilon)^2 = -4\phi(k_{i+1}) = 4a_i a_{i+1} \tag{10.3.6}$$

by (10.3.1). So $v_{i+1} = \frac{1}{v_i - q_i}$ for $i \geq 0$, which completes the proof. □

## 10.4 Equivalence of Indefinite Quadratic Forms

The algorithm of Theorem 10.3.1 constructs the continued fraction expansion of an arbitrary irrational quadratic number $v$. This procedure associates to $v$ a pair of integers $a_0$ and $k_0$, and recursively defines sequences $a_i$ and $k_i$ for $i > 0$, from which the terms $q_i$ of the continued fraction of $v$ are derived. If $\phi(x)$ is the principal polynomial whose discriminant equals that of $v$, then $a_i$ divides $\phi(k_i)$ for every $i \geq 0$. Thus this algorithm also produces a sequence of quadratic forms $(a_i \,:\, k_i)$ from a given form. When we take this viewpoint, we will also refer to $\langle q_0, q_1, ...\rangle$ as the *continued fraction of the quadratic form* $(a \,:\, k) = (a_0 \,:\, k_0)$. We may also refer to the method of Theorem 10.3.1 as the *equivalence algorithm* applied to an arbitrary indefinite quadratic form. The following theorem justifies this terminology.

**Theorem 10.4.1.** *Let $\phi(x)$ be the principal polynomial and let $f = (a \,:\, k)$ be a quadratic form of some positive discriminant $\Delta$. Define the sequences $a_i$, $k_i$, and $q_i$ for $i \geq 0$ as in the quadratic continued fraction algorithm applied to $v = \frac{-b+\sqrt{\Delta}}{2a}$, where $b = \phi'(k)$. For $i \geq 0$, let*

$$U_i = \begin{bmatrix} q_i & -1 \\ 1 & 0 \end{bmatrix} \quad \textit{and} \quad \overline{U_i} = \begin{bmatrix} q_i & 1 \\ -1 & 0 \end{bmatrix}. \tag{10.4.1}$$

*Then $(a_i \,:\, k_i) \circ U_i = (-a_{i+1} \,:\, k_{i+1})$ and $(-a_i \,:\, k_i) \circ \overline{U_i} = (a_{i+1} \,:\, k_{i+1})$, so that*

$$(a_i \,:\, k_i) \sim (-a_{i+1} \,:\, k_{i+1}) \quad \textit{and} \quad (-a_i \,:\, k_i) \sim (a_{i+1} \,:\, k_{i+1})$$

*for all $i \geq 0$.*

We can also describe this theorem in terms of ideals of the quadratic domain $D_\Delta$, using Theorem 5.1.5. Since $[a \,:\, k] = [-a \,:\, k]$, Theorem 10.4.1 implies that $[a_i \,:\, k_i] \sim [a_{i+1} \,:\, k_{i+1}]$ for all $i \geq 0$.

*Proof.* For a given $i$, let $(a_i \,:\, k_i) = a_i x^2 + b_i xy + c_i y^2$, where $\phi(k_i) = a_i c_i$ and $\phi'(k_i) = b_i$. By equation (4.2.2), we have that $(a_i \,:\, k_i) \circ U_i = (m \,:\, \ell)$, where

$$m = a_i q_i^2 + b_i q_i + c_i \quad \text{and} \quad \ell = -a_i q_i - b_i + k_i = -a_i q_i - k_i - \varepsilon = k_{i+1}.$$

(We use equation (10.3.2) in the final expression for $\ell$.) But from equation (10.3.3), we find that

$$\phi(k_{i+1}) = a_i^2 q_i^2 + a_i q_i (2k_i + \varepsilon) + \phi(k_i) = a_i(a_i q_i^2 + b_i q_i + c_i),$$

so that $m = -a_{i+1}$, from the definition of $a_{i+1}$ in (10.3.1). Thus $(a_i : k_i) \circ U_i = (-a_{i+1} : k_{i+1})$. □

**Exercise 10.4.1.** Verify that $(-a_i : k_i) \circ \overline{U_i} = (a_{i+1} : k_{i+1})$ to complete the proof of Theorem 10.4.1.

We can go further with the connection between equivalence of quadratic forms and the corresponding continued fraction produced by this algorithm.

**Theorem 10.4.2.** *Let $f = (a : k)$ be a quadratic form of discriminant $\Delta > 0$. Define $a_i$, $k_i$, and $q_i$ as in the equivalence algorithm on $f$, let $f_i = ((-1)^i a_i : k_i)$, let $m_i$ and $n_i$ be the numerator and denominator of the $i$-th convergent of the continued fraction $\langle q_0, q_1, q_2, \ldots \rangle$, and let*

$$W_i = \begin{bmatrix} m_{i-1} & (-1)^i m_{i-2} \\ n_{i-1} & (-1)^i n_{i-2} \end{bmatrix}. \tag{10.4.2}$$

*Then $f \circ W_i = f_i$ for every $i \geq 0$.*

Notice that the determinant of $W_i$ is $(-1)^i(m_{i-1}n_{i-2} - m_{i-2}n_{i-1})$, which equals 1 as an application of Lemma 9.3.4. Thus $W_i$ is a unimodular matrix.

*Proof.* We proceed by induction on $i$. Note that $W_0$ is the identity matrix by the definition of $m_{-2}$, $m_{-1}$, $n_{-2}$, and $n_{-1}$ from §9.3. Thus $f \circ W_0 = f = f_0$. So now let $i$ be a fixed nonnegative integer, and suppose we have established that $f \circ W_i = f_i$. If $i$ is even, then $f_i \circ U_i = f_{i+1}$, while if $i$ is odd, then $f_i \circ \overline{U_i} = f_{i+1}$, where $U_i$ and $\overline{U_i}$ are as defined in (10.4.1). But if $i$ is even, then

$$\begin{aligned} W_i U_i &= \begin{bmatrix} m_{i-1} & m_{i-2} \\ n_{i-1} & n_{i-2} \end{bmatrix} \cdot \begin{bmatrix} q_i & -1 \\ 1 & 0 \end{bmatrix} \\ &= \begin{bmatrix} m_{i-1}q_i + m_{i-2} & -m_{i-1} \\ n_{i-1}q_i + n_{i-2} & -n_{i-1} \end{bmatrix} = \begin{bmatrix} m_i & -m_{i-1} \\ n_i & -n_{i-1} \end{bmatrix} = W_{i+1}, \end{aligned}$$

using the definition of convergents in equation (9.3.1), and we conclude that

$$f_{i+1} = f_i \circ U_i = (f \circ W_i) \circ U_i = f \circ (W_i U_i) = f \circ W_{i+1}.$$

Similarly, if $i$ is odd, then $W_i \overline{U_i} = W_{i+1}$. The proof follows by induction. □

**Exercise 10.4.2.** Verify that $W_i \overline{U_i} = W_{i+1}$ if $i$ is odd to complete the proof of Theorem 10.4.2.

**Example.** In §10.3, we calculated the continued fraction of $\upsilon = \frac{2+\sqrt{17}}{3}$, a quadratic number of discriminant $\Delta = 612$. A table with the main data from the

quadratic continued fraction algorithm is repeated below, with additional rows for the numerator and denominator sequences.

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| $a$ | 9 | 1 | 9 | 13 | 8 | 9 | 8 | 13 | 9 |
| $k$ | $-9$ | $-15$ | $-15$ | $-9$ | $-10$ | $-12$ | $-12$ | $-10$ | $-9$ |
| $q$ | 2 | 24 | 2 | 1 | 2 | 2 | 2 | 1 | |
| $m$ | 2 | 49 | 100 | 149 | 398 | 945 | 2288 | 3233 | |
| $n$ | 1 | 24 | 49 | 73 | 195 | 463 | 1121 | 1584 | |

These calculations also arise from the equivalence algorithm on $f = (9 : -9) = 9x^2 - 12xy - 13y^2$, a quadratic form of discriminant $\Delta = 612$. Here we conclude by Theorem 10.4.1 that

$$(9 : -9) \sim (-1 : -15) \sim (9 : -15) \sim (-13 : -9)$$
$$\sim (8 : -10) \sim (-9 : -12) \sim (8 : -12) \sim (-13 : -10)$$

and

$$(-9 : -9) \sim (1 : -15) \sim (-9 : -15) \sim (13 : -9)$$
$$\sim (-8 : -10) \sim (9 : -12) \sim (-8 : -12) \sim (13 : -10).$$

As an example of the calculation in Theorem 10.4.2, we have that $W_3 = \begin{bmatrix} 100 & -49 \\ 49 & -24 \end{bmatrix}$ is a unimodular matrix for which $f \circ W_3 = f_3 = (-13 : -9)$, as can be verified by Proposition 4.2.1, among other methods. ♢

**Exercise 10.4.3.** For $i \geq 0$, let $U_i$ and $\overline{U_i}$ be defined as in (10.4.1), and let $W_i$ be given as in (10.4.2) for some continued fraction $\langle q_0, q_1, q_2, ... \rangle$. Use the proof of Theorem 10.4.2 to show that $W_t = U_0 \cdot \overline{U_1} \cdot U_2 \cdot \overline{U_3} \cdots U_{t-1}$ if $t$ is odd, and $W_t = U_0 \cdot \overline{U_1} \cdot U_2 \cdot \overline{U_3} \cdots \overline{U_{t-1}}$ if $t$ is even.

We now prove Theorem 10.1.2, the equivalence algorithm on candidate forms of positive discriminant, as a special case of the quadratic continued fraction algorithm, assuming one claim that we will establish as part of Theorem 11.1.1.

*Proof of Theorem* 10.1.2. Let $\phi(x) = x^2 + \varepsilon x + \frac{\varepsilon^2 - \Delta}{4}$ be the principal polynomial of some positive discriminant $\Delta$, and let $w = \frac{-\varepsilon - \sqrt{\Delta}}{2a}$, the smaller root of $\phi(x)$. Let $a$ be an integer with $0 < a < \frac{\sqrt{\Delta}}{2}$ and let $k$ be an integer with $w < k < w + a$. If $b = \phi'(k)$ and $v = \frac{-b + \sqrt{\Delta}}{2a}$, then we see that the equivalence algorithm on $(a : k)$ is the same as the quadratic continued fraction algorithm on $v$. The claim that $(a_i : k_i) \sim (-a_{i+1} : k_{i+1})$ and $(-a_i : k_i) \sim (a_{i+1} : k_{i+1})$ for all $i \geq 0$ immediately follows by Theorem 10.4.1.

Note that $w < k < w + a$ implies that $-\sqrt{\Delta} < b < -\sqrt{\Delta} + 2a$. We can rearrange these inequalities as $-2a < -b - \sqrt{\Delta} < 0$, and since $a$ is positive, then $-1 < \frac{-b-\sqrt{\Delta}}{2a} < 0$. Furthermore, if $a < \frac{\sqrt{\Delta}}{2}$, then $k < w + a < -\frac{\varepsilon}{2}$, from which it follows that $b$ is negative. But then $\upsilon = \frac{-b+\sqrt{\Delta}}{2a} > \frac{\sqrt{\Delta}}{2a} > 1$, again using the fact that $a < \frac{\sqrt{\Delta}}{2}$. Hence $\upsilon > 1$ and $-1 < \overline{\upsilon} < 0$, and so $\upsilon$ is a reduced quadratic number, in the terminology introduced in §9.5. The continued fraction of $\upsilon$ is thus purely periodic, and we can be sure that there is a smallest even positive integer $m$ for which $a_m = a$ and $k_m = k$, as claimed in Theorem 10.1.2.

Finally, let $a'$ and $k'$ be integers for which $a'$ divides $\phi(k')$, with $|a'| < \frac{\sqrt{\Delta}}{2}$ and $w < k' < w + |a'|$, and suppose that $f = (a : k) \sim (a' : k')$. Then $f$ represents $a'$, that is, $f(q, r) = a'$ for some integers $q$ and $r$. Since $|a'| < \frac{\sqrt{\Delta}}{2}$, we will see in Theorem 11.1.1 that $q$ and $r$ are the numerator and denominator of some convergent in the continued fraction of $\upsilon$ defined above, say $q = m_{i-1}$ and $r = n_{i-1}$ for some $i$. But now Theorem 10.4.2 shows that $a' = (-1)^i a_i$. We find that $\phi(k_i) < 0$ for all $i$, so that each $a_i$ is positive, and so we conclude that $a' = a_i$ for some *even* value of $i$, or $a' = -a_i$ for some *odd* value of $i$. We can assume that $0 < i \leq m$ because of the periodicity of the $a_i$ sequence.

So now there is a unimodular matrix $U$ with first column $\begin{bmatrix} q \\ r \end{bmatrix} = \begin{bmatrix} m_{i-1} \\ n_{i-1} \end{bmatrix}$ so that $f \circ U = (a' : k') = ((-1)^i a_i : k')$. But again by Theorem 10.4.2, we know that there is such a matrix $W_i$ for which $f \circ W_i = ((-1)^i a_i : k_i)$. By Proposition 4.2.4, then $k'$ and $k_i$ must be congruent modulo $a_i$. But with $w < k' < w + |a'|$, and with $w < k_i < w + a_i$ by the definition of the $k_i$ sequence, we conclude that $k'$ must equal $k_i$. □

## Class Groups of Positive Discriminant—Review

Our main goal for this chapter was to develop a method of constructing the class groups of ideals and quadratic domains of a fixed positive discriminant, as we did for an arbitrary negative discriminant in Chapter 6. Although there is no precise description of class representatives analogous to reduced quadratic forms of negative discriminant, we found in this chapter that we can determine these representatives in a systematic way using an algorithm connected to continued fractions. (We summarize our results below using the terminology of quadratic forms—we can make corresponding statements about ideals of positive discriminant.)

(1) Every quadratic form of positive discriminant $\Delta$ is equivalent to a form $(a : k)$ with $|a| < \sqrt{\Delta/4}$. Thus, using the principal polynomial $\phi(x)$ of discriminant $\Delta$, we can compile a list of all potential class representatives. There is

an algorithm (Theorem 10.1.2) to determine all other equivalences among these candidate forms. By this method, we obtain a complete description of the class group of quadratic forms of an arbitrary positive discriminant.

(2) Genus equivalence allows us to further describe the structure of these class groups in practice. In particular, we have a formula for the number of distinct genera of quadratic forms in terms of the prime factorization of $\Delta$. (This formula is slightly different for ideals of $D_\Delta$. See Theorem 10.2.1 for details.)

(3) We introduced a revised algorithm for constructing the continued fraction expansion of an arbitrary irrational quadratic number $v$ (Theorem 10.3.1). If $v$ has discriminant $\Delta$, this procedure produces a sequence of $a_i$ and $k_i$ pairs, eventually repeating some pattern, for which $a_i$ divides $\phi_\Delta(k_i)$. Thus the algorithm produces an infinite but repeating list of quadratic forms of a particular positive discriminant $\Delta$. We refer to this process as the *equivalence algorithm* applied to a given quadratic form when viewed in this way. We also refer to the continued fraction of $v$ as the continued fraction of the corresponding quadratic form $(a : k) = (a_0 : k_0)$.

(4) When $(a_0 : k_0), (a_1 : k_1), \ldots$ is a sequence of quadratic forms obtained by the equivalence algorithm, then

$$(a_0 : k_0) \sim (-a_1 : k_1) \sim (a_2 : k_2) \sim (-a_3 : k_3) \sim \cdots$$

and

$$(-a_0 : k_0) \sim (a_1 : k_1) \sim (-a_2 : k_2) \sim (a_3 : k_3) \sim \cdots .$$

If the algorithm produces the continued fraction $\langle q_0, q_1, q_2, \ldots \rangle$ of some irrational quadratic number $v$, we can describe these equivalences specifically using the $q_i$ values (Theorem 10.4.1), or with the numerator and denominator sequences of the convergents of that continued fraction (Theorem 10.4.2).

Thus we can compute the class group of quadratic forms or of ideals of an arbitrary positive discriminant. In Chapter 11, we will apply these calculations to describe representations of integers by indefinite quadratic forms.

# 11

# Representations by Indefinite Forms

In Chapter 10, we introduced an algorithm for the continued fraction expansion of an arbitrary irrational quadratic number. We saw that this algorithm also constructs a sequence of equivalent quadratic forms of a positive discriminant $\Delta$, which we can use to describe the class groups of ideals and quadratic forms of that discriminant. We also refer to the continued fraction produced by this algorithm as the continued fraction of a particular quadratic form (the first form in that sequence). In Chapter 11, we justify this terminology. We will see in particular that the convergents of the continued fraction provide representations of integers by the indefinite quadratic form in question. In some cases, we can be sure that all such representations are expressed in this way. We state and prove our main result in §11.1, applying this theorem in the remaining sections of Chapter 11. In §11.2, we classify the automorphs of (class representatives of) indefinite quadratic forms, and the units in $D_\Delta$ when $\Delta$ is positive. In §11.3 and §11.4, we describe the existence of representations of integers by quadratic forms of positive discriminant, and illustrate methods of constructing those solutions in practice.

## 11.1 The Continued Fraction of a Quadratic Form

Our main result for this chapter is a connection between representations of integers by a quadratic form of positive discriminant and the continued fraction of a particular quadratic number defined from that form. It will be convenient to combine several statements into the following theorem.

**Theorem 11.1.1.** *Let $f(x,y) = ax^2+bxy+cy^2$ be a primitive quadratic form with positive discriminant $\Delta = b^2-4ac$, not a square, and with $a > 0$. Write $f = (a : k)$ in ideal notation, and for each $i \geq 0$, let $a_i$, $k_i$, and $q_i$ be defined as in the equivalence algorithm applied to $(a : k)$ (that is, the quadratic continued fraction algorithm applied to $\upsilon = \frac{-b+\sqrt{\Delta}}{2a}$). Let $\ell$ be the period length of the continued fraction $\upsilon = \langle q_0, q_1, \ldots \rangle$, let $m_i$ and $n_i$ be the numerator and denominator in the i-th convergent of $\upsilon$, and let $w_i = m_{i-1} - n_{i-1}\upsilon$ for $i \geq 0$. Then the following statements are true.*

(1) *For all $i \geq 0$, $f(m_{i-1}, n_{i-1}) = (-1)^i a_i$.*

(2) *If $c < 0$, and $f(q,r) = d$ with $q$ and $r$ positive, $\gcd(q,r) = 1$, and $|d| < \sqrt{\Delta/4}$, then $q = m_i$ and $r = n_i$ for some $i \geq 0$.*

(3) *If $\upsilon$ is semi-reduced, then $w_i \cdot w_\ell = w_{\ell+i}$ for all $i \geq 0$.*

(4) *If $\upsilon$ is palindromic, then $a \cdot w_i \cdot w_{\ell-i} = a_i \cdot w_\ell$ for $0 \leq i \leq \ell$.*

(5) *If $\upsilon$ is palindromic, then $a_i = a$ if $\ell$ divides $i$. If $a = 1$, then $a_i = 1$ only if $\ell$ divides $i$.*

The following example illustrates some implications of Theorem 11.1.1.

**Example.** Let $f(x,y) = x^2 - 19y^2$, so that $\Delta = 76$ and $\upsilon = \frac{\sqrt{76}}{2} = \sqrt{19}$. We calculated the continued fraction of $\upsilon$ by direct means in §9.1. We leave it to the reader to verify that the following data are obtained from the quadratic continued fraction algorithm of Theorem 10.3.1, together with calculation of the numerator and denominator sequences of convergents, as in equation (9.3.1).

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| $a$ | 1 | 3 | 5 | 2 | 5 | 3 | 1 | 3 |
| $k$ | 0 | $-4$ | $-2$ | $-3$ | $-3$ | $-2$ | $-4$ | $-4$ |
| $q$ | 4 | 2 | 1 | 3 | 1 | 2 | 8 | |
| $m$ | 4 | 9 | 13 | 48 | 61 | 170 | 1421 | |
| $n$ | 1 | 2 | 3 | 11 | 14 | 39 | 326 | |

Since $a_7 = a_1$ and $k_7 = k_1$, we have that $\sqrt{19} = \langle 4, \overline{2,1,3,1,2,8} \rangle$, with period length $\ell = 6$. We noted in §9.6 that $\sqrt{d}$ is semi-regular and palindromic when $d > 0$ is not a square. (Notice that the repeating pattern in the continued fraction of $\sqrt{19}$, aside from the final term, forms a palindrome, as claimed in Proposition 9.6.7.) So all statements of Theorem 11.1.1 are true for this continued fraction.

(1) We can verify that $f(4,1) = -3$, $f(9,2) = 5$, $f(13,3) = -2$, and so forth, confirming statement (1) for small values of $i$. Notice that, because of the repetition of the $a$ row, the only values that we can obtain when $f$ is applied to a numerator and denominator pair are 1, $-3$, 5, and $-2$.

(2) The claim of statement (2) is that for $|d| \le \left\lfloor \sqrt{76/4} \right\rfloor = 4$, the *only* solutions of $x^2 - 19y^2 = d$ in relatively prime positive integers can occur as a numerator/denominator pair, $(x, y) = (m_i, n_i)$ for some $i$. Since $f(x, y) = f(\pm x, \pm y)$ in this case, we can then rule out any proper solutions of $x^2 - 19y^2 = 2$ or $x^2 - 19y^2 = 3$, for example.

(3) For $i > 6$, we can calculate $w_i$ (and so the terms $m_{i-1}$ and $n_{i-1}$) by multiplication rather than by the continued fraction algorithm. For instance,

$$w_7 = w_1 \cdot w_6 = (4 - \sqrt{19})(170 - 39\sqrt{19}) = 1421 - 326\sqrt{19},$$

as is confirmed by the values of $m_6$ and $n_6$ in the table.

(4) Statement (4) can be verified from the table—for example,

$$w_2 w_4 = (9 - 2\sqrt{19})(48 - 11\sqrt{19}) = 850 - 195\sqrt{19} = 5w_6.$$

(5) Statement (1) implies that $w_6 = 170 - 39\sqrt{19}$ is a solution of the equation $x^2 - 19y^2 = 1$. Statements (2), (3), and (5) combine to show that all positive integer solutions of $x^2 - 19y^2 = 1$ arise from powers of $w_6$. ◊

As illustrated in this example, if $f(x, y) = x^2 - dy^2$ for some positive integer $d$, not a square, then Theorem 11.1.1 implies that all solutions of Pell's equation, $x^2 - dy^2 = 1$, are obtained from the numerator and denominator sequences, $m_i$ and $n_i$, of the convergents in the continued fraction of $\sqrt{d}$. Specifically, if $\ell$ is the period length of that continued fraction, and $t = \operatorname{lcm}(\ell, 2)$, then $(x, y) = (m_{t-1}, n_{t-1})$ is the fundamental solution of Pell's equation, from which all other solutions can be constructed.

**Proofs of the Results.** The proof of our main theorem is rather long, and requires several technical lemmas. We establish each part separately in the remainder of this section. We will write each quadratic form $(a_i : k_i)$ as $a_i x^2 + b_i xy + c_i y^2$, and let

$$v_i = \frac{-b_i + \sqrt{\Delta}}{2a_i} \tag{11.1.1}$$

for $i \ge 0$. In the proof of Theorem 10.3.1, it is established that $v_0 = v$ and $v_{i+1} = \frac{1}{v_i - q_i}$ for $i \ge 0$.

**Lemma 11.1.2.** *Let $f(x) = ax^2 + bx + c$ be a quadratic polynomial with discriminant $\Delta = b^2 - 4ac$ not a square, having roots $v = \frac{-b+\sqrt{\Delta}}{2a}$ and $\overline{v} = \frac{-b-\sqrt{\Delta}}{2a}$. Let $q$ be an integer, and let $a_1 = -f(q)$ and $b_1 = -f'(q)$. Then the following equations are true.*

$$v - q = \frac{b_1 + \sqrt{\Delta}}{2a}, \quad \frac{1}{v - q} = \frac{-b_1 + \sqrt{\Delta}}{2a_1}, \quad (v - q)(\overline{v} - q) = -\frac{a_1}{a}. \tag{11.1.2}$$

*Proof.* We immediately have that $v - q = \frac{(-b-2aq)+\sqrt{\Delta}}{2a} = \frac{b_1+\sqrt{\Delta}}{2a}$, so that

$$\frac{1}{v-q} = \frac{2a}{b_1+\sqrt{\Delta}} \cdot \frac{b_1-\sqrt{\Delta}}{b_1-\sqrt{\Delta}} = \frac{2a(b_1-\sqrt{\Delta})}{b_1^2-\Delta}. \tag{11.1.3}$$

But

$$b_1^2 - \Delta = (-b-2aq)^2 - (b^2-4ac) = 4a(aq^2+bq+c) = -4aa_1, \tag{11.1.4}$$

so equation (11.1.3) simplifies to the second equation in (11.1.2). Finally

$$(v-q)(\overline{v}-q) = \frac{b_1+\sqrt{\Delta}}{2a} \cdot \frac{b_1-\sqrt{\Delta}}{2a} = \frac{b_1^2-\Delta}{4a^2} = \frac{-4aa_1}{4a^2} = -\frac{a_1}{a},$$

using equation (11.1.4). □

**Lemma 11.1.3.** *Let $f(x,y) = ax^2+bxy+cy^2$ be a quadratic form with discriminant $\Delta = b^2-4ac$ and let $v = \frac{-b+\sqrt{\Delta}}{2a}$ and $\overline{v} = \frac{-b-\sqrt{\Delta}}{2a}$. Let $w = q - rv$ for some integers $q$ and $r$, so that the norm of $w$ is $N(w) = (q-rv)(q-r\overline{v})$. Then $a \cdot N(w) = f(q,r)$.*

*Proof.* We find that

$$a(q-rv)(q-r\overline{v}) = a(q^2 - qr(v+\overline{v}) + r^2(v\overline{v})) = aq^2+bqr+cr^2$$

since $v+\overline{v} = -\frac{b}{a}$ and $v\overline{v} = \frac{b^2-\Delta}{4a^2} = \frac{4ac}{4a^2} = \frac{c}{a}$. □

*Proof of Theorem* 11.1.1*, part* (1). Let $\langle q_0, q_1, q_2, \ldots\rangle$ be the continued fraction of $v$, and define $v_i$ as in equation (11.1.1). For $i \geq 1$, we can write

$$v = \langle q_0, q_1, \ldots, q_{i-1}, v_i\rangle$$

by Lemma 9.4.1, which implies by Lemma 9.3.2 that

$$v = \frac{m_{i-1}\cdot v_i + m_{i-2}}{n_{i-1}\cdot v_i + n_{i-2}}, \quad \text{and so} \quad v_i = \frac{n_{i-2}v - m_{i-2}}{m_{i-1} - n_{i-1}v} = -\frac{w_{i-1}}{w_i} \tag{11.1.5}$$

for all $i \geq 1$, using the definition of $w_i$ in the statement of Theorem 11.1.1. We can then show by induction on $i$ that

$$w_i = \prod_{j=1}^{i}(q_{j-1} - v_{j-1}).$$

The claim holds for $i = 1$, since $w_1 = m_0 - n_0 v = q_0 - v_0$. (When $i = 1$, the product contains just one term.) Now suppose that $w_i = \prod_{j=1}^{i}(q_{j-1}-v_{j-1})$ for some $i \geq 1$. Then

$$\prod_{j=1}^{i+1}(q_{j-1}-v_{j-1}) = (q_i - v_i)\cdot\prod_{j=1}^{i}(q_{j-1}-v_{j-1}) = \left(q_i + \frac{w_{i-1}}{w_i}\right)\cdot w_i = q_i w_i + w_{i-1},$$

using equation (11.1.5) and the inductive hypothesis. But

$$q_i w_i + w_{i-1} = (q_i m_{i-1} + m_{i-2}) - (q_i n_{i-1} + n_{i-2})\upsilon = m_i - n_i \upsilon = w_{i+1}, \quad (11.1.6)$$

by the definition of the numerator and denominator sequences.

Applying Lemma 11.1.2, we find that

$$(\upsilon_i - q_i)(\overline{\upsilon}_i - q_i) = (q_i - \upsilon_i)(q_i - \overline{\upsilon}_i) = -\frac{a_{i+1}}{a_i}$$

for all $i \geq 0$. Then

$$N(w_i) = \prod_{j=1}^{i} \left[(q_{j-1} - \upsilon_{j-1})(q_{j-1} - \overline{\upsilon}_{j-1})\right]$$
$$= -\frac{a_1}{a_0} \cdot -\frac{a_2}{a_1} \cdot -\frac{a_3}{a_2} \cdots - \frac{a_i}{a_{i-1}} = (-1)^i \frac{a_i}{a}, \quad (11.1.7)$$

because (aside from the $i$ terms of $-1$) every term cancels except the denominator of the first quotient, which is $a_0 = a$, and the numerator of the last. But finally, then

$$f(m_{i-1}, n_{i-1}) = a \cdot N(m_{i-1} - n_{i-1}\upsilon) = a \cdot N(w_i) = a \cdot (-1)^i \cdot \frac{a_i}{a} = (-1)^i a_i,$$

by Lemma 11.1.3 and the equation (11.1.7). □

Thus the convergents in the continued fraction of $\upsilon$ provide solutions of $f(x, y) = d$ for some values of $d$. Part (2) of Theorem 11.1.1 implies that, under certain circumstances, all solutions of $f(x, y) = d$ are found in this way when $d$ is sufficiently small in absolute value. Before we prove this statement, we first establish the following general property of continued fractions.

**Lemma 11.1.4.** *Let $\upsilon$ be an irrational number, and suppose that $q$ and $r$ are relatively prime integers, with $r$ positive, for which $\left|\frac{q}{r} - \upsilon\right| < \frac{1}{2r^2}$. Then $\frac{q}{r}$ is a convergent in the continued fraction of $\upsilon$.*

*Proof.* Write $\frac{q}{r} - \upsilon$ as $\frac{\epsilon\theta}{r^2}$, where $\epsilon = \pm 1$ and $0 < \theta < \frac{1}{2}$. Recall from part (2) of Theorem 9.4.4 that a rational number can be expressed in two ways as a finite simple continued fraction, with an odd number of terms in one case and an even number in the other. Thus we can write $\frac{q}{r} = \langle q_0, q_1, \ldots, q_k \rangle$ with $k$ selected so that $\epsilon = (-1)^{k-1}$. Let $m_i$ and $n_i$ be the numerator and denominator of the $i$-th convergent in this continued fraction. Notice that $\frac{m_k}{n_k} = \langle q_0, q_1, \ldots, q_k \rangle$ also, and since $\gcd(q, r) = 1$ with $r > 0$, then $q = m_k$ and $r = n_k$. Now $m_{k-1}n_k - m_k n_{k-1} = (-1)^k$ by Lemma 9.3.4, so if we let $s = m_{k-1}$ and $t = n_{k-1}$, then $qt - rs = \epsilon$.

Now let $w = \frac{-tv+s}{rv-q}$, a real number since $v$ is irrational, and so cannot equal $\frac{q}{r}$. Then we find that $v = \frac{qw+s}{rw+t}$, so that

$$\frac{\epsilon\theta}{r^2} = \frac{q}{r} - v = \frac{q}{r} - \frac{qw+s}{rw+t} = \frac{qrw + qt - rqw - rs}{r(rw+t)} = \frac{\epsilon}{r(rw+t)},$$

which implies that $\theta = \frac{r}{rw+t}$. Since $0 < \theta < \frac{1}{2}$, then $\frac{rw+t}{r} = w + \frac{t}{r} > 2$. But since $t = n_{k-1}$ and $r = n_k$ with $k \geq 0$, we see that $0 \leq t \leq r$. Thus $\frac{t}{r} \leq 1$ and so $w > 1$. Now notice that

$$v = \frac{m_k \cdot w + m_{k-1}}{n_k \cdot w + n_{k-1}} = \langle q_0, q_1, \dots, q_k, w \rangle .$$

If $w = \langle q_0', q_1', \dots \rangle$, then $v = \langle q_0, q_1, \dots, q_k, q_0', q_1', \dots \rangle$ is a well-defined continued fraction, since $w > 1$ and so $q_0' > 0$. This must be the unique continued fraction of $v$, and then $\frac{q}{r} = \frac{m_k}{n_k}$ is a convergent for this expansion. □

**Exercise 11.1.1.** For each positive integer $r \leq 20$, find the value of $q$ so that $\frac{q}{r}$ is as close as possible to $\sqrt{2}$. Identify those values of $q$ and $r$ for which $|\frac{q}{r} - \sqrt{2}| < \frac{1}{2r^2}$. Verify that in those cases, $\frac{q}{r}$ is a convergent in the continued fraction expansion of $\sqrt{2}$.

**Exercise 11.1.2.** Repeat Exercise 11.1.1 with $\sqrt{3}$ in place of $\sqrt{2}$.

*Proof of Theorem* 11.1.1, *part* (2). Notice that $-\overline{v} = \frac{b+\sqrt{\Delta}}{2a}$ is positive under the assumption that $a > 0$ and $c < 0$, since in that case $\sqrt{\Delta} = \sqrt{b^2 - 4ac} > |b|$. Let $d = f(q, r)$ for some relatively prime positive integers $q$ and $r$, with $|d| < \sqrt{\Delta/4}$. Suppose first that $d > 0$. We have that $d = a(q - rv)(q - r\overline{v})$ by Lemma 11.1.3, and since $a$, $d$, $q$, $r$, and $-\overline{v}$ are all positive, then $q - rv > 0$ as well. It follows that $q - r\overline{v} > (q - r\overline{v}) - (q - rv) = r(v - \overline{v}) = r \cdot \frac{\sqrt{\Delta}}{a}$. Now we have

$$d = a(q - rv)(q - r\overline{v}) > (q - rv) \cdot r\sqrt{\Delta} \geq (q - rv) \cdot 2dr,$$

so that $\frac{1}{2r^2} > \frac{q}{r} - v$. By Lemma 11.1.4, then $\frac{q}{r}$ is a convergent in the continued fraction of $v$.

Now if $d < 0$, let $f_1(x, y) = -cx^2 - bxy - ay^2$, so that $f_1(r, q) = -d > 0$. The discriminant of $f_1$ is $\Delta$, with $-c > 0$ and $-a < 0$, and we find that $\frac{-(-b)+\sqrt{\Delta}}{2(-c)} = \frac{1}{v}$. By the same argument as above, we find that $\frac{r}{q}$ is a convergent in the continued fraction of $\frac{1}{v}$. By Exercise 9.4.6, this is the same as saying that $\frac{q}{r}$ is a convergent

of $\upsilon$. So in either case, $\frac{q}{r}$ must be the same as $\frac{m_i}{n_i}$ for some $i \geq 0$, and since $\gcd(q,r) = 1$, then $q = m_i$ and $r = n_i$. □

**Lemma 11.1.5.** *Let $f(x,y) = ax^2 + bxy + cy^2$ with $\Delta = b^2 - 4ac > 0$, and let $\upsilon = \frac{-b+\sqrt{\Delta}}{2a}$. Let $\upsilon$ be semi-reduced, so that $\upsilon = \langle q_0, \overline{q_1, q_2, \dots, q_{\ell-1}, q_\ell}\rangle$, with $q_\ell = q_0 + g$. If $m_i$ and $n_i$ are the numerator and denominator of the $i$-th convergent of $\sqrt{d}$, then*

$$a \cdot m_{\ell-2} = m_{\ell-1}(-ag) + n_{\ell-1}(-c) \tag{11.1.8}$$

*and*

$$a \cdot n_{\ell-2} = m_{\ell-1}(a) + n_{\ell-1}(b - ag). \tag{11.1.9}$$

*Proof.* Note that $f(\upsilon, 1) = a\upsilon^2 + b\upsilon + c = 0$. If $w = g + \upsilon$, then $w = \langle \overline{q_\ell, q_1, q_2, \dots, q_{\ell-1}}\rangle$, so that $\upsilon = \langle q_0, q_1, \dots, q_{\ell-1}, w\rangle$. By Lemma 9.3.2,

$$\upsilon = \frac{m_{\ell-1} \cdot w + m_{\ell-2}}{n_{\ell-1} \cdot w + n_{\ell-2}} = \frac{(m_{\ell-1}g + m_{\ell-2}) + m_{\ell-1}\upsilon}{(n_{\ell-1}g + n_{\ell-2}) + n_{\ell-1}\upsilon}.$$

Multiplying through by $a$ times the denominator of this last term, replacing $a\upsilon^2$ by $-b\upsilon - c$, and grouping factors, we find that

$$(an_{\ell-2} + n_{\ell-1}(ag - b) + m_{\ell-1}(-a)) \cdot \upsilon = am_{\ell-2} + m_{\ell-1}(ag) + n_{\ell-1}(c).$$

Since $\upsilon$ is irrational while all other terms in this equation are rational, then $am_{\ell-2} + m_{\ell-1}(ag) + n_{\ell-1}(c) = 0$ and $an_{\ell-2} + n_{\ell-1}(ag - b) - m_{\ell-1}a = 0$, which are the equations in (11.1.8) and (11.1.9) when solved for $am_{\ell-2}$ and $an_{\ell-2}$. □

*Proof of Theorem* 11.1.1, *part* (3). We use induction on $i$. When $i = 0$, then $w_0 = 1$, so that $w_0 \cdot w_\ell = w_\ell = w_{\ell+0}$. When $i = 1$, then $w_1 = m_0 - n_0\upsilon = q_0 - \upsilon$. So then $w_1 \cdot w_\ell = (q_0 - \upsilon)(m_{\ell-1} - n_{\ell-1}\upsilon)$, and we find that

$$a \cdot w_1 \cdot w_\ell = (m_{\ell-1}(aq_0) + n_{\ell-1}(-c)) - (m_{\ell-1}(a) + n_{\ell-1}(aq_0 + b)) \cdot \upsilon. \tag{11.1.10}$$

We know that $m_\ell = m_{\ell-1}q_\ell + m_{\ell-2}$ and $n_\ell = n_{\ell-1}q_\ell + n_{\ell-2}$. In this situation, we can use the fact that $q_\ell = q_0 + g$ together with (11.1.8) and (11.1.9) from Lemma 11.1.5 to see that

$$am_\ell = am_{\ell-1}(q_0 + g) + (m_{\ell-1}(-ag) + n_{\ell-1}(-c)) = m_{\ell-1}(aq_0) + n_{\ell-1}(-c)$$

and

$$an_\ell = an_{\ell-1}(q_0 + g) + (m_{\ell-1}(a) + n_{\ell-1}(b - ag)) = m_{\ell-1}(a) + n_{\ell-1}(aq_0 + b).$$

But then (11.1.10) implies that $a \cdot w_1 \cdot w_\ell = a(m_\ell - n_\ell\upsilon)$, so that $w_1 \cdot w_\ell = w_{\ell+1}$.

So now suppose that for some $i \geq 1$, we know that $w_i \cdot w_\ell = w_{\ell+i}$ and $w_{i-1} \cdot w_\ell = w_{\ell+i-1}$. Then by equation (11.1.6),

$$w_{i+1} \cdot w_\ell = (q_i w_i + w_{i-1}) \cdot w_\ell = q_i w_i \cdot w_\ell + w_{i-1} \cdot w_\ell = q_i w_{\ell+i} + w_{\ell+i-1}.$$

But since $i \geq 1$ and $\ell$ is the period of the continued fraction expansion of $\upsilon$, we know that $q_i = q_{\ell+i}$. So $w_{i+1} \cdot w_\ell = q_{\ell+i}w_{\ell+i} + w_{\ell+i-1} = w_{\ell+i+1}$, again using (11.1.6). The result follows by induction. □

**Lemma 11.1.6.** *Let $f(x,y) = ax^2+bxy+cy^2$ with $\Delta = b^2-4ac > 0$, and let $\upsilon = \frac{-b+\sqrt{\Delta}}{2a}$. Let $m_i$ and $n_i$ be the numerator and denominator of the $i$-th convergent of $\upsilon$. Suppose that $\upsilon$ is semi-reduced and palindromic, so that $\upsilon = \langle q_0, \overline{q_1, q_2, \ldots, q_{\ell-1}, q_\ell}\rangle$, with $q_\ell = q_0 + g$ for some integer $g$, and $q_i = q_{\ell-i}$ for $1 \leq i \leq \ell-1$. Then for $0 \leq i \leq \ell$,*

$$a \cdot m_{\ell-i-1} = (-1)^i\,(m_{\ell-1}(am_{i-1} + bn_{i-1}) + n_{\ell-1}(cn_{i-1})) \tag{11.1.11}$$

*and*

$$n_{\ell-i-1} = (-1)^i(m_{\ell-1}(-n_{i-1}) + n_{\ell-1}m_{i-1}). \tag{11.1.12}$$

*Proof.* In Exercise 9.6.8, we saw that if $\upsilon$ is palindromic, then $a$ divides $b$ and $g = q_0 + \frac{b}{a}$. When $i = 0$, equations (11.1.11) and (11.1.12) are true since $m_{-1} = 1$ and $n_{-1} = 0$. When $i = 1$, equations (11.1.11) and (11.1.12) reduce to $a \cdot m_{\ell-2} = -m_{\ell-1}(am_0 + bn_0) - n_{\ell-1}(cn_0)$ and $n_{\ell-2} = m_{\ell-1}n_0 - n_{\ell-1}m_0$, which are the equations of (11.1.8) and (11.1.9) established in Lemma 11.1.5, since $m_0 = q_0$, $n_0 = 1$, and $an = aq_0 + b$, as noted above.

So now suppose that equations (11.1.11) and (11.1.12) are true for $i = j$ and $i = j-1$, where $j$ is an integer with $1 \leq j < \ell$. We show that (11.1.11) must also be true for $i = j+1$, and thus that (11.1.11) holds for $0 \leq i \leq \ell$ by induction. Here $m_{\ell-(j+1)-1} = m_{\ell-j-2} = m_{\ell-j} - m_{\ell-j-1}q_{\ell-j}$, rewriting (9.3.1). Since $1 \leq j \leq \ell-1$, we know in this situation that $q_{\ell-j} = q_j$ by the symmetry in the continued fraction of $\upsilon$. Now by our inductive hypothesis,

$$\begin{aligned}
a \cdot m_{\ell-j-2} &= a \cdot m_{\ell-(j-1)-1} - a \cdot m_{\ell-j-1}q_j \\
&= (-1)^{j-1}\left(m_{\ell-1}(am_{j-2} + bn_{j-2}) + n_{\ell-1}(cn_{j-2})\right) \\
&\qquad - (-1)^j\left(m_{\ell-1}(am_{j-1} + bn_{j-1}) + n_{\ell-1}(cn_{j-1})\right)q_j \\
&= (-1)^{j+1}(m_{\ell-1}(a(m_{j-2} + m_{j-1}q_j) + b(n_{j-2} + n_{j-1}q_j)) \\
&\qquad + n_{\ell-1}c(n_{j-2} + n_{j-1}q_j)) \\
&= (-1)^{j+1}(m_{\ell-1}(am_j + bn_j) + n_{\ell-1}(cn_j)),
\end{aligned}$$

using (9.3.1) again. (We also use the fact that $(-1)^{j-1}$ and $-(-1)^j$ both equal $(-1)^{j+1}$.) But this is equation (11.1.11) with $j+1$ in place of $i$. The proof for equation (11.1.12) is similar, and is omitted. □

*Proof of Theorem* 11.1.1, *part* (4). Using the fact that $av^2 = -bv - c$, we have that

$$\begin{aligned} a \cdot w_i \cdot w_{\ell-i} &= a(m_{i-1} - n_{i-1}v)(m_{\ell-i-1} - n_{\ell-i-1}v) \\ &= (am_{i-1}m_{\ell-i-1} - cn_{i-1}n_{\ell-i-1}) \\ &\quad - (an_{i-1}m_{\ell-i-1} + (am_{i-1} + bn_{i-1})n_{\ell-i-1})v. \end{aligned}$$

We can substitute equations (11.1.11) and (11.1.12) here. We find that

$$\begin{aligned} &am_{i-1}m_{\ell-i-1} - cn_{i-1}n_{\ell-i-1} \\ &\quad = m_{i-1} \cdot (-1)^i (m_{\ell-1}(am_{i-1} + bn_{i-1}) + n_{\ell-1}(cn_{i-1})) \\ &\quad\quad - cn_{i-1} \cdot (-1)^i (m_{\ell-1}(-n_{i-1}) + n_{\ell-1}m_{i-1}) \\ &\quad\quad\quad = (-1)^i m_{\ell-1}(am_{i-1}^2 + bm_{i-1}n_{i-1} + cn_{i-1}^2), \end{aligned}$$

so that

$$am_{i-1}m_{\ell-i-1} - cn_{i-1}n_{\ell-i-1} = (-1)^i m_{\ell-1} \cdot f(m_{i-1}, n_{i-1}).$$

By a similar substitution and simplification,

$$an_{i-1}m_{\ell-i-1} + (am_{i-1} + bn_{i-1})n_{\ell-i-1} = (-1)^i n_{\ell-1} \cdot f(m_{i-1}, n_{i-1}).$$

But now

$$a \cdot w_i \cdot w_{\ell-i} = (-1)^i f(m_{i-1}, n_{i-1})(m_{\ell-1} - n_{\ell-1}v) = a_i \cdot w_\ell,$$

using part (1) of Theorem 11.1.1 and the definition of $w_\ell$. □

*Proof of Theorem* 11.1.1, *part* (5). When $i = \ell$, equation (11.1.11) simplifies to

$$am_{-1} = (-1)^\ell (am_{\ell-1}^2 + bm_{\ell-1}n_{\ell-1} + cn_{\ell-1}^2) = (-1)^\ell f(m_{\ell-1}, n_{\ell-1}).$$

Using part (1) of Theorem 11.1.1 and the fact that $m_{-1} = 1$, we conclude that $a = a_\ell$. Now part (3) of Theorem 11.1.1 implies that $N(w_i) \cdot N(w_\ell) = N(w_{\ell+i})$, or by multiplying both sides by $a^2$ and applying part (1) again, $(-1)^i a_i \cdot (-1)^\ell a_\ell = a(-1)^{\ell+i} a_{\ell+i}$. We conclude that $a_{\ell+i} = a_i$ for all $i \geq 0$. In particular, $a_\ell = a_{2\ell} = a_{3\ell} = \cdots = a$.

On the other hand, there is precisely one reduced irrational quadratic number with discriminant $\Delta$ of the form $\frac{u+\sqrt{\Delta}}{2}$. (Since $u$ must have the same parity as $\Delta$, the equation $-1 < \frac{u-\sqrt{\Delta}}{2} < 0$ leaves precisely one possibility for $u$.) If $a = 1$ and $a_i = 1$ for some $i$ with $0 < i \leq \ell$, we conclude that $v_i = v_\ell$, and thus $i = \ell$, since otherwise the period length of $v$ cannot be as large as $\ell$. □

## 11.2 Units and Automorphs

In the remainder of Chapter 11, we apply Theorem 11.1.1 to several questions about representations of integers by indefinite quadratic forms. Recall that an element $u$ in a quadratic domain $D = D_\Delta$ is called a *unit* if there is some $v$ in $D$ so that $uv = 1$. When $\Delta$ is negative, we listed the units of $D$ in full in Proposition 2.2.5. However, we saw that the set of units in $D$ might be infinite when $\Delta$ is positive.

**Exercise 11.2.1.** Let $D = D_\Delta$ be a quadratic domain with $\Delta$ positive. Show that if $D$ contains a unit $u$ not equal to $\pm 1$, then there is a smallest unit greater than 1 in $D$.

**Exercise 11.2.2.** Show that if $u$ is the smallest unit (greater than 1) of a quadratic domain $D = D_\Delta$ with $\Delta$ positive, then all units of $D$ are given by $\pm u^n$ with $n$ in $\mathbb{Z}$.

**Definition.** If $D = D_\Delta$ is a quadratic domain with $\Delta$ positive, and $D$ contains a unit other than $\pm 1$, then we refer to the smallest unit $u > 1$ of $D$ as the *fundamental unit* of $D$.

We will show that a quadratic domain of positive discriminant always contains a fundamental unit, and thus the set of all such units is infinite. Note that the fundamental solution of $x^2 - dy^2 = 1$ always gives us a unit in some quadratic domain, but not necessarily the fundamental unit, as the next example illustrates.

**Example.** In an example in §9.2, we found that $(x, y) = (9801, 1820)$ is the fundamental solution of $x^2 - 29y^2 = 1$. Thus $v = 9801 + 1820\sqrt{29}$ is a unit in $D = D_{29}$. But we also saw that $(x, y) = (70, 13)$ satisfies $x^2 - 29y^2 = -1$, and so $70 + 13\sqrt{29}$ is a smaller unit, with norm $-1$. Furthermore, the typical element of $D$ has the form $w = \frac{m+n\sqrt{29}}{2}$ with $m \equiv n \pmod 2$, so that $N(w) = \frac{m^2-29n^2}{4} = \pm 1$ if and only if $m^2 - 29n^2 = \pm 4$. We find that $u = \frac{5+\sqrt{29}}{2}$ (which equals $2 + z$, where $z = \frac{1+\sqrt{29}}{2}$ in $D$) is the fundamental unit in $D$, and can verify directly that $u^3 = 70 + 13\sqrt{29}$ and $u^6 = 9801 + 1820\sqrt{29}$. ◊

The following theorem is our main result on the fundamental unit in a domain $D_\Delta$ with $\Delta$ positive.

**Theorem 11.2.1.** *Let $\Delta$ be a positive discriminant value, with $z$ the basis element and $\varepsilon$ the basis index of discriminant $\Delta$, as in equation* (2.2.2). *Let $v = \frac{-\varepsilon+\sqrt{\Delta}}{2}$, let $\ell$ be the period length of the continued fraction of $v$, and let $m_i$ and $n_i$ be the numerator and denominator in the $i$-th convergent of this expansion. Then $u = m_{\ell-1} + n_{\ell-1}z$ is the fundamental unit of $D = D_\Delta$.*

*Proof.* Let $\phi(x,y) = x^2 + \varepsilon xy + \frac{\varepsilon^2-\Delta}{4}y^2$, so that $N(q+rz) = \phi(q,r)$ for all integers $q$ and $r$. All five parts of Theorem 11.1.1 apply to this quadratic form and the continued fraction expansion of $\upsilon = \frac{-\varepsilon+\sqrt{\Delta}}{2}$. In particular, parts (1) and (5) show that if $w_k = m_{k-1} - n_{k-1}\upsilon$, then $N(w_k) = \pm 1$ if and only if $\ell$ divides $k$, and part (2) shows that all solutions of $N(w) = \pm 1$ must have this form. But since $\upsilon = -\overline{z}$, we find that

$$N(m_{k-1} - n_{k-1}\upsilon) = N(m_{k-1} + n_{k-1}\overline{z}) = N(m_{k-1} + n_{k-1}z) = \phi(m_{k-1}, n_{k-1}).$$

In particular, $u = m_{\ell-1} + n_{\ell-1}z$ is the smallest element of $D$ larger than 1 for which $N(u) = \pm 1$. □

In practice, the information required to calculate the fundamental unit is obtained from the equivalence algorithm applied to $(1 : 0)$, the principal form of a given positive discriminant. We illustrate this approach in the following example.

**Example.** Let $\Delta = 61$ and $D = D_\Delta$. Every element of $D$ can be written uniquely as $w = q + rz$ for some $q$ and $r$ in $\mathbb{Z}$, where $z = \frac{1+\sqrt{61}}{2}$. In that case, $N(w) = q^2 + qr - 15r^2$, and $w$ is a unit in $D$ if and only if $N(w) = \pm 1$. If $\phi(x,y) = x^2 + xy - 15y^2$, then Theorem 11.1.1 implies that all such solutions must arise from the continued fraction of the semi-regular, palindromic number $\upsilon = \frac{-1+\sqrt{61}}{2}$. We obtain the following data from the quadratic continued fraction algorithm applied to $\upsilon$, and calculation of the numerator and denominator sequences of its convergents.

| $i$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| $a$ | 1 | 3 | 3 | 1 | 3 |
| $k$ | 0 | −4 | −3 | −4 | −4 |
| $q$ | 3 | 2 | 2 | 7 | |
| $m$ | 3 | 7 | 17 | | |
| $n$ | 1 | 2 | 5 | | |

By parts (1), (2), and (5) of Theorem 11.1.1, we can be sure that $(x,y) = (17,5)$ is the smallest positive solution of $x^2 + xy - 15y^2 = \pm 1$. Hence the fundamental unit of $D_{61}$ is $17 + 5z = \frac{39+5\sqrt{61}}{2}$. ♢

**Exercise 11.2.3.** Find the fundamental unit in the quadratic domain $D_\Delta$ for the given value of $\Delta$.

(a) $\Delta = 21$.

(b) $\Delta = 37$.

(c) $\Delta = 40$.

(d) $\Delta = 41$.

(e) $\Delta = 53$.

(f) $\Delta = 76$.

(g) $\Delta = 92$.

(h) $\Delta = 104$.

(i) $\Delta = 232$.

(j) $\Delta = 276$.

**Automorphs of Indefinite Quadratic Forms.** In §9.2, we used the fundamental solution of Pell's equation to find the automorphs of the quadratic form $x^2 - dy^2$ when $d$ is positive. For arbitrary quadratic forms of positive discriminant $\Delta$, it suffices to describe all automorphs of class representatives of $\mathcal{Q}_\Delta$, as we saw in Proposition 4.3.5. The following result accounts for every possibility.

**Theorem 11.2.2.** *Let $\phi(x)$ be the principal polynomial of some positive discriminant $\Delta$, and let $w$ be the smaller root of $\phi(x)$. Let $a$ and $k$ be integers for which $a$ divides $\phi(k)$, with $0 < a < \sqrt{\Delta/4}$ and $w < k < w + a$. Let $\ell$ be the period length, and let $m_i$ and $n_i$ be the numerator and denominator of the $i$-th convergent of the continued fraction of the quadratic form $(a : k)$. Then*

$$U = \begin{bmatrix} m_{t-1} & m_{t-2} \\ n_{t-1} & n_{t-2} \end{bmatrix} \quad \text{and} \quad \overline{U} = \begin{bmatrix} m_{t-1} & -m_{t-2} \\ -n_{t-1} & n_{t-2} \end{bmatrix} \tag{11.2.1}$$

*are automorphs of $f = (a : k)$ and $-\overline{f} = (-a : k)$, respectively, where $t = \operatorname{lcm}(\ell, 2)$. The group of automorphs of $f$ consists precisely of $\pm U^n$ for every integer $n$. Likewise, the group of automorphs of $-\overline{f}$ is made up of all $\pm\overline{U}^n$.*

*Proof.* We saw in the proof of Theorem 10.1.2 that, under the given conditions on $a$ and $k$, the continued fraction expansion of $(a : k)$ is purely periodic, say with period $\ell$. If $a_i$ and $k_i$ are defined for $i \geq 0$ as in the equivalence algorithm on $(a : k)$, then $a_\ell = a_0$ and $k_\ell = k_0$. But then Theorem 10.4.2 implies that

$$f \circ W_\ell = ((-1)^\ell a_\ell : k_\ell) = ((-1)^\ell a_0 : k_0),$$

where $W_\ell$ is defined as in (10.4.2). Note that if $t = \operatorname{lcm}(\ell, 2)$, then $W_t$ is the same as $U$ as defined in (11.2.1), and is an automorph of $f$. In general, if $(a : k) \circ W = (n : \ell)$, then $(-a : k) \circ \overline{W} = (-n : \ell)$, and so $\overline{U}$ is an automorph of $g$.

Since $t = \operatorname{lcm}(\ell, 2)$ is even, Exercise 10.4.3 shows that

$$U = U_0 \cdot \overline{U_1} \cdot U_2 \cdot \overline{U_3} \cdots U_{t-2} \cdot \overline{U_{t-1}} \quad \text{and} \quad \overline{U} = \overline{U_0} \cdot U_1 \cdot \overline{U_2} \cdot U_3 \cdots \overline{U_{t-2}} \cdot U_{t-1},$$

where $U_i$ and $\overline{U_i}$ are defined as in equation (10.4.1). But then since $U_i = U_{t+i}$ and $\overline{U_i} = \overline{U_{t+i}}$ for all $i$ by the periodicity of the continued fraction, we find that $U^2 = {W_t}^2 = W_{2t}$, and more generally $U^n = W_{nt}$ and $\overline{U}^n = \overline{W}_{nt}$ for all positive integers $n$. In Proposition 4.2.4, we saw that the first column of $W$ is sufficient to determine $f \circ W$ up to norm equivalence. It follows that the only automorphs of $f$ occur among the matrices $U^n$ for integers $n$, and their negatives. Similarly, the only automorphs of $g$ are $\overline{U}^n$ and their negatives. □

We illustrate a claim of this proof in the following example.

**Example.** Let $\Delta = 85$, so that $\phi(x) = x^2 + x - 21$, with smaller root $w = \frac{-1-\sqrt{85}}{2} \approx -5.11$. Among the quadratic forms $(a : k)$ with $0 < a < \sqrt{85/4}$ and $w < k < w + a$ is $f = (3 : -4) = 3x^2 - 7xy - 3y^2$. We compute the continued fraction of $f$ (that is, the continued fraction of $\upsilon = \frac{7+\sqrt{85}}{6}$), extending the following table beyond what is necessary to determine that expansion.

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| $a$ | 3 | 5 | 3 | 3 | 5 | 3 | 3 |
| $k$ | −4 | −3 | −3 | −4 | −3 | −3 | −4 |
| $q$ | 2 | 1 | 2 | 2 | 1 | 2 | |
| $m$ | 2 | 3 | 8 | 19 | 27 | 73 | |
| $n$ | 1 | 1 | 3 | 7 | 10 | 27 | |

Here $U = \begin{bmatrix} m_5 & m_4 \\ n_5 & n_4 \end{bmatrix} = \begin{bmatrix} 73 & 27 \\ 27 & 10 \end{bmatrix}$ is an automorph of $f$, since $\upsilon = \overline{\langle 2, 1, 2 \rangle}$ so that $t = \operatorname{lcm}(\ell, 2) = 6$. Note from the fact that $a_2 = 3$ that $f(x, y) = 3$ has a smaller solution in positive integers, namely $x = m_1 = 3$ and $y = n_1 = 1$. But there is no automorph of $f$ having first column entries 3 and 1. We find that if $V = \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix}$, then $f \circ V = (3 : -3)$ and any other unimodular matrix with the same first column produces a form that is norm equivalent to $(3 : -3)$. (We can also apply Proposition 4.3.4 in this case.) So $U$ is the simplest automorph of $f$ with positive entries, and the automorph group of $f$ consists of $\pm U^n$ for all integers $n$. ♢

**Example.** Let $\Delta = \Delta(30, 1) = 120$, so that $\phi(x) = x^2 - 30$. From the table

| $x$ | ±5 | ±4 | ±3 | ±2 | ±1 | 0 |
|---|---|---|---|---|---|---|
| $\phi(x)$ | −5 | −14 | −21 | −26 | −29 | −30 |

we find that $f = (2 : -4)$ satisfies the condition of Theorem 11.2.2. Applying the quadratic continued fraction algorithm to $a = 2$ and $k = -4$, we find that $\overline{\langle 4, 1, 2, 1 \rangle}$ is the continued fraction of $\upsilon = \frac{8+\sqrt{120}}{4}$, with convergents as in the

following table.

| $i$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| $a$ | 2 | 7 | 3 | 7 | 2 |
| $k$ | $-4$ | $-4$ | $-3$ | $-3$ | $-4$ |
| $q$ | 4 | 1 | 2 | 1 | |
| $m$ | 4 | 5 | 14 | 19 | |
| $n$ | 1 | 1 | 3 | 4 | |

So $U = \begin{bmatrix} 19 & 14 \\ 4 & 3 \end{bmatrix}$ and $\overline{U} = \begin{bmatrix} 19 & -14 \\ -4 & 3 \end{bmatrix}$ are automorphs of $f(x, y) = 2x^2 - 8xy - 7y^2$ and $g(x, y) = -2x^2 - 8xy + 7y^2$, respectively, as can be verified by direct calculation. ♢

**Exercise 11.2.4.** Find all automorphs of distinct class representatives of quadratic forms of the given discriminant $\Delta$. (These values of $\Delta$ appear in Exercise 10.2.1.)

(a) $\Delta = 37$.

(b) $\Delta = 40$.

(c) $\Delta = 61$.

(d) $\Delta = 92$.

(e) $\Delta = 93$.

(f) $\Delta = 105$.

## 11.3 Existence of Representations by Indefinite Forms

In Chapter 7, we used the structure of the ideal class group $\mathcal{C}_\Delta$, or the form class group $\mathcal{F}_\Delta$, of a negative discriminant $\Delta$ to describe the integers properly represented by positive definite quadratic forms of that discriminant. We often illustrated our conclusions with specific calculations, particularly using tables of forms $ax^2 + cy^2$ with $a$ and $c$ both positive. In the next two sections, we will likewise make general statements about representations by *indefinite* forms, using the group structure of $\mathcal{F}_\Delta$ when $\Delta$ is positive. We will find that we can often make precise descriptions of all integers properly represented by various quadratic forms of positive discriminant. However, it is more difficult to verify our claims numerically. As an example, while we can find all solutions of $2x^2+3y^2 = m$ for any given $m$ by testing finitely many values of $x$ and $y$, the equation $2x^2 - 3y^2 = m$ might have very large solutions $(x, y)$ for relatively small values of $m$. (For instance, $(x, y) = (1564, 1277)$ satisfies the equation $2x^2-3y^2 = 5$.) In this section, we will obtain statements about the *existence* of representations

of an integer $m$ by forms of a particular positive discriminant. We concentrate on specific examples that are typical of more general cases, and we leave many details of the calculations for the reader to confirm. We will consider the problem of constructing these representations in §11.4.

**Example.** Let $\Delta = \Delta(6,1) = 24$, so that $\phi(x) = x^2 - 6$ and $u_\Delta = \left\lfloor \sqrt{\Delta/4} \right\rfloor = 2$. We find by the methods of §10.1 that every quadratic form in $\mathcal{Q}_\Delta$ is equivalent to one of the following forms:

$$(1 : -2), \qquad (-1 : -2), \qquad (2 : -2), \qquad (-2 : -2).$$

But applying the equivalence algorithm of Theorem 10.1.2 to $(1 : -2)$ shows that $(1 : -2) \sim (-2 : -2)$, and so $(-1 : -2) \sim (2 : -2)$, hence there are two distinct classes of quadratic forms in $\mathcal{Q}_\Delta$. The genus symbols defined for a quadratic form $f$ of discriminant 24 are $\left(\frac{-2}{f}\right)$ and $\left(\frac{f}{3}\right)$, and we conclude that there are two genera of such forms, each containing a single class. Among other possible class representatives (including those already listed), we might select $f = (1 : 0) = x^2 - 6y^2$, for which $\left(\frac{-2}{f}\right) = 1 = \left(\frac{f}{3}\right)$, and $g = (2 : 0) = 2x^2 - 3y^2$, with $\left(\frac{-2}{g}\right) = -1 = \left(\frac{g}{3}\right)$. The form class group is $\mathcal{F}_{24} = \{[f], [g]\}$, with identity element $[f]$ and invariant factor type (2). (On the other hand, there is just one class of ideals of $D = D_{24}$, since $[1 : -2] = [-1 : -2]$. So $\mathcal{C}_\Delta$ is trivial and $D$ is a unique factorization domain.) ◊

We classify the integers $m$ that are properly represented by quadratic forms of discriminant 24 in the following proposition.

**Proposition 11.3.1.** *Let $m$ be an integer not divisible by 4, by 9, or by a prime $p$ congruent to 7, 11, 13, or 17 modulo 24. Let $a$ be the squarefree part of $m$, written as*

$$a = (-1)^q \cdot 2^r \cdot 3^e \cdot p_1 \cdots p_s \cdot q_1 \cdots q_t,$$

*where each of $q$, $r$, and $e$ is either 0 or 1, each $p_i$ is a distinct prime number congruent to 5 or 23 modulo 24, and each $q_i$ is a distinct prime number congruent to 1 or 19 modulo 24. Then $m$ is properly represented by $f(x,y) = x^2 - 6y^2$ if $q + r + s$ is even, and is properly represented by $g(x,y) = 2x^2 - 3y^2$ if $q + r + s$ is odd.*

*Proof.* Using the fact that $\left(\frac{6}{p}\right) = \left(\frac{-2}{p}\right)\left(\frac{-3}{p}\right) = \left(\frac{-2}{p}\right)\left(\frac{p}{3}\right)$, the conditions on $m$ are necessary and sufficient so that $x^2 - 6 \equiv 0 \pmod{m}$ has a solution, say $\ell$. Note that $(-1 : 0) \sim g$ and $(2 : 0) \sim g$, while $(3 : 0) \sim f$. (Using an involution, $(3 : 0) \sim (-2 : 0)$, which is equivalent to $(-2 : -2)$ and so to $(1 : -2)$, as we noted above.) Each form $(p_i : \ell)$ is equivalent to $g$, and each $(q_i : \ell)$ is

equivalent to $f$. Since the square of each element in the form class group $G = \mathcal{F}_{24}$ is the identity, we find that $(m : \ell)$ is equivalent to

$$(-1 : 0)^q \cdot (2 : 0)^r \cdot (3 : 0)^e \cdot (p_1 : \ell) \cdots (p_s : \ell) \cdot (q_1 : \ell) \cdots (q_t : \ell),$$

which is equivalent to $g^{q+r+s} \cdot f^{e+t}$. Thus $(m : \ell) \sim f$ if $q + r + s$ is even, and $(m : \ell) \sim g$ if $q + r + s$ is odd. This conclusion is independent of the choice of $\ell$ when more than one solution of $\phi(x) \equiv 0 \pmod{m}$ exists. Therefore $m$ is properly represented by $f(x, y) = x^2 - 6y^2$ if $q + r + s$ is even, and is properly represented by $g(x, y) = 2x^2 - 3y^2$ if $q + r + s$ is odd. □

**Example.** Let $\Delta = 73$. In an example from §10.1, we found that every quadratic form in $\mathcal{Q}_\Delta$ is in the same class under equivalence. Thus a positive or negative integer $m$ is represented by the quadratic form $f = (1 : 0) = x^2 + xy - 18y^2$ if and only if the congruence $x^2 + x - 18 \equiv 0 \pmod{m}$ has a solution. This is the case if and only if $m$ is not divisible by $73^2$ nor by any odd prime $p$ for which $\left(\frac{p}{73}\right) = -1$. ◊

**Example.** Let $\Delta = \Delta(35, 1) = 140$, so that $\phi(x) = x^2 - 35$ and $u_\Delta = \left\lfloor \sqrt{140/4} \right\rfloor = 5$. Here we find that each quadratic form in $\mathcal{Q}_{140}$ is equivalent to at least one of the following:

$$(1 : -5), \quad (-1 : -5), \quad (2 : -5), \quad (-2 : -5), \quad (5 : -5), \quad (-5 : -5).$$

Applying the equivalence algorithm to two of these forms,

| $i$ | 0 | 1 | 2 |
|---|---|---|---|
| $a$ | 1 | 10 | 1 |
| $k$ | −5 | −5 | −5 |

| $i$ | 0 | 1 | 2 |
|---|---|---|---|
| $a$ | 2 | 5 | 2 |
| $k$ | −5 | −5 | −5 |

we find that there are four *distinct* classes of forms in $\mathcal{Q}_{140}$. We can use the following as representatives for these classes:

$$(1 : 0) = x^2 - 35y^2, \quad (-1 : 0) = -x^2 + 35y^2,$$
$$(5 : 0) = 5x^2 - 7y^2, \quad (-5 : 0) = -5x^2 + 7y^2.$$

Each of these forms is its own conjugate, so the form class group $\mathcal{F}_{140}$ has invariant factor type $(2, 2)$. Genus equivalence of a form $f$ is determined by the genus symbols $\left(\frac{-1}{f}\right)$, $\left(\frac{f}{5}\right)$, and $\left(\frac{f}{7}\right)$, whose product equals 1. Each genus consists of a single class of forms. ◊

Here we can make the following statement.

**Proposition 11.3.2.** *Let $m$ be a positive squarefree integer, relatively prime to* 140 *and not divisible by any prime $p$ for which $\left(\frac{140}{p}\right) = -1$. Let $q$ be the number of*

*prime divisors $p$ of $m$ for which $\left(\frac{-1}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{p}{7}\right) = 1$; let $r$ be the number of such divisors so that $\left(\frac{-1}{p}\right) = 1$ and $\left(\frac{p}{5}\right) = -1 = \left(\frac{p}{7}\right)$; let $s$ be the number for which $\left(\frac{p}{5}\right) = 1$ and $\left(\frac{-1}{p}\right) = -1 = \left(\frac{p}{7}\right)$; and let $t$ be the number for which $\left(\frac{p}{7}\right) = 1$ and $\left(\frac{-1}{p}\right) = -1 = \left(\frac{p}{5}\right)$. Then the following statements are true.*

(1) *If $r$, $s$, and $t$ all have the same parity, then $x^2 - 35y^2 = m$ has an integer solution.*

(2) *If $r$ has the opposite parity of $s$ and $t$, then $5x^2 - 7y^2 = m$ has an integer solution.*

(3) *If $s$ has the opposite parity of $r$ and $t$, then $-x^2 + 35y^2 = m$ has an integer solution.*

(4) *If $t$ has the opposite parity of $r$ and $s$, then $-5x^2 + 7y^2 = m$ has an integer solution.*

**Exercise 11.3.1.** Let $p$ be an odd prime other than 5 or 7.

(a) Show that $\left(\frac{-1}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{p}{7}\right) = 1$ if and only if $p$ is congruent to 1, 9, 29, 81, 109, or 121 modulo 140.

(b) Show that $\left(\frac{-1}{p}\right) = 1$ and $\left(\frac{p}{5}\right) = -1 = \left(\frac{p}{7}\right)$ if and only if $p$ is congruent to 13, 17, 33, 73, 97, or 117 modulo 140.

(c) Show that $\left(\frac{p}{5}\right) = 1$ and $\left(\frac{-1}{p}\right) = -1 = \left(\frac{p}{7}\right)$ if and only if $p$ is congruent to 19, 31, 59, 111, 131, or 139 modulo 140.

(d) Show that $\left(\frac{p}{7}\right) = 1$ and $\left(\frac{-1}{p}\right) = -1 = \left(\frac{p}{5}\right)$ if and only if $p$ is congruent to 23, 43, 67, 107, 123, or 127 modulo 140.

**Example.** For instance, if $m = 247 = 13 \cdot 19$, then $r = 1$, $s = 1$, and $t = 0$. So $t$ has the opposite parity of $r$ and $s$, and $f(x, y) = -5x^2 + 7y^2$ represents $m = 247$. ◊

*Proof.* Let $g = (1 : 0)$ and $h = (5 : 0)$, with $-g = (-1 : 0)$ and $-h = (-5 : 0)$. We have that $[g]$ is the identity element of the form class group $G = \mathcal{F}_{140}$, with $[-g]^2 = [h]^2 = [-h]^2 = [g]$, and $[-g] \cdot [h] = [-h]$. If $m$ is as given, then there is some integer $\ell$ so that $f = (m : \ell)$ is a quadratic form of discriminant 140. From the definition of $q$, $r$, $s$, and $t$, it follows that

$$[f] = [g]^q \cdot [h]^r \cdot [-g]^s \cdot [-h]^t = [h]^{r+t} \cdot [-g]^{s+t}.$$

Now we find that if $r$, $s$, and $t$ are all even or all odd, then $r+t$ and $s+t$ are even, and $[f] = [g]$, from which it follows that $m$ is represented by $g(x,y) = x^2 - 35y^2$. If $r$ has the opposite parity of $s$ and $t$, then $r+t$ is odd but $s+t$ is even, so that $[f] = [h]$, and $m$ is represented by $h(x,y) = 5x^2 - 7y^2$. The remaining cases are similar. □

**Example.** In an example from §10.1, we calculated that there are four classes of quadratic forms of discriminant $\Delta = 221$. We can use the following representatives of these classes:

$$(1 : 0) = x^2 + xy - 55y^2, \qquad (-1 : 0) = -x^2 + xy + 55y^2,$$

$$(5 : 0) = 5x^2 + xy - 11y^2, \qquad (-5 : 0) = -5x^2 + xy + 11y^2.$$

Genus equivalence of these forms is determined by the genus symbols $\left(\frac{f}{13}\right)$ and $\left(\frac{f}{17}\right)$, with both symbols equal to 1 for $(1 : 0)$ and $(-1 : 0)$, and equal to $-1$ for $(5 : 0)$ and $(-5 : 0)$. The form class group $G = \mathcal{F}_{221}$ has invariant factor type (4), and we can use the class of $(5 : 0)$ as a generator of $G$. ♢

The following are examples of statements that we can make about representations in this case.

**Proposition 11.3.3.** *Let $p$ be an odd prime number other than 5.*

(1) *If $\left(\frac{p}{13}\right) = 1 = \left(\frac{p}{17}\right)$, then either $x^2 + xy - 55y^2$ or $-x^2 + xy + 55y^2$, but not both, represents $p$.*

(2) *If $\left(\frac{p}{13}\right) = -1 = \left(\frac{p}{17}\right)$, then both $5x^2 + xy - 11y^2$ and $-5x^2 + xy + 11y^2$ represent $5p$.*

Alternatively, in case (1) we have that $x^2 + xy - 55y^2$ represents $p$ or $-p$, but not both, while in case (2), $5x^2 + xy - 11y^2$ represents both $5p$ and $-5p$.

*Proof.* The congruence $\phi(x) = x^2 + x - 55 \equiv 0 \pmod{p}$ has two solutions in both cases (1) and (2), which can be written as $k$ and $-k-1$. If $\left(\frac{p}{13}\right) = 1 = \left(\frac{p}{17}\right)$, then either $(p : k) \sim (1 : 0)$ or $(p : k) \sim (-1 : 0)$. But then $(p : -k-1) \sim (1 : -1) \sim (1 : 0)$ or $(p : -k-1) \sim (-1 : -1) \sim (-1 : 0)$. So one but only one of the two forms can represent $p$.

For the second claim, note first that $(-5 : 0) \sim (5 : -1)$ in $\mathcal{Q}_{221}$. (This can be seen by direct calculation, with $(-5 : 0) \circ \begin{bmatrix} 1 & 2 \\ -1 & -1 \end{bmatrix} = (5 : -1)$, or by noting

that $(5 : -1)$ is the conjugate of $(5 : 0)$, and so must be its inverse in $\mathcal{F}_{221}$.) Now if $\left(\frac{p}{13}\right) = -1 = \left(\frac{p}{17}\right)$, we can select $k$ so that $(p : k) \sim (5 : 0)$. Then

$$(p : k) \cdot (5 : 0) \sim (5 : 0) \cdot (5 : 0) \sim (-1 : 0)$$

and

$$(p : k) \cdot (5 : -1) \sim (5 : 0) \cdot (5 : -1) \sim (1 : 0).$$

Since $p \neq 5$, both $(p : k) \cdot (5 : 0)$ and $(p : k) \cdot (5 : -1)$ are primitive, and so both $(1 : 0)$ and $(-1 : 0)$ represent $-5p$. □

In summary, these examples illustrate that the structure of the group of classes of quadratic forms of a given positive discriminant can provide information about the integers properly represented by those forms. This information is typically complete if the form class group has invariant factor type $(2, 2, \ldots, 2)$, so that each genus of forms contains exactly one class, but can provide partial information in other cases as well, as our last example demonstrates.

**Exercise 11.3.2.** Let $\Delta = \Delta(7, 1) = 28$.

(a) Show that every quadratic form of discriminant $\Delta$ is equivalent either to $f(x, y) = x^2 - 7y^2$ or to $g(x, y) = -x^2 + 7y^2$.

(b) Let $p$ be a prime number other than 2 or 7. Show that if $\left(\frac{-1}{p}\right) = 1 = \left(\frac{p}{7}\right)$, then $p$ is represented by $f$ and $-p$ is represented by $g$. Show that if $\left(\frac{-1}{p}\right) = -1 = \left(\frac{p}{7}\right)$, then $p$ is represented by $g$ and $-p$ is represented by $f$.

**Exercise 11.3.3.** Let $\Delta = \Delta(10, 1) = 40$.

(a) Show that every quadratic form of discriminant $\Delta$ is equivalent either to $f(x, y) = x^2 - 10y^2$ or to $g(x, y) = 2x^2 - 5y^2$.

(b) Let $p$ be a prime number other than 2 or 5. Show that if $\left(\frac{2}{p}\right) = 1 = \left(\frac{p}{5}\right)$, then $p$ and $-p$ are represented by $f$. Show that if $\left(\frac{2}{p}\right) = -1 = \left(\frac{p}{5}\right)$, then $p$ and $-p$ are represented by $g$.

**Exercise 11.3.4.** Let $\Delta = \Delta(57, 1) = 57$.

(a) Show that every quadratic form of discriminant $\Delta$ is equivalent either to $f(x, y) = x^2 + xy - 14y^2$ or to $g(x, y) = 2x^2 + xy - 7y^2$.

(b) Let $p$ be an odd prime number other than 3 or 19. Show that if $\left(\frac{p}{3}\right) = 1 = \left(\frac{p}{19}\right)$, then $p$ is represented by $f$ and $-p$ is represented by $g$. Show that if $\left(\frac{p}{3}\right) = -1 = \left(\frac{p}{19}\right)$, then $p$ is represented by $g$ and $-p$ is represented by $f$.

**Exercise 11.3.5.** Let $\Delta = \Delta(65, 1) = 65$.

(a) Show that every quadratic form of discriminant $\Delta$ is equivalent either to $f(x, y) = x^2 + xy - 16y^2$ or to $g(x, y) = 2x^2 + xy - 8y^2$.

(b) Let $p$ be an odd prime number other than 5 or 13. Show that if $\left(\frac{p}{5}\right) = 1 = \left(\frac{p}{13}\right)$, then $p$ and $-p$ are represented by $f$. Show that if $\left(\frac{p}{5}\right) = -1 = \left(\frac{p}{13}\right)$, then $p$ and $-p$ are represented by $g$.

**Exercise 11.3.6.** Let $\Delta = \Delta(23, 1) = 92$.

(a) Show that every quadratic form of discriminant $\Delta$ is equivalent either to $f(x, y) = x^2 - 23y^2$ or to $g(x, y) = -x^2 + 23y^2$.

(b) Let $p$ be a prime number other than 2 or 23. Show that if $\left(\frac{-1}{p}\right) = 1 = \left(\frac{p}{23}\right)$, then $p$ is represented by $f$ and $-p$ is represented by $g$. Show that if $\left(\frac{-1}{p}\right) = -1 = \left(\frac{p}{23}\right)$, then $p$ is represented by $g$ and $-p$ is represented by $f$.

## 11.4 Constructing Representations by Indefinite Forms

In §11.3, we determined criteria for representation of an integer by some quadratic form of positive discriminant $\Delta$, using the structure of the form class group $\mathcal{F}_\Delta$. For example, we found that $f(x, y) = -5x^2 + 7y^2$, a quadratic form of discriminant $\Delta = 140$, represents $m = 247$. But a claim of this type might be difficult to verify by direct calculation, since there are no immediate upper bounds on the values of $x$ and $y$ in such a solution. In this section, we develop methods of constructing these representations in practice.

Recall from §4.3 that we have a relation of $f$-equivalence on solutions of $f(x, y) = m$ for a particular quadratic form $f$ and integer $m$, defined in terms of automorphs of $f$. In §11.2, we showed that the group of automorphs of an indefinite quadratic form is infinite. Thus if $f(x, y) = m$ has a solution, it has infinitely many solutions. The number of $f$-equivalence classes of representations is finite, however, and is in one-to-one correspondence with solutions $\ell$ of

$\phi(x) \equiv 0 \pmod{m}$ for which $(m : \ell)$ is equivalent to $f$. In particular, Theorem 4.3.1 implies that if $(m : \ell) = f \circ U$, then $f(q, r) = m$, where $q$ and $r$ are the entries in the first column of $U$. The following example illustrates this approach to constructing representations of $m$ by an indefinite quadratic form.

**Example.** If $\Delta = \Delta(55, 1) = 220$, then $\phi(x) = x^2 - 55$, with smaller root $w = -\sqrt{55} \approx -7.4$. Using the table

| $x$ | $\pm7$ | $\pm6$ | $\pm5$ | $\pm4$ | $\pm3$ | $\pm2$ | $\pm1$ | $0$ |
|---|---|---|---|---|---|---|---|---|
| $\phi(x)$ | $-6$ | $-19$ | $-30$ | $-39$ | $-46$ | $-51$ | $-54$ | $-55$ |

we find the following quadratic forms $(a : k)$ with $0 < a \le \left\lfloor \sqrt{220/4} \right\rfloor = 7$ and $w < k < w + a$:

$$(1 : -7), \quad (2 : -7), \quad (3 : -7), \quad (3 : -5), \quad (5 : -5), \quad (6 : -7), \quad (6 : -5).$$

Applying the equivalence algorithm to two of these forms,

| $i$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| $a$ | 1 | 6 | 5 | 6 | 1 |
| $k$ | $-7$ | $-7$ | $-5$ | $-5$ | $-7$ |

| $i$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| $a$ | 2 | 3 | 10 | 3 | 2 |
| $k$ | $-7$ | $-7$ | $-5$ | $-5$ | $-7$ |

we find that there are two classes of ideals in $D_{220}$, but four classes of quadratic forms in $\mathcal{Q}_{220}$ (since the period length in each expansion above is even). For each $f$ in $\mathcal{Q}_{220}$, the genus symbols $\left(\frac{-1}{f}\right)$, $\left(\frac{f}{5}\right)$, and $\left(\frac{f}{11}\right)$ are defined, and we find the following combinations of genus symbols for representatives of the four classes:

$$\begin{aligned}
+++ : \quad & (1 : -7) &&= x^2 - 14xy - 6y^2 \\
-+- : \quad & (-1 : -7) &&= -x^2 - 14xy + 6y^2 \\
+-- : \quad & (2 : -7) &&= 2x^2 - 14xy - 3y^2 \\
--+ : \quad & (-2 : -7) &&= -2x^2 - 14xy + 3y^2
\end{aligned}$$

An integer $m$ is properly represented by one of these forms if and only if $x^2 \equiv 55 \pmod{m}$ has a solution. For example, if $m = 247 = 13 \cdot 19$, then $\left(\frac{55}{13}\right) = 1 = \left(\frac{55}{19}\right)$, so $\phi(x) \equiv 0 \pmod{247}$ has four distinct solutions. We find that $x^2 \equiv 55 \pmod{13}$ has solutions $\pm4$ and $x^2 \equiv 55 \pmod{19}$ has solutions $\pm6$, hence $\pm82$ and $\pm108$ satisfy $\phi(x) \equiv 0 \pmod{247}$. With $247 \equiv 3 \pmod{4}$, $\left(\frac{247}{5}\right) = \left(\frac{2}{5}\right) = -1$, and $\left(\frac{247}{11}\right) = \left(\frac{5}{11}\right) = 1$, each form $(247 : \ell)$ is in the same genus as $f = (-2 : -7)$. There are four distinct $f$-equivalence classes of solutions of $f(x, y) = 247$, which we can find as follows.

Since $\phi(82) = 6669 = 247 \cdot 27$, we have that $(247 : 82) \leftrightarrow_3 (27 : -1)$ by an involution and translation (using notation introduced in §7.4). Likewise,

$(27 : -1) \leftrightarrow_4 (-2 : -7)$. (Notice that a translation by *positive* 4 transforms $(-2 : 1)$ to $(-2 : -7)$.) Since

$$\begin{bmatrix} 4 & 1 \\ -1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 3 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 11 & 4 \\ -3 & -1 \end{bmatrix},$$

we conclude that $f(11, -3) = 247$, as in Proposition 7.4.2. Similarly, the sequence

$$(247 : -82) \leftrightarrow_{-3} (27 : 1) \leftrightarrow_3 (-2 : -7)$$

leads to the conclusion that $f(-10, 3) = 247$.

With $\phi(108) = 11609 = 247 \cdot 47$ and $\phi(-14) = 141 = 47 \cdot 3$, we find that

$$(247 : 108) \leftrightarrow_2 (47 : -14) \leftrightarrow_{-7} (3 : -7).$$

Now we might recognize, from a table above, that $(3 : -7) \sim (-2 : -7)$, with

$$(3 : -7) = (-2 : -7) \circ \begin{bmatrix} 7 & 1 \\ -1 & 0 \end{bmatrix},$$

using Theorem 10.4.2. Combining these calculations, we have that

$$\begin{aligned}(247 : 108) = (-2 : -7) \circ \left( \begin{bmatrix} 7 & 1 \\ -1 & 0 \end{bmatrix} \cdot \begin{bmatrix} -7 & 1 \\ -1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 2 & 1 \\ -1 & 0 \end{bmatrix} \right) \\ = (-2 : -7) \circ \begin{bmatrix} -107 & -50 \\ 15 & 7 \end{bmatrix},\end{aligned}$$

and conclude that $f(-107, 15) = 247$.

Finally, we find that

$$(247 : -108) \leftrightarrow_{-2} (47 : 14) \leftrightarrow_3 (3 : -5).$$

Here we might again use Theorem 10.4.2 to write

$$(3 : -5) = (-2 : -7) \circ \begin{bmatrix} 36 & 29 \\ -5 & -4 \end{bmatrix},$$

or by applying the equivalence algorithm to the pair $a = 3$ and $k = -5$, we find that

$$(-2 : -7) = (3 : -5) \circ \begin{bmatrix} 4 & -1 \\ 1 & 0 \end{bmatrix}.$$

From the second approach, we then have that

$$(247 : -108) = (-2 : -7) \circ \begin{bmatrix} 2 & -1 \\ 15 & -7 \end{bmatrix},$$

and conclude that $f(2, 15) = 247$. $\Diamond$

This example illustrates how we can use a reduction process with involutions and translations on a quadratic form $(m : \ell)$ to obtain an equivalent form $(a : k)$ with $|a| < \sqrt{\Delta/4}$. At that point, the process of Theorem 10.1.2 ensures that $(a : k)$ belongs to some predetermined class of forms, and we can find a representation of $m$ by a particular form in that class. The following theorem gives us a more direct approach, although not necessarily one that is easier for calculation, as we will see.

**Theorem 11.4.1.** *Let $\phi(x)$ be the principal polynomial of some positive discriminant $\Delta$, and let $a$ and $k$ be a pair of integers for which $a$ divides $\phi(k)$. Define the sequences $a_i$, $k_i$, and $q_i$ for $i \geq 0$ as in the equivalence algorithm on $f = (a : k)$, and let $m_i$ and $n_i$ be the numerator and denominator of the $i$-th convergent of the continued fraction $\langle q_0, q_1, q_2, \ldots \rangle$. Let $f_i$ be the quadratic form $((-1)^i a_i : k_i)$. Then $f_i(n_{i-2}, (-1)^{i-1} n_{i-1}) = a$ for every $i \geq 0$.*

*Proof.* Let $f = (a : k)$. By Theorem 10.4.2, we have that $f \circ W_i = f_i$ for all $i \geq 0$, where

$$W_i = \begin{bmatrix} m_{i-1} & (-1)^i m_{i-2} \\ n_{i-1} & (-1)^i n_{i-2} \end{bmatrix}.$$

But then $f = f_i \circ {W_i}^{-1}$, with

$${W_i}^{-1} = \begin{bmatrix} (-1)^i n_{i-2} & (-1)^{i-1} m_{i-2} \\ -n_{i-1} & m_{i-1} \end{bmatrix}.$$

It follows that $f_i((-1)^i n_{i-2}, -n_{i-1}) = a$, as we noted in the preceding example. Since $f(x, y)$ always equals $f(-x, -y)$ when $f$ is a quadratic form, we can also say that

$$f_i((-1)^i \cdot (-1)^i n_{i-2}, (-1)^i \cdot -n_{i-1}) = f_i(n_{i-2}, (-1)^{i-1} n_{i-1}) = a,$$

as we wanted to show. □

**Example.** Let $\Delta = 220$, and let $a = 247$ and $k = 82$, as in one case of the preceding example. Here we find the following data from the equivalence algorithm on $(247 : 82)$, together with the denominator sequence on the resulting continued fraction.

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| $a$ | 247 | −110 | 27 | 2 | 3 | 10 | 3 | 2 | 3 |
| $k$ | 82 | 165 | −55 | 1 | −7 | −5 | −5 | −7 | −7 |
| $q$ | −1 | 1 | 2 | 3 | 4 | 1 | 4 | 7 | |
| $n$ | 1 | 1 | 3 | 10 | 43 | 53 | 255 | 1838 | |

For example, the conjugate of $k_0 = 82$ is $-82$, and $k_1 = 165$ is the smallest value greater than $u = -\sqrt{55}$ with $k_1 \equiv -82 \pmod{247}$. So $a_1 = -\frac{\phi(165)}{247} = -110$.

Since $a_1$ is negative, we then want the largest integer less than $u$ congruent to $-165$ modulo 110, that is, $k_2 = -55$. Then $a_2 = -\frac{\phi(-55)}{-110} = 27$. Continuing in this way, we eventually come to a repeating pattern, finding that $a_8 = a_4$ and $k_8 = k_4$.

Now for example, $f_7 = (-2 : -7)$, so that $f_7(n_5, n_6) = a$, that is,

$$f_7(53, 255) = -2(53)^2 - 14 \cdot 53 \cdot 255 + 3 \cdot 255^2 = 247.$$

This is not the same solution arising from $(247 : 82)$ that we found in the preceding example, but must be equivalent to $(11, -3)$. In fact, we find by Theorem 11.2.2 and previous calculations that $U = \begin{bmatrix} 173 & -36 \\ -24 & 5 \end{bmatrix}$ is an automorph of $(-2 : -7)$, and can verify that $-U^{-1} \cdot \begin{bmatrix} 11 \\ -3 \end{bmatrix} = \begin{bmatrix} 53 \\ 255 \end{bmatrix}$. ◊

**Example.** Let $f(x, y) = x^2 - 5xy - 2y^2$. We will use Theorem 11.4.1 to find a solution of $f(x, y) = -29$. Here the discriminant of $f$ is $\Delta = 33$, so that $\phi(x) = x^2 + x - 8$ is the principal polynomial of discriminant $\Delta$. Since $\left(\frac{33}{29}\right) = 1$, we find that $\phi(x) \equiv 0 \pmod{29}$ has two solutions, and direct calculation shows that $x = 13$ and $x = -14$ are those solutions. We may apply Theorem 11.4.1 to $a = -29$ and $k = 13$, for example, using the following table of data.

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| $a$ | $-29$ | 6 | 1 | 2 | 3 | 2 | 1 | 2 |
| $k$ | 13 | $-14$ | 1 | $-3$ | $-2$ | $-2$ | $-3$ | $-3$ |
| $q$ | 0 | 2 | 3 | 2 | 1 | 2 | 5 | |
| $n$ | 1 | 2 | 7 | 16 | 23 | 62 | 333 | |

Here we find that $f_6 = (1 : -3) = x^2 - 5xy - 2y^2$, so that $f$ represents $-29$. One solution of $f(x, y) = -29$ is $(n_4, (-1)^5 n_5) = (23 - 62)$, as we can verify. ◊

**Exercise 11.4.1.** In each part, a solution $k$ of $x^2 \equiv 6 \pmod{p}$ for some prime $p$ is given. In each case, use the algorithm of Theorem 11.4.1 to find a solution of $x^2 - 6y^2 = p$ or $x^2 - 6y^2 = -p$.

(a) $k = 11$ and $p = 23$.

(b) $k = 18$ and $p = 53$.

(c) $k = 26$ and $p = 67$.

(d) $k = 15$ and $p = 73$.

**Exercise 11.4.2.** In each part, use the methods of this section to find a solution of the given equation. (Note that each quadratic form listed here refers to an example in the exercises of §11.3.)

(a) $x^2 - 7y^2 = 53$.

(b) $x^2 - 7y^2 = -47$.

(c) $x^2 - 10y^2 = 31$.

(d) $x^2 - 10y^2 = -31$.

(e) $2x^2 - 5y^2 = 43$.

(f) $2x^2 - 5y^2 = -43$.

(g) $x^2 + xy - 14y^2 = -41$.

(h) $2x^2 + xy - 7y^2 = 41$.

(i) $x^2 + xy - 16y^2 = 29$.

(j) $x^2 + xy - 16y^2 = -29$.

(k) $2x^2 + xy - 8y^2 = 83$.

(l) $2x^2 + xy - 8y^2 = -83$.

(m) $x^2 - 23y^2 = 29$.

(n) $x^2 - 23y^2 = -79$.

## Representations by Indefinite Forms—Review

In the quadratic continued fraction algorithm of Theorem 10.3.1, we saw that the method of calculating the continued fraction of an irrational quadratic number also produces an infinite (but repeating) sequence of quadratic forms of the same positive discriminant $\Delta$. In this chapter, we demonstrated how this process provides important information about the integers represented by indefinite quadratic forms of that discriminant.

(1) We can associate a particular quadratic number $v$ to a given indefinite quadratic form $f(x, y)$, and we refer to the continued fraction of $v$ as the continued fraction of $f(x, y)$ as well. If

$$(a_0 : k_0), (a_1 : k_1), (a_2 : k_2), \ldots$$

is the sequence of quadratic forms that arises from the quadratic continued fraction algorithm applied to $v$, then there are corresponding solutions of $f(x, y) = (-1)^i a_i$ for all $i$. Specifically, these representations are expressed in terms of the numerator and denominator sequences of convergents in the continued fraction of $f(x, y)$. (See Theorem 11.1.1 for details.)

(2) If $f(x, y) = ax^2 + bxy + cy^2$ has positive discriminant $\Delta = b^2 - 4ac$, with $a$ positive and $c$ negative, and $d$ is an integer with $|d| < \sqrt{\Delta/4}$, then all proper solutions of $f(x, y) = d$ in positive integers are obtained from the convergents in the continued fraction associated with $f$.

(3) If $d$ is positive and not a square, the continued fraction of $f(x, y) = x^2 - dy^2$ eventually produces a solution of $x^2 - dy^2 = 1$, and we can be sure that all solutions in positive integers are powers of a particular quadratic number. Thus we can calculate the fundamental solution of Pell's equation in practice.

(4) In a similar way, the continued fraction of the principal form of discriminant $\Delta > 0$ is guaranteed to produce the fundamental unit in the quadratic domain $D_\Delta$. We can also use this approach to determine the group of automorphs of an indefinite quadratic form.

(5) We can use the structure of the class group of quadratic forms of positive discriminant $\Delta$ to describe criteria for representations of integers by a given indefinite quadratic form. We can also use continued fraction expansions to construct these representations when they are known to exist.

In summary for the last three chapters, we have seen that continued fractions of irrational quadratic numbers allow us to perform the same sort of calculations for positive discriminants as we developed for negative discriminants in previous chapters. In particular, we can systematically determine class groups (of quadratic forms or of ideals) of positive discriminant. Thus we can often provide precise criteria for representations of integers by indefinite quadratic forms.

# Part Five: Quadratic Recursive Sequences

**Overview.** As our final topic, we consider patterns in specific solutions of second-order recurrence relations, with the Fibonacci sequence as the most familiar example. We find that each sequence of this type is closely related to the roots of a particular quadratic polynomial, connecting this topic to previous consideration of quadratic integers.

Chapter 12 introduces our objects of interest as sequences defined recursively as linear combinations of its two preceding terms, with specified initial values. We can say that each such sequence is defined by a quadratic *characteristic polynomial*, and we show that powers of a root of that polynomial can be calculated using terms of the sequence. We consider patterns in these sequences when they are reduced modulo a prime $p$, and find that we can describe these patterns most easily by working within a field with $p^2$ elements. We use these fields to develop a method of calculating the *suborder* of a quadratic recursive sequence modulo $p$, that is, the index of the first term of the sequence that is divisible by $p$.

In Chapter 13, we describe several connections between quadratic sequences and properties of quadratic domains, particularly those with positive discriminant. We show that we can use the smallest solution in positive integers of a quadratic form equation $f(x, y) = 1$ to define a quadratic recursive sequence, which then produces all other solutions of that equation. We use this approach to describe the smallest positive solution of $x^2 - dy^2 = 1$ when $d$ is divisible by a square greater than 1. Finally, we use these quadratic sequences to determine class groups of quadratic domains of positive discriminant that are contained in other quadratic domains, thus demonstrating that it is sufficient to compute the class group of a *complete* quadratic domain, as we saw in Chapter 8 is the case for class groups of negative discriminant.

**Requirements for Part Five.** We will see that many results about a quadratic recursive sequence, particularly when we reduce its terms modulo a prime

number $p$, are best obtained and explained by working within a field $\mathbb{E} = \mathbb{E}_p$ containing $p^2$ elements, that is, a *quadratic extension field* of $\mathbb{F}_p$, the base field with $p$ elements. We list several properties of these fields that we assume throughout Part Five.

(1) We can construct a field with $p^2$ elements using any example of an irreducible quadratic polynomial in $\mathbb{F}_p[x]$. (Here $\mathbb{F}_p[x]$ is the set of all polynomials having coefficients in the field $\mathbb{F}_p$.) Specifically, if $g(x)$ is an irreducible quadratic polynomial in $\mathbb{F}_p[x]$, then there is a field

$$\mathbb{E} = \{a + bz \mid a, b \in \mathbb{F}_p \text{ and } g(z) = 0\}.$$

This field has $p^2$ elements, and contains $\mathbb{F}_p$ as a subfield.

(2) Any two fields with $p^2$ elements are isomorphic. In other words, our choice of the irreducible polynomial $g(x)$ does not affect the algebraic structure of $\mathbb{E}$ as a field. (Likewise, no other way of constructing a field with $p^2$ elements can produce different algebraic properties.)

(3) If $f(x)$ is any quadratic polynomial with coefficients in $\mathbb{F}_p$, then $f(x)$ factors as a product of linear polynomials in $\mathbb{E}[x]$. Specifically, if

$$f(x) = x^2 + bx + c$$

with $b$ and $c$ elements of $\mathbb{F}_p$, then we can write

$$f(x) = (x - u)(x - v)$$

for some elements $u$ and $v$ in $\mathbb{E}$.

(4) The function $\psi : \mathbb{E} \to \mathbb{E}$ defined by $\psi(x) = x^p$ is an *automorphism*, that is, a bijective homomorphism between $\mathbb{E}$ and itself. Here $\psi(v) = v$ if and only if $v$ is an element of the subfield $\mathbb{F}_p$ of $\mathbb{E}$. Furthermore, if $v$ is a root of a polynomial $f(x)$ in $\mathbb{F}_p[x]$, then $\psi(v)$ is also a root of $f(x)$.

(5) The set, $\mathbb{E}^\times$, of nonzero elements of $\mathbb{E}$ forms a *cyclic* group under multiplication. Thus there is an element $w$ in $\mathbb{E}$ so that every element $v \neq 0$ in $\mathbb{E}$ can be written uniquely as $v = w^t$ with $1 \leq t \leq p^2 - 1$. We will often need to make statements about the order of an element in $\mathbb{E}^\times$ or in $\mathbb{F}_p^\times$. In general, if $a$ is an element in a finite group $G$ (written multiplicatively), then the order of $a$ is the smallest positive integer $t$ for which $a^t = 1$, the identity element of $G$. In this case, we write $t = \text{ord}(a)$. The following fact will be particularly useful on several occasions. If $a$ is an element of order $t$ in $G$, and $k$ is an integer, then $\text{ord}(a^k) = \frac{t}{\gcd(k,t)}$.

Proofs of these claims and more general properties of finite fields and groups appear in Appendix C.

# 12

# Properties of Recursive Sequences

The *Fibonacci sequence*, $F_n$, is defined for $n \geq 0$ by setting $F_0 = 0$ and $F_1 = 1$, and defining each successive term to be the sum of the two preceding terms, $F_n = F_{n-1} + F_{n-2}$, as follows.

$$F_n : \quad 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, \ldots .$$

In the next two chapters, we consider arithmetic properties of this and similarly defined recursive sequences, noting in particular their connections to other questions in quadratic number theory. In §12.1, we associate a quadratic polynomial to each such sequence. We show that the roots of this polynomial help us describe divisibility properties of these sequences, such as common divisors of two particular terms. In §12.2, we consider patterns in these terms when they are reduced modulo a prime $p$. We will find that these sequences exhibit a periodic nature, which is best described using powers of those same roots in a field with $p^2$ elements. In §12.3 and §12.4, we introduce a function defined on a field with $p$ elements that further illuminates the behavior of recursive sequences modulo the prime $p$. In Chapter 13, we will illustrate applications of these concepts to Pell's equation, and to class groups of quadratic subdomains of positive discriminant. We see in this way further evidence that results about integers can be obtained via algebraic properties of other sets of numbers.

## 12.1 Divisibility Properties of Quadratic Recursive Sequences

We generalize the definition of the Fibonacci sequence as follows.

**Definition.** Let $f(x) = x^2 - sx - t$, where $s$ and $t$ are integers with $t \neq 0$. Then the *quadratic recursive sequence* $r_n$ with *characteristic polynomial* $f(x)$ is the sequence defined for $n \geq 0$ as follows:

$$r_0 = 0, \quad r_1 = 1, \quad \text{and} \quad r_n = sr_{n-1} + tr_{n-2} \quad \text{if } n \geq 2. \tag{12.1.1}$$

The equation $r_n = sr_{n-1} + tr_{n-2}$ is, more precisely, a *second-order, linear, homogeneous recurrence relation with integer coefficients.* We will reserve the term *quadratic recursive sequence* for the specific solution of this recurrence relation when $r_0 = 0$ and $r_1 = 1$. We consider other solutions of this type of recurrence relation, that is, other possibilities for the initial terms, at the end of this section.

**Example.** The Fibonacci sequence is the quadratic recursive sequence with characteristic polynomial $f(x) = x^2 - x - 1$. We will continue to denote the $n$-th term in the Fibonacci sequence as $F_n$. ◊

To simplify terminology, we will often refer to the quadratic recursive sequence $r_n$ with characteristic polynomial $f(x)$ as the *quadratic sequence defined by* $f(x)$. It is always assumed that $r_0 = 0$ and $r_1 = 1$ when we use this wording. In this section, we consider divisibility properties of these sequences, such as which terms divide other terms, or what common divisors two terms of the sequence can have. We will see that some of these properties can be most easily explained by reference to powers of specific quadratic integers. The following theorem is the key connection between these concepts.

**Theorem 12.1.1.** *Let $r_n$ be the quadratic recursive sequence with characteristic polynomial $f(x) = x^2 - sx - t$, as in equation* (12.1.1)*. If $v$ is a root of $f(x)$, then $v^n = r_n v + tr_{n-1}$ for every $n \geq 1$.*

*Proof.* The equation $v^1 = r_1 v + tr_0$ is immediate from the definition of the initial terms of the sequence. If $v^k = r_k v + tr_{k-1}$ for some $k \geq 1$, then

$$\begin{aligned} v^{k+1} = v \cdot v^k = r_k v^2 + tr_{k-1}v &= r_k(sv + t) + tr_{k-1}v \\ &= (sr_k + tr_{k-1})v + tr_k = r_{k+1}v + tr_k, \end{aligned}$$

using the assumption that $f(v) = v^2 - sv - t = 0$, along with the recursive definition of $r_n$. The result follows by induction. □

**Example.** The roots of $f(x) = x^2 - x - 1$, the characteristic polynomial of the Fibonacci sequence, are $v = \frac{1+\sqrt{5}}{2}$ and $w = \frac{1-\sqrt{5}}{2}$. Since $v^2 = v + 1$, we find that

$\upsilon^3 = \upsilon^2 + \upsilon = 2\upsilon + 1$, and then $\upsilon^4 = 2\upsilon^2 + \upsilon = 3\upsilon + 2$, and so forth. In general, $\upsilon^n = F_n\upsilon + F_{n-1}$. Note that $w^n = F_n w + F_{n-1}$ as well, since the only property of $\upsilon$ required in Theorem 12.1.1 is that it be a root of $f(x)$. ♢

The final observation of this example helps us obtain the following formula for the terms in a quadratic sequence.

**Theorem 12.1.2.** *Let $r_n$ be the quadratic recursive sequence with characteristic polynomial $f(x) = x^2 - sx - t$. Suppose that $f(x)$ factors as $(x - \upsilon)(x - w)$ for some complex numbers $\upsilon$ and $w$. Then for all $n \geq 0$,*

$$r_n = \frac{\upsilon^n - w^n}{\upsilon - w}, \quad \text{if } \upsilon \neq w \qquad \text{and} \qquad r_n = n\upsilon^{n-1}, \quad \text{if } \upsilon = w. \tag{12.1.2}$$

*Proof.* Since $t \neq 0$ by definition, we know that $\upsilon$ and $w$ are nonzero. So the equations in (12.1.2) both produce $r_n = 0$ when $n = 0$. By Theorem 12.1.1, we have that $\upsilon^n = r_n\upsilon + tr_{n-1}$ and $w^n = r_n w + tr_{n-1}$ for all $n \geq 1$. Thus $\upsilon^n - w^n = r_n(\upsilon - w)$ if $n \geq 1$. If $\upsilon \neq w$, the first equation of (12.1.2) follows immediately.

Suppose then that $\upsilon = w$. In this case, $x^2 - sx - t = x^2 - 2\upsilon x + \upsilon^2$, so that $s = 2\upsilon$ and $t = -\upsilon^2$. We can prove (12.1.2) by induction on $n$. If $n = 1$, then $r_1 = 1 = 1 \cdot \upsilon^0$. If $n = 2$, then $r_2 = sr_1 + tr_0 = s = 2 \cdot \upsilon^1$. So suppose that $r_k = k\upsilon^{k-1}$ and $r_{k+1} = (k+1)\upsilon^k$ for some $k \geq 1$. Then by definition,

$$r_{k+2} = sr_{k+1} + tr_k = 2\upsilon \cdot (k+1)\upsilon^k - \upsilon^2 \cdot k\upsilon^{k-1} = (k+2)\upsilon^{k+1}.$$

Since this is the second formula of (12.1.2) with $k + 2$ in place of $n$, the result follows by induction. □

**Example.** For the Fibonacci sequence, with $\upsilon = \frac{1+\sqrt{5}}{2}$ and $w = \frac{1-\sqrt{5}}{2}$, we have that

$$F_n = \frac{\upsilon^n - w^n}{\upsilon - w} = \frac{\upsilon^n - w^n}{\sqrt{5}}$$

for all $n$. Notice that $|w| < 1$, so that $w^n$ approaches 0 as $n$ increases. Thus $F_n$ is closely approximated by $\upsilon^n/\sqrt{5}$ for large values of $n$. (For example, $\upsilon^{15}/\sqrt{5} \approx 609.9997$ while $F_{15} = 610$.) We have in particular that

$$\lim_{n\to\infty} \frac{F_{n+1}}{F_n} = \lim_{n\to\infty} \frac{\upsilon^{n+1} - w^{n+1}}{\sqrt{5}} \cdot \frac{\sqrt{5}}{\upsilon^n - w^n}$$

$$= \lim_{n\to\infty} \frac{\upsilon^{n+1} - w^{n+1}}{\upsilon^n - w^n} = \lim_{n\to\infty} \frac{\upsilon^{n+1}}{\upsilon^n} = \upsilon.$$

We observed this fact in connection with the continued fraction of the golden ratio $\varphi = \frac{1+\sqrt{5}}{2}$ in §9.1. ♢

**Divisibility in Quadratic Recursive Sequences.** In this subsection, we use the connection between quadratic sequences and powers of quadratic integers to prove some general properties of those sequences.

**Lemma 12.1.3.** *Let $\upsilon$ and $w$ be the roots of a quadratic polynomial $f(x) = x^2 - sx - t$. If $a\upsilon + b = c\upsilon + d$, $aw + b = cw + d$, and $\upsilon \neq w$, then $a = c$ and $b = d$.*

*Proof.* We have that $(a - c)\upsilon = d - b = (a - c)w$, so that $(a - c)(\upsilon - w) = 0$. If $\upsilon \neq w$, then $a - c = 0$ and so $d - b = 0$. □

**Theorem 12.1.4.** *Let $r_n$ be the quadratic sequence with characteristic polynomial $f(x) = x^2 - sx - t$. Let $m > 0$ and $n \geq 0$ be integers. Then*

$$r_{m+n} = r_m r_{n+1} + t r_{m-1} r_n. \tag{12.1.3}$$

*Proof.* Equation (12.1.3) is true when $n = 0$, since $r_0 = 0$ and $r_1 = 1$. So assume that $m$ and $n$ are both positive. Let $\upsilon$ and $w$ be the roots of the characteristic polynomial $x^2 - sx - t$. By Theorem 12.1.1, we have that $\upsilon^{m+n} = r_{m+n}\upsilon + t r_{m+n-1}$. On the other hand,

$$\begin{aligned}
\upsilon^{m+n} = \upsilon^m \cdot \upsilon^n &= (r_m\upsilon + t r_{m-1})(r_n\upsilon + t r_{n-1}) \\
&= r_m r_n \upsilon^2 + (t r_m r_{n-1} + t r_{m-1} r_n)\upsilon + t^2 r_{m-1} r_{n-1} \\
&= (s r_m r_n + t r_m r_{n-1} + t r_{m-1} r_n)\upsilon + (t r_m r_n + t^2 r_{m-1} r_{n-1}) \\
&= (r_m(s r_n + t r_{n-1}) + t r_{m-1} r_n)\upsilon + (t r_m r_n + t^2 r_{m-1} r_{n-1}) \\
&= (r_m r_{n+1} + t r_{m-1} r_n)\upsilon + (t r_m r_n + t^2 r_{m-1} r_{n-1}).
\end{aligned}$$

The same equations hold with $w$ in place of $\upsilon$. If $\upsilon \neq w$, then Lemma 12.1.3 implies that we can identify coefficients of $\upsilon$ in the equations above, and conclude that $r_{m+n} = r_m r_{n+1} + t r_{m-1} r_n$.

If $\upsilon = w$, then $r_n = n\upsilon^{n-1}$ for all $n \geq 1$, and $t = -\upsilon^2$. But then

$$\begin{aligned}
r_m r_{n+1} + t r_{m-1} r_n &= m\upsilon^{m-1} \cdot (n+1)\upsilon^n - \upsilon^2 \cdot (m-1)\upsilon^{m-2} \cdot n\upsilon^{n-1} \\
&= (m(n+1) - (m-1)n)\upsilon^{m+n-1} = (m+n)\upsilon^{m+n-1} = r_{m+n},
\end{aligned}$$

so that equation (12.1.3) holds in that case as well. □

**Example.** We have that $F_{m+n} = F_m F_{n+1} + F_{m-1} F_n$ for all $m \geq 1$ and $n \geq 0$, since $t = 1$ for the Fibonacci sequence. For instance, if $m = 8$ and $n = 6$, then $F_8 \cdot F_7 + F_7 \cdot F_6 = 21 \cdot 13 + 13 \cdot 8 = 377 = F_{14}$. ◊

**Corollary 12.1.5.** *If $r_n$ is the quadratic sequence defined by $x^2 - sx - t$, then $r_{2n+1} = r_{n+1}^2 + t r_n^2$ for all $n \geq 0$.*

*Proof.* We can write $2n + 1$ as $m + n$ with $m = n + 1$. Then this result follows immediately from Theorem 12.1.4. □

**Corollary 12.1.6.** *Let $r_n$ be the quadratic sequence defined by $x^2 - sx - t$. If $m$ divides $n$ for some nonnegative integers $m$ and $n$, then $r_m$ divides $r_n$.*

*Proof.* If $m = 0$, then $m$ divides $n$ only when $n = 0$. In that case, $r_m$ also divides $r_n$. So let $m$ be positive. We can prove the corollary by showing that $r_m$ divides $r_{mk}$ for all $k \geq 0$. We do so by induction on $k$.

If $k = 0$, then $r_{mk} = r_0 = 0$, and so $r_m$ divides $r_{mk}$. So suppose that $r_m$ divides $r_{mk}$ for some $k \geq 0$. Then $r_{m(k+1)} = r_{m+mk} = r_m r_{mk+1} + t r_{m-1} r_{mk}$ by Theorem 12.1.4. Thus $r_{m(k+1)}$ is a combination of $r_m$ and $r_{mk}$, and since $r_m$ divides $r_{mk}$ by the inductive hypothesis, it follows that $r_m$ divides $r_{m(k+1)}$. □

**Exercise 12.1.1.** Use the fact that $F_m$ divides $F_n$ if $m$ divides $n$ to help find the prime factorizations of the following Fibonacci numbers.

(a) $F_{15} = 610$.

(b) $F_{18} = 2584$.

(c) $F_{20} = 6765$.

(d) $F_{24} = 46368$.

(e) $F_{30} = 832040$.

(f) $F_{36} = 14930352$.

As a consequence of Corollary 12.1.6, a Fibonacci number $F_n$ can be prime only when $n = 4$ or $n$ is prime. (Here $F_4 = 3$ is divisible by $F_2 = 1$, but this does not preclude $F_4$ from being prime. However, if $n$ is an even integer with $n > 4$, then either $n = 2m$ with $m > 1$ an odd integer, or $n$ is divisible by 4. In either case, $F_n$ has a proper divisor greater than 1.) The converse of this statement is not true. The smallest prime $p$ for which $F_p$ is composite is $p = 19$.

For the next several properties, it will be useful to extend Theorem 12.1.1 to negative powers of a root $v$ of the characteristic polynomial of a quadratic sequence. Since we assume that $t$ is nonzero, a root of $f(x) = x^2 - sx - t$ is nonzero as well, so has an inverse in the complex numbers.

**Theorem 12.1.7.** *Let $r_n$ be the quadratic recursive sequence with characteristic polynomial $f(x) = x^2 - sx - t$, and let $v$ be a root of $f(x)$. Then for every positive integer $n$,*

$$(-t)^n v^{-n} = -r_n v + r_{n+1}. \tag{12.1.4}$$

*Proof.* Since $v^2 - sv - t = 0$, then $v(v - s) = t$, so that $v^{-1} = t^{-1}(v - s)$, or $-tv^{-1} = -v + s$. So equation (12.1.4) holds for $n = 1$, since $r_1 = 1$ and

$r_2 = sr_1 + tr_0 = s$. Now assume that (12.1.4) holds for some positive integer $n$. Then

$$\begin{aligned}(-t)^{n+1}v^{-(n+1)} &= (-t)^n v^{-n} \cdot (-t)v^{-1} \\ &= (-r_n v + r_{n+1})(-v + s) = r_n v^2 + (-sr_n - r_{n+1})v + sr_{n+1} \\ &= (sr_n - sr_n - r_{n+1})v + (sr_{n+1} + tr_n) = -r_{n+1}v + r_{n+2}.\end{aligned}$$

This proves (12.1.4) for all $n \geq 1$ by induction. □

**Theorem 12.1.8.** *Let $r_n$ be the quadratic sequence defined by $x^2 - sx - t$. Let $m$ and $n$ be integers with $m \geq n \geq 0$. Then*

$$(-t)^n r_{m-n} = r_m r_{n+1} - r_{m+1} r_n. \tag{12.1.5}$$

*Proof.* When $n = 0$, then

$$(-t)^n r_{m-n} = r_m = r_m r_1 - r_{m+1} r_0 = r_m r_{n+1} - r_{m+1} r_n.$$

When $n = m$, then

$$(-t)^n r_{m-n} = (-t)^m r_0 = 0 = r_m r_{m+1} - r_{m+1} r_m = r_m r_{n+1} - r_{m+1} r_n.$$

So assume that $m > n > 0$, and let $v$ and $w$ be the roots of the characteristic polynomial $x^2 - sx - t$. By Theorem 12.1.1,

$$(-t)^n v^{m-n} = (-t)^n r_{m-n} v - (-t)^{n+1} r_{m-n-1}.$$

On the other hand, using equation (12.1.4),

$$\begin{aligned}(-t)^n v^{m-n} &= v^m \cdot (-t)^n v^{-n} \\ &= (r_m v + t r_{m-1})(-r_n v + r_{n+1}) \\ &= -r_m r_n v^2 + (r_m r_{n+1} - t r_{m-1} r_n)v + t r_{m-1} r_{n+1} \\ &= (r_m r_{n+1} - t r_{m-1} r_n - s r_m r_n)v + (t r_{m-1} r_{n+1} - t r_m r_n) \\ &= (r_m r_{n+1} - r_n(t r_{m-1} + s r_m))v + t(r_{m-1} r_{n+1} - r_m r_n) \\ &= (r_m r_{n+1} - r_n r_{m+1})v + t(r_{m-1} r_{n+1} - r_m r_n).\end{aligned}$$

The same equations hold with $w$ in place of $v$, so if $v \neq w$, then we can identify coefficients of $v$ and conclude that $(-t)^n r_{m-n} = r_m r_{n+1} - r_{m+1} r_n$.

When $v = w$, so that $r_n = n v^{n-1}$ for all $n \geq 1$, and $-t = v^2$, we can prove equation (12.1.5) directly. In that case,

$$(-t)^n r_{m-n} = v^{2n}(m-n)v^{m-n-1} = (m-n)v^{m+n-1},$$

while

$$\begin{aligned}r_m r_{n+1} - r_{m+1} r_n &= m v^{m-1} \cdot (n+1)v^n - (m+1)v^m \cdot n v^{n-1} \\ &= (m(n+1) - (m+1)n)v^{m+n-1}.\end{aligned}$$

Since $m(n+1)-(m+1)n = mn+m-mn-n = m-n$, equation (12.1.5) follows. □

**Corollary 12.1.9.** *Let $r_n$ be the quadratic recursive sequence defined by $f(x) = x^2 - sx - t$. Then $r_m^2 - r_{m+1}r_{m-1} = (-t)^{m-1}$ for all $m \geq 1$.*

*Proof.* This is a consequence of (12.1.5), letting $n = m-1$. □

**Example.** We have $F_m^2 - F_{m+1}F_{m-1} = (-1)^{m-1}$ since $t = 1$ for the Fibonacci sequence. Equivalently, $F_{m+1}F_{m-1} - F_m^2 = (-1)^m$ for all $m \geq 1$. For example,

$$F_{12} \cdot F_{10} - F_{11}^2 = 144 \cdot 55 - 89^2 = 7920 - 7921 = -1 = (-1)^{11}$$

when $m = 11$. ◊

Note that if $t = 1$ or $t = -1$, then Corollary 12.1.9 implies that we can write 1 as a combination of $r_m$ and $r_{m+1}$. Thus, under this assumption, two consecutive terms of a quadratic recursive sequence must be relatively prime. Our next corollary strengthens this result.

**Theorem 12.1.10.** *Let $r_n$ be the quadratic sequence defined by $x^2 - sx - t$, where $t = 1$ or $t = -1$. Then $\gcd(r_m, r_n) = |r_{\gcd(m,n)}|$ for every pair of nonnegative integers $m$ and $n$.*

**Example.** For the Fibonacci sequence, we have $\gcd(F_{14}, F_{21}) = F_7$, that is, $\gcd(377, 10946) = 13$. ◊

*Proof.* Let $m$ and $n$ be integers and let $g = \gcd(m, n)$. Since $g$ divides $m$ and $g$ divides $n$, we know by Theorem 12.1.6 that $r_g$ divides $r_m$ and $r_g$ divides $r_n$. So $r_g$ is a common divisor of $r_m$ and $r_n$. If we can show that $r_g$ is a combination of $r_m$ and $r_n$, then it follows that $\gcd(r_m, r_n) = |r_g|$.

Since $\gcd(m, n) = g$, then $mq - nr = g$ for some positive integers $q$ and $r$. With $t = \pm 1$, Theorem 12.1.8 implies that $\pm r_g = r_{mq}r_{nr+1} - r_{mq+1}r_{nr}$. Since $r_m$ divides $r_{mq}$ and $r_n$ divides $r_{nr}$, we then have $r_g$ written as a combination of $r_m$ and $r_n$, as we wanted to find. □

**Example.** Let $r_n = 2r_{n-1} - r_{n-2}$ with $r_0 = 0$ and $r_1 = 1$. This sequence begins:

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, \ldots .$$

Since its characteristic polynomial $x^2 - 2x + 1$ factors as $(x-1)^2$, Theorem 12.1.2 implies that $r_n = n \cdot 1^{n-1} = n$ for all $n$, which confirms the pattern above. With $t = -1$, each of the theorems and corollaries that we have proved in this section apply to this sequence. For example, equations (12.1.3) and (12.1.5) imply, respectively, that

$$m + n = m(n+1) - (m-1)n \quad \text{and} \quad m - n = m(n+1) - (m+1)n.$$

It is clearly true that $r_m$ divides $r_n$ if $m$ divides $n$, and that $\gcd(r_m, r_n) = r_{\gcd(m,n)}$ as in Corollary 12.1.6 and Theorem 12.1.10. Notice that

$$r_n^2 - r_{n-1} \cdot r_{n+1} = n^2 - (n-1)(n+1) = n^2 - (n^2 - 1) = 1 = (-t)^{n-1}$$

for all $n \geq 1$, as should be the case by Corollary 12.1.9. ♢

**Exercise 12.1.2.** In each part, a quadratic recursive sequence $r_n$ (with $r_0 = 0$ and $r_1 = 1$) is defined. Find the terms of the given sequence up to $r_{10}$, and find a formula for $r_n$ as in Theorem 12.1.2. Verify in each case (for $m, n \leq 10$) that if $m$ divides $n$, then $r_m$ divides $r_n$. Verify the claim of Theorem 12.1.8 for $10 \geq m \geq n \geq 0$.

(a) $r_n = 2r_{n-2}$.

(b) $r_n = 2r_{n-1} + r_{n-2}$.

(c) $r_n = 2r_{n-1} - 3r_{n-2}$.

(d) $r_n = 2r_{n-1} + 3r_{n-2}$.

(e) $r_n = 2r_{n-1} - 2r_{n-2}$.

(f) $r_n = 5r_{n-1} - 6r_{n-2}$.

(g) $r_n = 3r_{n-1} - 4r_{n-2}$.

(h) $r_n = 3r_{n-1} - 5r_{n-2}$.

All of our results about a quadratic sequence $r_n$ in this section are under the assumption that its initial terms are $r_0 = 0$ and $r_1 = 1$. If we drop this restriction, we can make the following more general statement.

**Theorem 12.1.11.** *Let $s$ and $t$ be integers and let $r_n$ be defined by $r_n = sr_{n-1} + tr_{n-2}$ for $n \geq 2$, with $r_0 = 0$ and $r_1 = 1$. Let $q_n$ be another sequence satisfying $q_n = sq_{n-1} + tq_{n-2}$ for all $n \geq 2$, but with $q_0$ and $q_1$ some unspecified integers. Then for all $n \geq 1$,*

$$q_n = tq_0 \cdot r_{n-1} + q_1 \cdot r_n. \tag{12.1.6}$$

In other words, we can calculate the $n$-th term in the second sequence $q_n$ using only our previous results about $r_n$ and the initial terms of $q_n$.

*Proof.* We use induction on $n$. If $n = 1$, then $q_1 = tq_0 \cdot r_0 + q_1 \cdot r_1$ is true. If $n = 2$, then $q_2 = sq_1 + tq_0 = tq_0 \cdot r_1 + q_1 \cdot r_2$, since $r_2 = sr_1 + tr_0 = s$. So now suppose that $q_k = tq_0 \cdot r_{k-1} + q_1 \cdot r_k$ and $q_{k+1} = tq_0 \cdot r_k + q_1 \cdot r_{k+1}$ for some $k \geq 1$. Then

$$\begin{aligned} q_{k+2} = sq_{k+1} + tq_k &= s(tq_0 \cdot r_k + q_1 \cdot r_{k+1}) + t(tq_0 \cdot r_{k-1} + q_1 \cdot r_k) \\ &= tq_0(sr_k + tr_{k-1}) + q_1(sr_{k+1} + tr_k) = tq_0 \cdot r_{k+1} + q_1 \cdot r_{k+2}, \end{aligned}$$

which is (12.1.6) with $k+2$ in place of $n$. Thus (12.1.6) holds for all $n \geq 1$ by induction. □

**Example.** The *Lucas sequence* is defined by $L_n = L_{n-1} + L_{n-2}$ for $n \geq 2$, with $L_0 = 2$ and $L_1 = 1$. (This sequence begins: $2, 1, 3, 4, 7, 11, 18, 29, \ldots$.) By Theorem 12.1.11, then $L_n = 2F_{n-1} + F_n$ for every $n \geq 1$, where $F_n$ is the $n$-th term of the Fibonacci sequence. ◊

## 12.2 Periodicity of Quadratic Recursive Sequences

If each term of the Fibonacci sequence is replaced by its remainder on division by $m = 2$, we obtain the following sequence of elements of $\mathbb{Z}_2$.

$$F_n \bmod 2: \quad 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, \ldots.$$

Note that we do not need to calculate this sequence by dividing each $F_n$ by 2. Beginning with 0 and 1, we can merely add two consecutive terms of the sequence in $\mathbb{Z}_2$, where $1 + 1 = 0$, to obtain the next term. Likewise, we find:

$F_n \bmod 3$: $0, 1, 1, 2, 0, 2, 2, 1, 0, 1, 1, 2, 0, 2, 2, 1, 0, 1, 1, 2, 0, 2, 2, 1, 0, 1, \ldots$

$F_n \bmod 4$: $0, 1, 1, 2, 3, 1, 0, 1, 1, 2, 3, 1, 0, 1, 1, 2, 3, 1, 0, 1, 1, 2, 3, 1, 0, 1, \ldots$

$F_n \bmod 5$: $0, 1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1, 0, 1, 1, 2, 3, 0, \ldots$

$F_n \bmod 6$: $0, 1, 1, 2, 3, 5, 2, 1, 3, 4, 1, 5, 0, 5, 5, 4, 3, 1, 4, 5, 3, 2, 5, 1, 0, 1, \ldots$

$F_n \bmod 7$: $0, 1, 1, 2, 3, 5, 1, 6, 0, 6, 6, 5, 4, 2, 6, 1, 0, 1, 1, 2, 3, 5, 1, 6, 0, 6, \ldots$

If there is a value of $\ell > 0$ for which $F_\ell \equiv 0 \pmod{m}$ and $F_{\ell+1} \equiv 1 \pmod{m}$, then $F_n$ modulo $m$ repeats the pattern for $0 \leq n < \ell$ indefinitely. Such an $\ell$ exists for each $m$ considered above, and the following proposition ensures that the same is true for all positive integers $m$. We state this result for an arbitrary solution of a second-order recurrence relation.

**Proposition 12.2.1.** *Let $r_0$ and $r_1$ be integers, and let $r_n = sr_{n-1} + tr_{n-2}$ for $n \geq 2$, where $s$ and $t$ are fixed integers. If $m$ is a positive integer and $\gcd(m, t) = 1$, then there is an $\ell > 0$ so that $r_{\ell+n} \equiv r_n \pmod{m}$ for all $n \geq 0$.*

*Proof.* The set of pairs of congruence classes modulo $m$ is finite, so there is some $j \geq 0$ and $\ell > 0$ with $r_{\ell+j} \equiv r_j \pmod{m}$ and $r_{\ell+j+1} \equiv r_{j+1} \pmod{m}$. We can assume that $j$ is as small as possible so that this occurs. If $j$ is positive, we then have that

$$tr_{\ell+j-1} \equiv r_{\ell+j+1} - sr_{\ell+j} \equiv r_{j+1} - sr_j \equiv tr_{j-1} \pmod{m}.$$

If $\gcd(m, t) = 1$, then $r_{\ell+j-1} \equiv r_{j-1} \pmod{m}$, contradicting the definition of $j$. So $j = 0$, and with $r_\ell \equiv r_0 \pmod{m}$ and $r_{\ell+1} \equiv r_1 \pmod{m}$, then we see by induction that $r_{\ell+n} \equiv r_n \pmod{m}$ for all $n \geq 0$. □

In the remainder of this section, let $r_n$ be a quadratic recursive sequence with characteristic polynomial $f(x)$, as in (12.1.1). In particular, we again assume that the initial terms of the sequence are $r_0 = 0$ and $r_1 = 1$, and we often simplify our terminology by saying that $r_n$ is the quadratic sequence defined by $f(x)$.

**Definition.** Let $r_n$ be the quadratic sequence defined by $x^2 - sx - t$. Let $m$ be a positive integer with $\gcd(m, t) = 1$. If $\ell$ is the smallest positive integer for which $r_\ell \equiv 0 \pmod{m}$ and $r_{\ell+1} \equiv 1 \pmod{m}$, then we say that $\ell$ is the *order* of $r_n$ modulo $m$, and write $\ell = \mathrm{ord}_m(r_n)$. If $k$ is the smallest positive integer for which $r_k \equiv 0 \pmod{m}$, we say that $k$ is the *suborder* of $r_n$ modulo $m$, and write $k = \mathrm{sub}_m(r_n)$.

By Proposition 12.2.1, both $\mathrm{sub}_m(r_n)$ and $\mathrm{ord}_m(r_n)$ must exist if $r_n$ is a quadratic recursive sequence defined by $f(x) = x^2 - sx - t$ and $\gcd(m, t) = 1$.

**Example.** For the Fibonacci sequence $F_n$, our calculations above show that $\mathrm{ord}_3(F_n) = 8$ and $\mathrm{sub}_3(F_n) = 4$, while $\mathrm{ord}_4(F_n) = 6 = \mathrm{sub}_4(F_n)$. ◊

For the next proposition, recall that if $\gcd(a, m) = 1$, then there is a smallest positive integer $t$ so that $a^t \equiv 1 \pmod{m}$ (see Exercise 0.1.7). We call $t$ the *order* of $a$ modulo $m$, and write $\mathrm{ord}_m(a) = t$.

**Proposition 12.2.2.** *Let $r_n$ be the quadratic sequence defined by $x^2 - sx - t$, and let $m$ be a positive integer with $\gcd(m, t) = 1$. Let $k$ be the suborder of $r_n$ modulo $m$, and let $a = r_{k+1}$. Then $\gcd(a, m) = 1$, so that $\mathrm{ord}_m(a)$ exists, and $\mathrm{ord}_m(r_n) = \mathrm{sub}_m(r_n) \cdot \mathrm{ord}_m(a)$.*

*Proof.* If $a = r_{k+1}$, then $r_k \equiv ar_0 \pmod{m}$ and $r_{k+1} \equiv ar_1 \pmod{m}$, and it follows inductively that $r_{k+n} \equiv ar_n \pmod{m}$ for all $n \geq 0$. Now write the order of $r_n$ modulo $m$ as $\ell = kq + d$ with $q \geq 1$ and $0 \leq d < k$. We find that $r_\ell \equiv a^q r_d \equiv 0 \pmod{m}$ and $r_{\ell+1} \equiv a^q r_{d+1} \equiv 1 \pmod{m}$. The second congruence shows that $a^q$ must be relatively prime to $m$, so that $\gcd(a, m) = 1$, and then the first implies that $r_d \equiv 0 \pmod{m}$. We must conclude that $d = 0$ to avoid contradicting the definition of $k = \mathrm{sub}_m(r_n)$. Therefore $\ell = kq$ and $a^q \equiv 1 \pmod{m}$. Furthermore, to avoid contradicting the definition of $\ell = \mathrm{ord}_m(r_n)$, we see that $q$ must be the smallest positive integer for which this is true, that is, $q = \mathrm{ord}_m(a)$. □

**Finite Quadratic Extension Fields.** We will now restrict our attention to consideration of the order and suborder of a quadratic sequence $r_n$ modulo $m$ when $m = p$ is prime. We can view the terms $r_n \bmod p$ as elements of a field $\mathbb{F}_p$ with $p$ elements. (We take $\mathbb{F}_p$ to be the set of congruence classes modulo $p$, which we have also denoted as $\mathbb{Z}_p$.) If $r_n$ is defined by $f(x) = x^2 - sx - t$ for some

integers $s$ and $t$, we will assume that $p$ does not divide $t$, that is, $t \neq 0$ in $\mathbb{F}_p$, so that the order and suborder of $r_n$ modulo $p$ are defined. If $p = 2$, so that $t = 1$, then there are only two possibilities for $f(x)$.

(1) If $s = 0$, then $f(x) = x^2 - 1 = (x-1)^2$. Here $r_n = r_{n-2}$ for $n > 1$ and we find that $\mathrm{sub}_2(r_n) = 2 = \mathrm{ord}_2(r_n)$.

(2) If $s = 1$, then $r_n$ is the Fibonacci sequence modulo 2, with $\mathrm{sub}_2(r_n) = 3 = \mathrm{ord}_2(r_n)$.

In what follows, we restrict our attention to quadratic sequences modulo *odd* primes $p$.

As in §12.1, we will see that patterns in these sequences can be described using powers of the roots of the characteristic polynomial of $r_n$. It is convenient to view these powers modulo $p$ as well, by working within a *quadratic extension field* $\mathbb{E} = \mathbb{E}_p$ of $\mathbb{F}_p$, that is, a field with $p^2$ elements. By properties of these extension fields listed in the introduction to Part Five, we know that the characteristic polynomial of a quadratic recursive sequence $r_n$ factors in $\mathbb{E}[x]$. Our next theorem shows that the order and suborder of $r_n$ modulo $p$ can be calculated from this factorization.

**Theorem 12.2.3.** *Let $f(x) = x^2 - sx - t$ in $\mathbb{F}_p[x]$, and suppose that $f(x) = (x-u)(x-v)$ for some $u$ and $v$ in $\mathbb{E}$, a quadratic extension field of $\mathbb{F}_p$. Let $r_n$ be the quadratic recursive sequence with characteristic polynomial $f(x)$. Then for all $n \geq 1$,*

$$r_n = \sum_{i=0}^{n-1} u^{n-1-i}v^i = u^{n-1} + u^{n-2}v + \cdots + uv^{n-2} + v^{n-1}. \tag{12.2.1}$$

*Thus the following are true if $t \neq 0$ in $\mathbb{F}_p$.*

(1) *If $u = v$, then $r_n = 0$ if and only if $p$ divides $n$.*

(2) *If $u \neq v$, then $r_n = 0$ if and only if $u^n = v^n$, and $r_n = 0$ and $r_{n+1} = 1$ if and only if $u^n = 1 = v^n$.*

*Proof.* Comparing coefficients of $f(x) = x^2 - sx - t = (x-u)(x-v)$, we have that $s = u + v$ and $t = -uv$. Equation (12.2.1) holds for $n = 1$, since the sum has just one term in that case, $u^0v^0 = 1$. For $n = 2$, we have that $r_2 = sr_1 + tr_0 = s = u + v = \sum_{i=0}^{1} u^{1-i}v^i$. So now let $n$ be larger than 1, and

suppose that we have established (12.2.1) for $r_n$ and $r_{n-1}$. Then

$$\begin{aligned} r_{n+1} = sr_n + tr_{n-1} &= (u+v)\sum_{i=0}^{n-1} u^{n-1-i}v^i - uv\sum_{i=0}^{n-2} u^{n-2-i}v^i \\ &= \sum_{i=0}^{n-1}(u^{n-i}v^i + u^{n-1-i}v^{i+1}) - \sum_{i=0}^{n-2} u^{n-1-i}v^{i+1} \\ &= uv^{n-1} + v^n + \sum_{i=0}^{n-2} u^{n-i}v^i = \sum_{i=0}^{n} u^{n-i}v^i, \end{aligned}$$

which is (12.2.1) with $n+1$ in place of $n$. Thus the equation is true for all $n \geq 1$ by induction.

Now if $u = v$, we have

$$r_n = \sum_{i=0}^{n-1} u^{n-1-i}u^i = \sum_{i=0}^{n-1} u^{n-1} = nu^{n-1}$$

for $n \geq 1$. If $t \neq 0$ in $\mathbb{F}_p$, then $u^{n-1}$ cannot equal zero in $\mathbb{E}$. Therefore $r_n = 0$ if and only if $n = 0$ in $\mathbb{F}_p$, that is, $p$ divides $n$. On the other hand, (12.2.1) implies that

$$(u-v)r_n = (u-v)(u^{n-1} + u^{n-2}v + \cdots + uv^{n-2} + v^{n-1}) = u^n - v^n,$$

and if $u \neq v$, it follows that $r_n = 0$ if and only if $u^n = v^n$. Assuming that this is the case, then

$$(u-v)r_{n+1} = u^{n+1} - v^{n+1} = u^n u - v^n v = u^n(u-v) = v^n(u-v),$$

so that $r_n = 0$ and $r_{n+1} = 1$ if and only if $u^n$ and $v^n$ both equal 1. □

Let $p$ be an odd prime, and let $f(x) = x^2 - sx - t = (x-u)(x-v)$, with $s$ and $t \neq 0$ elements of $\mathbb{F}_p$, and with $u$ and $v$ in $\mathbb{E}$. Then the discriminant of $f(x)$ is

$$\Delta = s^2 + 4t = (u+v)^2 - 4uv = (u-v)^2.$$

If $p$ divides $\Delta$, then $u$ must equal $v$, and this common value is an element of $\mathbb{F}_p$. (Specifically, we find that $s = 2u$, so that $u = 2^{-1}s$ in $\mathbb{F}_p$.) If $\left(\frac{\Delta}{p}\right) = 1$, then $u$ and $v$ are distinct nonzero elements of $\mathbb{F}_p$, while if $\left(\frac{\Delta}{p}\right) = -1$, then $u$ and $v$ are distinct elements of $\mathbb{E}$, not in $\mathbb{F}_p$. We can make some general statements about the suborder and order of a quadratic sequence modulo an odd prime $p$, based on these possibilities.

**Corollary 12.2.4.** *Let $p$ be an odd prime, and let $f(x) = x^2 - sx - t$ with $s$ and $t$ in $\mathbb{F}_p$, and $t \neq 0$. Suppose that $p$ divides $\Delta = s^2 + 4t$, so that $f(x) = (x-a)^2$ for some*

*$a \neq 0$ in $\mathbb{F}_p$. Let $r_n$ be the quadratic sequence defined by $f(x)$. Then the suborder of $r_n$ modulo $p$ is $\mathrm{sub}_p(r_n) = p$, and the order of $r_n$ modulo $p$ is $\mathrm{ord}_p(r_n) = p \cdot \mathrm{ord}_p(a)$.*

*Proof.* The first claim follows immediately from statement (1) in Theorem 12.2.3. Note in this case that $r_{p+1} = (p+1)a^p = a^p = a$ in $\mathbb{F}_p$, since $a^{p-1} = 1$ for every nonzero element $a$ in $\mathbb{F}_p$. By Proposition 12.2.2, then the order of $r_n$ modulo $p$ is $p \cdot \mathrm{ord}_p(a)$. □

**Example.** If $f(x) = x^2 - x - 1$, then $\Delta = 5$, and we find that $f(x) = (x-3)^2$ in $\mathbb{F}_5[x]$. Since $\mathrm{ord}_5(3) = 4$, we conclude that the Fibonacci sequence has suborder 5 and order $5 \cdot 4 = 20$ modulo $p = 5$. This is confirmed by calculations at the beginning of this section. ◊

**Corollary 12.2.5.** *Let $p$ be an odd prime, and let $f(x) = x^2 - sx - t$ with $s$ and $t$ in $\mathbb{F}_p$, and $t \neq 0$. Let $\Delta = s^2 + 4t$ and suppose that $\left(\frac{\Delta}{p}\right) = 1$, so that $f(x) = (x-a)(x-b)$ for some distinct nonzero elements $a$ and $b$ in $\mathbb{F}_p$. If $r_n$ is the quadratic sequence defined by $f(x)$, then the suborder of $r_n$ modulo $p$ is $\mathrm{sub}_p(r_n) = \mathrm{ord}_p(ab^{-1})$ and the order of $r_n$ modulo $p$ is $\mathrm{ord}_p(r_n) = \mathrm{lcm}(\mathrm{ord}_p(a), \mathrm{ord}_p(b))$.*

Corollary 12.2.5 implies that when $\left(\frac{\Delta}{p}\right) = 1$, then $\mathrm{sub}_p(r_n)$ and $\mathrm{ord}_p(r_n)$ both divide $p - 1$.

*Proof.* Statement (2) of Theorem 12.2.3 implies that $\mathrm{sub}_p(r_n)$ is the smallest $n > 0$ for which $a^n = b^n$. But $a^n = b^n$ if and only if $a^n(b^{-1})^n = (ab^{-1})^n = 1$, so that $n = \mathrm{ord}_p(ab^{-1})$. Likewise, $\mathrm{ord}_p(r_n)$ is the smallest $n > 0$ for which $a^n = 1 = b^n$. Since $a^n = 1$ if and only if $n$ is a multiple of the order of $a$ modulo $p$, and similarly for $b$, we find that $n = \mathrm{lcm}(\mathrm{ord}_p(a), \mathrm{ord}_p(b))$. □

**Example.** Since $\left(\frac{5}{11}\right) = \left(\frac{11}{5}\right) = 1$, we know that $f(x) = x^2 - x - 1$ factors in $\mathbb{F}_{11}[x]$, and we can verify that $f(x) = (x-4)(x-8)$. We find that $\mathrm{ord}_{11}(4) = 5$ and $\mathrm{ord}_{11}(8) = 10$, with $4 \cdot 8^{-1} = 4 \cdot 7 = 6$ also of order 10. The Fibonacci sequence modulo 11,

$$F_n \bmod 11 : \quad 0, 1, 1, 2, 3, 5, 8, 2, 10, 1, 0, 1, 1, 2, \ldots,$$

has suborder and order both equal to 10. ◊

**Corollary 12.2.6.** *Let $p$ be an odd prime, and let $f(x) = x^2 - sx - t$ with $s$ and $t$ in $\mathbb{F}_p$, and $t \neq 0$. Let $\Delta = s^2 + 4t$ and suppose that $\left(\frac{\Delta}{p}\right) = -1$. Let $v$ be a root of $f(x)$ in a quadratic extension field $\mathbb{E}$ of $\mathbb{F}_p$. If $r_n$ is the quadratic sequence defined by $f(x)$, then the suborder of $r_n$ modulo $p$ equals the order of $v^{p-1}$ as an element*

*of the group $\mathbb{E}^\times$ of units in $\mathbb{E}$, while the order of $r_n$ modulo $p$ equals the order of $v$ in $\mathbb{E}^\times$.*

*Proof.* If $\left(\frac{\Delta}{p}\right) = -1$, then $f(x)$ is irreducible in $\mathbb{F}_p[x]$, but factors as $f(x) = (x-u)(x-v)$ in $\mathbb{E}[x]$. Since $v$ is not an element of $\mathbb{F}_p$, then $v^p \neq v$, but $v^p$ is a root of $f(x)$. (See property (4) of finite fields listed in the introduction to Part Five.) We must conclude that $v^p = u$.

Now statement (2) of Theorem 12.2.3 again applies, so that $\text{sub}_p(r_n)$ is the smallest $n > 0$ for which $u^n = v^n$, in which case $(uv^{-1})^n = (v^{p-1})^n = 1$. This is by definition the order of $v^{p-1}$ in $\mathbb{E}^\times$. Likewise, $\text{ord}_p(r_n)$ is the smallest $n > 0$ for which $u^n = 1 = v^n$. Since $\mathbb{E}^\times$ has $p^2 - 1$ elements, and $\gcd(p, p^2-1) = 1$, it follows that $u = v^p$ has the same order in $\mathbb{E}^\times$ as does $v$. So we conclude that the order of $r_n$ modulo $p$ is the same as the order of $v$ in $\mathbb{E}^\times$. □

Note that $(v^{p-1})^{p+1} = v^{p^2-1}$ must equal 1, since $\mathbb{E}^\times$ has $p^2 - 1$ elements. It follows that the suborder of $r_n$ modulo $p$ is a divisor of $p+1$ when $\left(\frac{\Delta}{p}\right) = -1$.

**Example.** Since $\left(\frac{5}{13}\right) = \left(\frac{13}{5}\right) = \left(\frac{3}{5}\right) = -1$, the polynomial $f(x) = x^2 - x - 1$ is irreducible in $\mathbb{F}_{13}[x]$. The Fibonacci sequence modulo $p = 13$ begins

$$F_n \bmod 13 : \quad 0, 1, 1, 2, 3, 5, 8, 0, 8, 8, 3, 11, 1, 12, 0, \ldots,$$

with suborder $k = 7$, a divisor of $p+1$. Since $F_8 \equiv 8 \pmod{13}$, the order of $F_n$ modulo 13 is $\text{sub}_{13}(F_n) \cdot \text{ord}_{13}(8) = 7 \cdot 4 = 28$. ◊

We summarize our results with the following corollary. The proofs of these claims appear among the various theorems and corollaries in this subsection.

**Corollary 12.2.7.** *Let $r_n$ be the quadratic recursive sequence with characteristic polynomial $f(x) = x^2 - sx - t$, and let $\Delta = s^2 + 4t$. Let $p$ be an odd prime number that does not divide $t$. Then*

$$\text{sub}_p(r_n) \textit{ divides } \begin{cases} p, & \textit{if } p \textit{ divides } \Delta, \\ p-1, & \textit{if } \left(\frac{\Delta}{p}\right) = 1, \\ p+1, & \textit{if } \left(\frac{\Delta}{p}\right) = -1, \end{cases}$$

*and*

$$\text{ord}_p(r_n) \textit{ divides } \begin{cases} p(p-1), & \textit{if } p \textit{ divides } \Delta, \\ p-1, & \textit{if } \left(\frac{\Delta}{p}\right) = 1, \\ (p+1)(p-1), & \textit{if } \left(\frac{\Delta}{p}\right) = -1. \end{cases}$$

**Example.** Let $r_n = r_{n-1} - r_{n-2}$ for $n \geq 2$, with $r_0 = 0$ and $r_1 = 1$. This sequence begins:

$$0, 1, 1, 0, -1, -1, 0, 1, 1, 0, -1, -1, 0, \ldots .$$

Here the pattern of the first six terms continues indefinitely, so that this sequence is periodic modulo every odd prime $p$, with $\text{sub}_p(r_n) = 3$ and $\text{ord}_p(r_n) = 6$. (Since $1 \equiv -1 \pmod 2$, the sequence has order 3 modulo $p = 2$.) Note that the characteristic polynomial of $r_n$ is $f(x) = x^2 - x + 1$, so that $\Delta = -3$, with $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$ for every odd prime $p$. We leave it to the reader to verify that our results are consistent with Corollary 12.2.7. ◊

**Exercise 12.2.1.** In each part, a characteristic polynomial $f(x)$ of a quadratic sequence $r_n$ is given. Find the order of $r_n$ modulo $p = 3$, modulo $p = 5$, and modulo $p = 7$. Show that your results are consistent with Corollary 12.2.7 and other results from this section.

(a) $f(x) = x^2 + 1$.

(b) $f(x) = x^2 + 2$.

(c) $f(x) = x^2 + x + 1$.

(d) $f(x) = x^2 + x + 2$.

(e) $f(x) = x^2 + 2x + 1$.

(f) $f(x) = x^2 + 2x + 2$.

(g) $f(x) = x^2 - x + 2$.

(h) $f(x) = x^2 + x - 2$.

(i) $f(x) = x^2 - 2x - 1$.

(j) $f(x) = x^2 - 2x - 2$.

## 12.3 Suborder Functions

In §12.2, we established formulas for the order and suborder of a quadratic recursive sequence $r_n$ modulo a prime number $p$, based on factorization properties of the characteristic polynomial of $r_n$ in $\mathbb{F}_p[x]$. The application of these formulas, however, requires calculations of orders of elements in $\mathbb{F}_p^\times$, or in $\mathbb{E}^\times$, where $\mathbb{E}$ is a quadratic extension field of $\mathbb{F}_p$, which are likely to be at least as difficult computationally as direct calculation of the order or suborder of a quadratic sequence. In this section and the next, we introduce a different method of calculating the suborder of an arbitrary quadratic sequence modulo a prime number. It will be

convenient in this section to write a field containing $p$ elements, where $p$ is an odd prime, as

$$\mathbb{F}_p = \left\{0, 1, -1, \ldots, \frac{p-1}{2}, -\frac{p-1}{2}\right\}.$$

For example, $\mathbb{F}_{11} = \{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$, with 6 written as $-5$, and so forth.

**Proposition 12.3.1.** *Let $\mathbb{E}$ be a quadratic extension field of $\mathbb{F}_p$ for some odd prime $p$. Then for every $c$ in $\mathbb{F}_p$, there is a unique pair of inverse elements $z$ and $z^{-1}$ (not necessarily distinct) in $\mathbb{E}^\times$ so that $c = z + z^{-1}$.*

*Proof.* The quadratic polynomial $g(x) = x^2 - cx + 1$ must factor in $\mathbb{E}[x]$, say as $(x-v)(x-z)$. Comparing coefficients, we have $vz = 1$, so that $v = z^{-1}$, and then $c = v + z = z + z^{-1}$. Conversely, if $c = z + z^{-1}$ for some $z$ in $\mathbb{E}$, then $cz = z^2 + 1$ and $cz^{-1} = 1 + (z^{-1})^2$, so that $z$ and $z^{-1}$ are roots of $g(x)$. The factorization of $g(x)$ in $\mathbb{E}[x]$ is unique, so this pair of inverses is uniquely determined by $c$. □

**Definition.** Let $\mathbb{E}$ be a quadratic extension field of $\mathbb{F}_p$ for some odd prime $p$. If $c$ is an element of $\mathbb{F}_p$ and $c = z + z^{-1}$ for some $z$ in $\mathbb{E}$, define $\mathrm{sub}_p(c)$ to equal the order of $z$ in $\mathbb{E}^\times$. We refer to $\mathrm{sub}_p(c)$ as the *suborder* of $c$ modulo $p$, defining in this way the *suborder function* on $\mathbb{F}_p$.

The discriminant of $g(x) = x^2 - cx + 1$ is $\Delta = c^2 - 4 = (c-2)(c+2)$. If $c = 2$, then $z = 1 = z^{-1}$, while if $c = -2$, then $z = -1 = z^{-1}$. So $\mathrm{sub}_p(2) = 1$ and $\mathrm{sub}_p(-2) = 2$. If $c \neq \pm 2$ in $\mathbb{F}_p$, then $z \neq z^{-1}$, and these inverse elements have the same order in $\mathbb{E}^\times$. In that case, Theorem 12.2.3 shows that $\mathrm{sub}_p(c)$ is the same as the order of the quadratic sequence defined by $g(x) = x^2 - cx + 1$. (It follows that $\mathrm{sub}_p(c)$ does not depend on our choice of the field $\mathbb{E}$, nor on which element in the pair of inverses we label as $z$.) We use this fact to calculate certain values of $\mathrm{sub}_p(c)$ which hold for every prime $p$.

**Proposition 12.3.2.** *Let $p$ be an odd prime, and let $\mathrm{sub}_p(c)$ be the suborder function on $\mathbb{F}_p$, as defined above. Then the following statements are true.*

(1) $\mathrm{sub}_p(c) = 1$ *if and only if* $c \equiv 2 \pmod{p}$.

(2) $\mathrm{sub}_p(c) = 2$ *if and only if* $c \equiv -2 \pmod{p}$.

(3) $\mathrm{sub}_p(c) = 4$ *if and only if* $c \equiv 0 \pmod{p}$.

(4) $\mathrm{sub}_p(c) = 3$ *if and only if* $c \equiv -1 \pmod{p}$ *and* $p > 3$.

(5) $\mathrm{sub}_p(c) = 6$ *if and only if* $c \equiv 1 \pmod{p}$ *and* $p > 3$.

Note that $-1 = 2$ and $1 = -2$ in $\mathbb{F}_3$, so that $\mathrm{sub}_3(-1) = 1$ and $\mathrm{sub}_3(1) = 2$ by statements (1) and (2).

*Proof.* Let $\mathbb{E}$ be a quadratic extension field of $\mathbb{F}_p$. The group of units of $\mathbb{E}$ is cyclic of order $p^2-1$, say with $w$ as a generator. So $1 = w^0$ and $-1 = w^{(p^2-1)/2}$ are the only elements of $\mathbb{E}^\times$ of order one or two. Each is its own inverse, so $1+1=2$ and $-1+(-1)=-2$ can be the only elements of $\mathbb{F}_p$ with suborder one or two, respectively. This establishes (1) and (2).

For (3), note that 4 divides $p^2-1$, and we find that $z = w^{(p^2-1)/4}$ and $v = w^{3(p^2-1)/4}$ are the only elements of $\mathbb{E}^\times$ with order four. Here $v = z^{-1}$, so there can be only one element $c = z + z^{-1}$ in $\mathbb{F}_p$ having suborder four. But if $c = 0$, the quadratic sequence defined by $x^2 - cx + 1$ begins $0, 1, 0, -1, 0, 1, \ldots$, with order four.

For (4) and (5), note that if $p > 3$, then 3 and 6 divide $p^2-1$. We find a single pair of inverse elements of order three in $\mathbb{E}^\times$, and a single pair of inverse elements of order six in $\mathbb{E}^\times$, so there is only one element of suborder three and only one element of suborder six in $\mathbb{F}_p$ when $p > 3$. But for $c = -1$ and $c = 1$, we find that the sequences defined by $x^2 - cx + 1$ are

$$0, 1, -1, 0, 1, \ldots \qquad \text{and} \qquad 0, 1, 1, 0, -1, -1, 0, 1, \ldots,$$

with order three and order six, respectively. □

The following definition and theorem connect the suborder function to suborders of quadratic sequences.

**Definition.** Let $p$ be an odd prime, and let $f(x) = x^2 - sx - t$ for some integers $s$ and $t$ with $t$ not divisible by $p$. Then we define the *suborder number* of $f(x)$ modulo $p$ to be the element $c_p(f) = s^2(-t)^{-1} - 2$ in the field $\mathbb{F}_p$.

**Theorem 12.3.3.** *Let $p$ be an odd prime, and let $f(x) = x^2 - sx - t$ with $t$ not divisible by $p$. Let $r_n$ be the quadratic recursive sequence with characteristic polynomial $f(x)$. That is, let $r_n = sr_{n-1} + tr_{n-2}$ for $n > 1$, with $r_0 = 0$ and $r_1 = 1$. Let $c = c_p(f)$ be the suborder number of $f(x)$ modulo $p$. If $c \neq 2$, then the suborder of $r_n$ modulo $p$ is the same as the suborder of $c$ modulo $p$, that is, $\mathrm{sub}_p(r_n) = \mathrm{sub}_p(c)$. On the other hand, if $c = 2$, then the suborder of $r_n$ modulo $p$ equals $p$.*

*Proof.* Notice that if $c = s^2(-t)^{-1} - 2$, so that $s^2 = (c+2)(-t)$, then the discriminant of $f(x)$ is $\Delta = s^2 + 4t = (c-2)(-t)$. If $c = 2$, then $f(x)$ has a repeated root modulo $p$, and in that case, Theorem 12.2.3 implies that $\mathrm{sub}_p(r_n) = p$. On the other hand, if $c \neq 2$, then $f(x) = (x-u)(x-v)$ for some $u \neq v$ in $\mathbb{E}$, since then $\Delta \neq 0$. Then $s = u + v$ and $-t = uv$, so that

$$\begin{aligned} c = s^2(-t)^{-1} - 2 &= (u+v)^2(uv)^{-1} - 2 \\ &= (u^2 + 2uv + v^2)(u^{-1}v^{-1}) - 2 = uv^{-1} + u^{-1}v. \end{aligned}$$

Since $u \neq v$, the suborder of $r_n$ modulo $p$ is the order of $uv^{-1}$ in $\mathbb{E}^\times$, as in Theorem 12.2.3. But since $c = z + z^{-1}$ with $z = uv^{-1}$, the order of $uv^{-1}$ is also equal to $\mathrm{sub}_p(c)$. □

If $c \neq -2$, then $f(x) = x^2 + (c+2)x + (c+2)$ is a polynomial with $c(f) = c$. So every $c$ in $\mathbb{F}_p$ equals $c_p(f)$ for some polynomial in $\mathbb{F}_p[x]$. An implication of Theorem 12.3.3 is that if $k \neq 0$ in $\mathbb{F}_p$, then the quadratic sequences defined by $f(x) = x^2 - sx - t$ and $g(x) = x^2 - ksx - k^2t$ have the same suborder. We can see this directly also. If $r_n = sr_{n-1} + tr_{n-2}$ and $r'_n = ksr'_{n-1} + k^2tr'_{n-2}$, with $r_0 = 0 = r'_0$ and $r_1 = 1 = r'_1$, then $r'_n = k^{n-1}r_n$ for all $n$. Since $k^{n-1} \neq 0$, then $r'_n = 0$ if and only if $r_n = 0$.

**Example.** For the Fibonacci sequence, defined by $f(x) = x^2 - x - 1$, we have that $c = 1^2(-1)^{-1} - 2 = -3$ for all primes $p$. If $p = 7$, for example, we find that $\mathrm{sub}_7(-3) = 8$, since in $\mathbb{F}_7$ the quadratic sequence defined by $x^2 + 3x + 1$ begins $0, 1, -3, 1, 0, -1, 3, -1, 0, 1, \ldots$, with order eight. ◊

**Properties of Suborder Functions.** Theorem 12.3.3 associates an element $c$ in $\mathbb{F}_p$ to a polynomial $f(x) = x^2 - sx - t$, and, if $c \neq 2$, tells us that $\mathrm{sub}_p(c)$ equals the suborder modulo $p$ of the quadratic sequence $r_n$ defined by $f(x)$. But to this point, aside from a few special cases, our only methods of computing $\mathrm{sub}_p(c)$ require calculations in a quadratic extension field $\mathbb{E}$, or calculation of the order modulo $p$ of another quadratic sequence, which has no particular advantage over merely considering $r_n$ itself. Our goal in the remainder of this section and in §12.4 is to establish some general facts about the suborder function that make calculation of $\mathrm{sub}_p(c)$, for an individual $c$ or for all $c$ in $\mathbb{F}_p$, practical for relatively small primes. We begin with the following observation.

**Proposition 12.3.4.** *Let $p$ be an odd prime and let $c$ be an element of $\mathbb{F}_p$. Let $m = \mathrm{sub}_p(c)$ and $n = \mathrm{sub}_p(-c)$. Then the following are true.*

(1) *If $m$ is odd, then $n = 2m$.*

(2) *If $m \equiv 2 \pmod 4$, then $n = \frac{m}{2}$.*

(3) *If 4 divides $m$, then $n = m$.*

*Proof.* Note that if $c = z + z^{-1}$ for some $z$ in a quadratic extension field $\mathbb{E}$ of $\mathbb{F}_p$, then $-c = -z - z^{-1} = (-z) + (-z)^{-1}$. The suborder of $c$ modulo $p$ is the order of $z$ in $\mathbb{E}^\times$, and likewise the suborder of $-c$ modulo $p$ is the order of $-z$ in $\mathbb{E}^\times$. Let $m$ and $n$ be these respective orders.

If $z^m = 1$, then $(-z)^{2m} = (-1)^{2m}(z^m)^2 = 1$. It follows that $n$ divides $2m$. In the same way, since $z^{2n} = (-1)^{2n}((-z)^n)^2 = 1$, then $m$ divides $2n$. So we see that $n = 2m$, $n = m$, or $n = \frac{m}{2}$ (possible only when $m$ is even). Now we consider three cases as above.

(1) If $m$ is odd, then $(-z)^m = (-1)^m z^m = -1$. So $n \neq m$, and we must conclude that $n = 2m$.

(2) If $m = 2k$ with $k$ odd, then $z^k = -1$ since $w = z^k$ satisfies $w^2 = 1$, but $w$ is not itself 1. (The equation $x^2 - 1 = (x-1)(x+1) = 0$ has at most two solutions in a field.) But now $(-z)^k = (-1)^k z^k = -(-1) = 1$, and so $n = k = \frac{m}{2}$.

(3) If 4 divides $m$, then $n$ must also be even. But now note that $(-z)^m = z^m = 1$ and $z^n = (-1)^n(-z)^n = 1$. It follows that $n$ divides $m$ and $m$ divides $n$, and so $n = m$.

Thus we obtain the claimed results in every case. □

The following theorem places additional restrictions on the possibilities for the suborder of a given $c$ modulo a prime $p$.

**Theorem 12.3.5.** *Let $p$ be an odd prime and let $c \neq \pm 2$ be an element of $\mathbb{F}_p$, with $m = \mathrm{sub}_p(c)$. Let $e_2(m)$ denote the exponent of 2 in $m$. Then the following are true.*

(1) *If $\left(\frac{c+2}{p}\right) = \left(\frac{c-2}{p}\right)$, then $m$ divides $p-1$, with $e_2(m) < e_2(p-1)$ if and only if $\left(\frac{c+2}{p}\right) = 1$.*

(2) *If $\left(\frac{c+2}{p}\right) = -\left(\frac{c-2}{p}\right)$, then $m$ divides $p+1$, with $e_2(m) < e_2(p+1)$ if and only if $\left(\frac{c+2}{p}\right) = 1$.*

*Proof.* Consider the polynomial $f(x) = x^2 + (c+2)x + (c+2)$, for which $c_p(f) = c$ and $\Delta = \Delta(f) = (c+2)^2 - 4(c+2) = (c+2)(c-2)$. If $c \neq \pm 2$ in $\mathbb{F}_p$, then $f(x)$ factors as $(x-u)(x-v)$ for some $u \neq v$ in $\mathbb{E}$, a quadratic extension field of $\mathbb{F}_p$. We saw in the proof of Theorem 12.3.3 that in this case, $\mathrm{sub}_p(c)$ is the same as the order of $uv^{-1}$ in $\mathbb{E}^\times$. Note also that $uv = c+2$, by comparing coefficients in the two expressions for $f(x)$. We consider two cases.

Suppose first that $\left(\frac{\Delta}{p}\right) = 1$, so that $u$ and $v$ are nonzero elements of $\mathbb{F}_p$. Let $g$ be a generator of $\mathbb{F}_p^\times$, a cyclic group with $p-1$ elements. We can write $uv^{-1} = g^k$ for some integer $k$, and in that case the order of $uv^{-1}$ in $\mathbb{F}_p^\times$, and in $\mathbb{E}^\times$, is $m = \frac{p-1}{\gcd(k,p-1)}$. Since $p-1$ is even, $e_2(m) = e_2(p-1)$ if and only if $k$ is odd. Now $c+2 = uv = uv^{-1} \cdot v^2$, so that $\left(\frac{c+2}{p}\right) = \left(\frac{uv^{-1}}{p}\right)\left(\frac{v}{p}\right)^2 = \left(\frac{g}{p}\right)^k$ since $u$ and $v$ are elements of $\mathbb{F}_p$. A generator of $\mathbb{F}_p^\times$ cannot be a square of an

element of $\mathbb{F}_p^\times$, and so $\left(\frac{g}{p}\right) = -1$. We conclude that $\left(\frac{c+2}{p}\right) = 1 = \left(\frac{c-2}{p}\right)$ if $k$ is even, so that $e_2(m) < e_2(p-1)$, while $\left(\frac{c+2}{p}\right) = -1 = \left(\frac{c-2}{p}\right)$ if $k$ is odd, so that $e_2(m) = e_2(p-1)$.

Now suppose that $\left(\frac{\Delta}{p}\right) = -1$. In this case, we have seen that $u = v^p$, so that $uv^{-1} = v^{p-1}$ and $c+2 = uv = v^{p+1}$. Let $w$ be a generator of $\mathbb{E}^\times$, a cyclic group with $p^2-1$ elements, and write $v = w^k$ for some integer $k$. Then $uv^{-1} = w^{k(p-1)}$ has order $m = \frac{p^2-1}{\gcd(k(p-1),p^2-1)} = \frac{p+1}{\gcd(k,p+1)}$, since $p^2-1 = (p-1)(p+1)$. Thus we have that $e_2(m) = e_2(p+1)$ if and only if $k$ is odd. Finally, note that $g = w^{p+1}$ must be an element of $\mathbb{F}_p^\times$, and a generator of that group, since its order in $\mathbb{E}^\times$ is $p-1$. So $c+2 = v^{p+1} = (w^k)^{p+1} = g^k$, and then $\left(\frac{c+2}{p}\right) = \left(\frac{g}{p}\right)^k = (-1)^k$. We conclude that $\left(\frac{c+2}{p}\right) = 1$ and $\left(\frac{c-2}{p}\right) = -1$ if $k$ is even, so that $e_2(m) < e_2(p+1)$, while $\left(\frac{c+2}{p}\right) = -1$ and $\left(\frac{c-2}{p}\right) = 1$ if $k$ is odd, so that $e_2(m) = e_2(p+1)$. □

**Example.** For $f(x) = x^2 - x - 1$, we saw above that $c_p(f) = -3$. Thus $\left(\frac{c+2}{p}\right) = \left(\frac{-1}{p}\right)$ and $\left(\frac{c-2}{p}\right) = \left(\frac{-5}{p}\right)$, and these symbols are equal if and only if $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = 1$. Therefore, if $m$ is the suborder of the Fibonacci sequence modulo $p$, then $m$ divides $p-1$ if $p \equiv 1$ or $4 \pmod 5$, and $m$ divides $p+1$ if $p \equiv 2$ or $3 \pmod 5$. (This is consistent with results in Corollary 12.2.7.) We can now also say that $m$ is smaller than this maximum value if $\left(\frac{c+2}{p}\right) = 1$, that is, $p \equiv 1 \pmod 4$. For example, if $p = 73$, then the suborder $m$ of the Fibonacci sequence modulo $p$ divides $p+1 = 74$, with $e_2(m) < e_2(74) = 1$. We conclude that $m = 37$, since $p = 73$ does not divide $F_1 = 1$. That is, $F_{37}$ is the first Fibonacci number (other than $F_0 = 0$) divisible by 73. ♢

**Example.** To illustrate our results so far, we consider the suborder function on $\mathbb{F}_{11}$. Using facts already established (and recalled below), it suffices to calculate $\mathrm{sub}_{11}(c)$ for $c = 3$, 4, and 5.

(1) If $c = 3$, then $\left(\frac{c+2}{p}\right) = \left(\frac{5}{11}\right) = 1$ and $\left(\frac{c-2}{p}\right) = \left(\frac{1}{11}\right) = 1$. Thus $m = \mathrm{sub}_{11}(3)$ divides $p-1 = 10$ with $e_2(m) < e_2(10)$. The only possibilities are $m = 1$ and $m = 5$, but Proposition 12.3.2 shows that $m \neq 1$. So $m = \mathrm{sub}_{11}(3) = 5$, which implies also that $\mathrm{sub}_{11}(-3) = 10$ by Proposition 12.3.4.

(2) If $c = 4$, then $\left(\frac{c+2}{p}\right) = \left(\frac{6}{11}\right) = -1$ and $\left(\frac{c-2}{p}\right) = \left(\frac{2}{11}\right) = -1$. In this case, $m = \text{sub}_{11}(4)$ divides $p - 1 = 10$ with $e_2(m) = e_2(10)$, so that $m = 2$ or $m = 10$. Again we can rule out $m = 2$ by Proposition 12.3.2, and so $\text{sub}_{11}(4) = 10$ and $\text{sub}_{11}(-4) = 5$ by Proposition 12.3.4.

(3) If $c = 5$, then $\left(\frac{c+2}{p}\right) = \left(\frac{7}{11}\right) = -1$ and $\left(\frac{c-2}{p}\right) = \left(\frac{3}{11}\right) = 1$. Thus $m = \text{sub}_{11}(5)$ divides $p + 1 = 12$ with $e_2(m) = e_2(12)$. The only possibilities are $m = 4$ and $m = 12$, but we can again eliminate $m = 4$ by Proposition 12.3.2. Therefore $\text{sub}_{11}(5) = 12 = \text{sub}_{11}(-5)$ by Proposition 12.3.4.

The following table summarizes all values of the suborder function on $\mathbb{F}_{11}$.

| $c$ | $-5$ | $-4$ | $-3$ | $-2$ | $-1$ | $0$ | $1$ | $2$ | $3$ | $4$ | $5$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $\text{sub}_{11}(c)$ | 12 | 5 | 10 | 2 | 3 | 4 | 6 | 1 | 5 | 10 | 12 |

As a specific example of the implications of the suborder function, consider the quadratic recursive sequence $r_n$ with characteristic polynomial $f(x) = x^2 - 3x + 7$. If $p = 11$, then $c = c_p(f) = (3)^2(7)^{-1} - 2 = 9 \cdot 8 - 2 = 70 = 4$ in $\mathbb{F}_{11}$. The table above implies that the suborder modulo 11 of the quadratic sequence defined by $r_n = 3r_{n-1} - 7r_{n-2}$ is $m = 10$. We verify this claim with the following calculations of $r_n$ modulo 11:

$$0, 1, 3, 2, -4, -4, 5, -1, -5, 3, 0, \ldots .$$

The first $m > 0$ for which $r_m = 0$ is $m = 10$. ◊

**Exercise 12.3.1.** For each prime $p$ below, find all values of the suborder function on the field $\mathbb{F}_p$.

(a) $p = 7$.

(b) $p = 13$.

(c) $p = 17$.

(d) $p = 19$.

**Exercise 12.3.2.** In each part below, find the suborder of the quadratic sequence $r_n$ modulo the given prime $p$ by direct calculation. (Assume that $r_0 = 0$ and $r_1 = 1$ in each case.) If $f(x)$ is the characteristic polynomial of $r_n$, find the value of $c = c_p(f)$ as defined in Theorem 12.3.3, and verify that $\text{sub}_p(r_n) = \text{sub}_p(c)$. (Use the calculations of the suborder function in Exercise 12.3.1, along with the suborder function on $\mathbb{F}_{11}$ calculated previously.)

(a) $r_n = 2r_{n-1} + r_{n-2}$, with $p = 7$.

(b) $r_n = 2r_{n-1} + r_{n-2}$, with $p = 11$.

(c) $r_n = 2r_{n-1} + r_{n-2}$, with $p = 13$.

(d) $r_n = 2r_{n-1} + r_{n-2}$, with $p = 17$.

(e) $r_n = 2r_{n-1} + r_{n-2}$, with $p = 19$.

(f) $r_n = r_{n-1} - 3r_{n-2}$, with $p = 7$.

(g) $r_n = r_{n-1} - 3r_{n-2}$, with $p = 11$.

(h) $r_n = r_{n-1} - 3r_{n-2}$, with $p = 13$.

(i) $r_n = r_{n-1} - 3r_{n-2}$, with $p = 17$.

(j) $r_n = r_{n-1} - 3r_{n-2}$, with $p = 19$.

## 12.4 Suborder Sequences

In §12.3, we defined the suborder function on $\mathbb{F}_p$, where $p$ is an odd prime, and we showed how this function allows us to calculate the suborder of a quadratic recursive sequence modulo $p$. In this section, we will further describe the calculation of this function in practice. In particular, we introduce what we call suborder sequences, which often allow us to calculate many values of the suborder function at once. The following theorem defines this concept.

**Theorem 12.4.1.** *Let $p$ be an odd prime and let $\mathbb{E}$ be a quadratic extension field of $\mathbb{F}_p$. Let $c$ be an element of $\mathbb{F}_p$, and let $z$ be an element of $\mathbb{E}$ for which $c = z + z^{-1}$, so that $m = \mathrm{sub}_p(c)$ is the order of $z$ in $\mathbb{E}^\times$. For each integer $k$, let $c_k = z^k + z^{-k}$. Then the following statements are true for all integers $k$ and $\ell$.*

(1) *$c_k$ is an element of $\mathbb{F}_p$.*

(2) *$c_k = c_\ell$ if and only if $\ell \equiv k \pmod{m}$ or $\ell \equiv -k \pmod{m}$.*

(3) *$c_k = -c_\ell$ if and only if $m$ is even and either $\ell \equiv \frac{m}{2} + k \pmod{m}$ or $\ell \equiv \frac{m}{2} - k \pmod{m}$.*

(4) *$c_k \cdot c_\ell = c_{k+\ell} + c_{k-\ell}$.*

(5) *$c_{2k} = c_k^2 - 2$.*

(6) *$c_{k+1} = c \cdot c_k - c_{k-1}$.*

*Proof.* Note that $c_0 = z^0 + z^0 = 2$ in every case, and that $c_1 = c$, given to be an element of $\mathbb{F}_p$. For positive values of $k$, then statement (6) shows inductively that $c_k$ is an element of $\mathbb{F}_p$ for all $k \geq 0$, and statement (2) extends that conclusion to negative values of $k$. We will prove these statements independently of the assumption that $c_k$ is in $\mathbb{F}_p$, and so establish statement (1).

For statement (2), note that $z^k + z^{-k} = z^\ell + z^{-\ell}$ if and only if

$$0 = z^\ell - z^k - z^{-k} + z^{-\ell} = (z^\ell - z^k)(1 - z^{-k}z^{-\ell}).$$

So either $z^\ell = z^k$ or $z^{-k}z^{-\ell} = 1$, in which case $z^\ell = z^{-k}$. If $z$ has order $m$ in $\mathbb{E}^\times$, one of these equations holds if and only if either $\ell \equiv k \pmod m$ or $\ell \equiv -k \pmod m$.

Similarly, $c_k = -c_\ell$ if and only if $(z^k + z^{-\ell})(1 + z^{-k}z^\ell) = 0$, so that $z^{\ell+k} = -1$ or $z^{\ell-k} = -1$. Either equation forces the order $m$ of $z$ to be even, and then we have $z^{\ell+k} = z^{m/2}$ or $z^{\ell-k} = z^{m/2}$, from which statement (3) follows.

For statement (4), we have

$$c_k \cdot c_\ell = (z^k + z^{-k})(z^\ell + z^{-\ell}) = z^{k+\ell} + z^{k-\ell} + z^{-(k-\ell)} + z^{-(k+\ell)} = c_{k+\ell} + c_{k-\ell}.$$

Statement (5) is obtained from (4) by letting $\ell = k$, so that $c_k^2 = c_{2k} + c_0$, and using the fact that $c_0 = 2$.

Statement (6) is obtained from (4) by letting $\ell = 1$, so that $c_k \cdot c_1 = c_{k+1} + c_{k-1}$, and using the fact that $c_1 = c$. □

**Corollary 12.4.2.** *Let $p$ be an odd prime and let $c$ be an element of $\mathbb{F}_p$. Define a recursive sequence $c_n$ of elements of $\mathbb{F}_p$ by $c_{n+1} = c \cdot c_n - c_{n-1}$ for positive integers $n$, with $c_0 = 2$ and $c_1 = c$. Then there is a smallest positive integer $m$ for which $c_m = 2$, and the suborder of $c_k$ modulo $p$ is $\mathrm{sub}_p(c_k) = \dfrac{m}{\gcd(m,k)}$ for every integer $k$.*

**Definition.** We refer to the sequence $c_n$ of elements of $\mathbb{F}_p$ defined in this way as the *suborder sequence* of $c$ modulo $p$.

*Proof.* Let $c = z + z^{-1}$ for some $z$ in a quadratic extension field $\mathbb{E}$ of $\mathbb{F}_p$, as we know is possible by Proposition 12.3.1. Part (6) of Theorem 12.4.1 shows that then $c_k$ is the same as $z^k + z^{-k} = (z^k) + (z^k)^{-1}$ for all $k$. There is a smallest positive integer $m$ for which $z^m = 1$, and in that case $c_m = 1 + 1^{-1} = 2$. Since $m = \mathrm{sub}_p(c)$ by definition, part (2) of Theorem 12.4.1 then implies that $c_\ell = 2 = c_0$ if and only if $\ell \equiv \pm 0 \pmod m$, and so $m$ is the smallest positive integer for which $c_m = 2$. Finally, note that $\mathrm{sub}_p(c_k)$ is the order of $z^k$ in $\mathbb{E}^\times$. Since $z$ has order $m$ in $\mathbb{E}^\times$, then the order of $z^k$ is $\dfrac{m}{\gcd(m,k)}$. □

Corollary 12.4.2 implies that we can calculate $\mathrm{sub}_p(c)$ using a sequence defined in terms of $c$. More importantly, if we find values of $c$ for which $\mathrm{sub}_p(c) = p-1$ and $\mathrm{sub}_p(c) = p+1$, this corollary allows us to calculate the entire suborder function on $\mathbb{F}_p$ with no additional work. We illustrate the idea with an example.

**Example.** Let $p = 23$. If $c = 3$, then $\left(\frac{c+2}{p}\right) = \left(\frac{5}{23}\right) = -1$ while $\left(\frac{c-2}{p}\right) = \left(\frac{1}{23}\right) = 1$. Theorem 12.3.5 implies that $m = \mathrm{sub}_{23}(3)$ divides $p + 1 = 24$, with

$e_2(m) = e_2(24)$. So $c = 3$ is a candidate for an element of $F_{23}$ with $\text{sub}_p(c) = 24$. If we let $c_{k+1} = 3c_k - c_{k-1}$ for $k > 0$, with $c_0 = 2$ and $c_1 = 3$, we obtain the following sequence of elements of $\mathbb{F}_{23}$:

$$2, 3, 7, -5, 1, 8, 0, -8, -1, 5, -7, -3, -2,$$
$$-3, -7, 5, -1, -8, 0, 8, 1, -5, 7, 3, 2, \ldots,$$

with $m = 24$ the smallest positive integer for which $c_m = 2$. So $\text{sub}_{23}(3) = 24$. Now we also have $\text{sub}_{23}(c_k) = 24$ if $\gcd(k, 24) = 1$, while $\text{sub}_{23}(c_k) = 12$ if $\gcd(k, 24) = 2$, and so forth. Notice that there is no repetition of the values of $c_k$ for $0 \leq k \leq 12$, as must be the case by part (2) of Theorem 12.4.1, so we obtain the suborder of thirteen elements of $F_{23}$ from one sequence.

In a similar way, if $c = -4$, we find that $\left(\frac{c+2}{p}\right) = \left(\frac{-2}{23}\right) = -1$ and $\left(\frac{c-2}{p}\right) = \left(\frac{-6}{23}\right) = -1$. This implies that $m = \text{sub}_{23}(-4)$ divides $p - 1 = 22$, with $e_2(m) = e_2(22)$, and thus $m = 22$ by Proposition 12.3.2. The sequence defined by $c_{k+1} = -4c_k - c_{k-1}$ with $c_0 = 2$ and $c_1 = -4$ is as follows:

$$2, -4, -9, -6, 10, -11, 11, -10, 6, 9, 4, -2,$$
$$4, 9, 6, -10, 11, -11, 10, -6, -9, -4, 2, \ldots,$$

with $c_m = 2$ for $m = 22$. So $\text{sub}_{23}(c_k) = 22$ if $\gcd(k, 22) = 1$, and $\text{sub}_{23}(c_k) = 11$ if $\gcd(k, 22) = 2$. From these two values of $c$, we have calculated the entire suborder function on $\mathbb{F}_{23}$. ◊

Table 12.1 compiles values of $\text{sub}_p(c)$ for primes $p < 60$, calculated using suborder sequences as in the preceding example. Using Propositions 12.3.2 and 12.3.4, it suffices to list $\text{sub}_p(c)$ with $3 \leq c \leq \frac{p-1}{2}$. For instance, since $\text{sub}_{37}(14) = 18$, then $\text{sub}_{37}(-14) = 9$, whereas $\text{sub}_{37}(15) = 12 = \text{sub}_{37}(-15)$.

**Exercise 12.4.1.** For $p = 17$, calculate the suborder sequences of $c = 3$ and of $c = 5$ modulo $p$. Use those sequences to verify all other entries of Table 12.1 for $p = 17$.

**Exercise 12.4.2.** For $p = 37$, calculate the suborder sequences of $c = 3$ and of $c = 4$ modulo $p$. Use those sequences to verify all other entries of Table 12.1 for $p = 37$.

**Exercise 12.4.3.** For $p = 43$, calculate the suborder sequences of $c = 3$ and of $c = 5$ modulo $p$. Use those sequences to verify all other entries of Table 12.1 for $p = 43$.

Table 12.1. Suborder Functions: $\mathrm{sub}_p(c)$ for $p < 60$

| $c\backslash p$ | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 | 37 | 41 | 43 | 47 | 53 | 59 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3 | 8 | 5 | 14 | 18 | 9 | 24 | 7 | 15 | 38 | 20 | 44 | 16 | 54 | 29 |
| 4 | | 10 | 12 | 18 | 5 | 11 | 15 | 32 | 36 | 14 | 11 | 23 | 9 | 58 |
| 5 | | 12 | 14 | 16 | 10 | 8 | 5 | 16 | 9 | 40 | 42 | 23 | 27 | 29 |
| 6 | | | 14 | 8 | 20 | 11 | 10 | 15 | 38 | 5 | 44 | 23 | 54 | 20 |
| 7 | | | | 9 | 9 | 12 | 7 | 15 | 19 | 10 | 22 | 8 | 27 | 29 |
| 8 | | | | 16 | 20 | 24 | 30 | 8 | 19 | 21 | 7 | 48 | 13 | 58 |
| 9 | | | | | 9 | 22 | 30 | 32 | 9 | 40 | 11 | 48 | 13 | 60 |
| 10 | | | | | | 11 | 28 | 32 | 19 | 42 | 42 | 23 | 52 | 30 |
| 11 | | | | | | 11 | 14 | 32 | 38 | 14 | 21 | 48 | 13 | 12 |
| 12 | | | | | | | 28 | 5 | 38 | 42 | 21 | 12 | 54 | 58 |
| 13 | | | | | | | 28 | 10 | 38 | 40 | 21 | 46 | 13 | 30 |
| 14 | | | | | | | 15 | 16 | 18 | 7 | 11 | 23 | 9 | 29 |
| 15 | | | | | | | | 30 | 12 | 40 | 7 | 24 | 26 | 30 |
| 16 | | | | | | | | | 36 | 21 | 44 | 23 | 52 | 58 |
| 17 | | | | | | | | | 36 | 8 | 44 | 46 | 54 | 29 |
| 18 | | | | | | | | | 38 | 20 | 44 | 16 | 18 | 29 |
| 19 | | | | | | | | | | 21 | 7 | 23 | 54 | 29 |
| 20 | | | | | | | | | | 42 | 42 | 48 | 52 | 30 |
| 21 | | | | | | | | | | | 22 | 46 | 52 | 20 |
| 22 | | | | | | | | | | | | 24 | 27 | 60 |
| 23 | | | | | | | | | | | | 23 | 27 | 29 |
| 24 | | | | | | | | | | | | | 52 | 29 |
| 25 | | | | | | | | | | | | | 52 | 5 |
| 26 | | | | | | | | | | | | | 13 | 10 |
| 27 | | | | | | | | | | | | | | 29 |
| 28 | | | | | | | | | | | | | | 60 |
| 29 | | | | | | | | | | | | | | 60 |

The preceding example and exercises illustrate certain patterns in suborder sequences, which typically allow us to reduce the amount of calculation necessary in compiling values taken on by the suborder function. Our next result summarizes the conclusions we can reach based on partial calculation of these sequences.

**Corollary 12.4.3.** *Let $p$ be an odd prime, let $c$ be an element of $\mathbb{F}_p$, and let $m = \mathrm{sub}_p(c)$. For $k \geq 0$, let $c_k$ be the $k$-th term in the suborder sequence of $c$ modulo $p$. Then the following statements are true.*

(1) $m = 2k + 1$ *if and only if $k$ is the smallest positive integer for which* $c_k = c_{k+1}$.

(2) $m = 4k + 2$ *if and only if $k$ is the smallest positive integer for which* $c_k = -c_{k+1}$.

(3) $m = 4k$ *if and only if $k$ is the smallest positive integer for which* $c_k = 0$.

(4) $m = 3k$ *if and only if $k$ is the smallest positive integer for which* $c_k = -1$.

(5) $m = 6k$ *if and only if $k$ is the smallest positive integer for which* $c_k = 1$.

*Proof.* We will prove statements (2) and (4), leaving the remaining statements as Exercise 12.4.4. For (2), note that if $m = 4k+2$, then $c_{\frac{m}{2}-k} = c_{k+1} = -c_k$ by part (3) of Theorem 12.4.1. Conversely, if $c_k = -c_{k+1}$, the same theorem shows that $m$ is even and either $k+1 \equiv \frac{m}{2} + k \pmod{m}$ (which occurs only when $c = -2$ and $m = 2 = 4k+2$) or $k+1 \equiv \frac{m}{2} - k \pmod{m}$, which implies that $4k+2 \equiv 0 \pmod{m}$. Now $m$ is an *even* divisor of $4k+2$, so must have the form $4\ell+2$ for some $\ell \leq k$. But then we have $c_{\ell+1} = -c_\ell$, as in the first part of this proof. If we assume that $k$ is as small as possible with that property, then $m = 4k+2$.

For (4), if $m = 3k$, then $c_{m-k} = c_{2k} = c_k$. But $c_{2k} = c_k^2 - 2$ by part (5) of Theorem 12.4.1, and we find that $c_k$ satisfies $x^2 - x - 2 = (x-2)(x+1) = 0$. Here $c_k \neq 2$ since $k < m$, so we must have $c_k = -1$. Conversely, if $c_k = -1$, then $c_{2k} = (-1)^2 - 2 = -1$ also. Thus we have either $2k \equiv k \pmod{m}$, so that $m$ divides $k$ (but this is impossible since $c_k$ would then equal 2), or $2k \equiv -k \pmod{m}$, so that $m$ divides $3k$. Since, as noted, $m$ does not divide $k$, then $m$ must equal $3\ell$ for some $\ell \leq k$. We conclude as in part (2) that $m = 3k$. □

**Exercise 12.4.4.** Let $c_k$ be the $k$-th term in the suborder sequence of $c$ modulo $p$, where $p$ is an odd prime and $c$ is an element of $\mathbb{F}_p$. Let $m$ be the suborder of $c$ modulo $p$.

(a) Show that $m = 2k+1$ if and only if $k$ is the smallest integer so that $c_k = c_{k+1}$.

(b) Show that $m = 4k$ if and only if $k$ is the smallest integer so that $c_k = 0$.

(c) Show that $m = 6k$ if and only if $k$ is the smallest integer so that $c_k = 1$.

**Example.** Let $p = 59$ and $c = 10$. The sequence in $\mathbb{F}_{59}$ defined by $c_{k+1} = 10c_k - c_{k-1}$, with $c_0 = 2$ and $c_1 = 10$, begins

$$2, 10, -20, 26, -15, 1, 25, 13, -13, \ldots .$$

Since $c_5$ is the first occurrence of 1, we know that $m = \text{sub}_{59}(10) = 6 \cdot 5 = 30$. (We obtain the same conclusion from the fact that $c_7 = -c_8$, so that $m = 4(7)+2$.) Note that with $m = 30$ even, then $c_{15-k} = -c_k$ for all $k$, and $c_{30-k} = c_k$. So we can easily continue this sequence if needed. The terms calculated so far are sufficient for determining all elements of $\mathbb{F}_{59}$ whose suborder divides 30. For example, the elements of suborder 30 are precisely of the form $c_k$ with $\gcd(k, 30) = 1$, that is, $c_1 = 10$, $c_7 = 13$, $c_{11} = -c_4 = 15$, and $c_{13} = -c_2 = 20$ (with $c_{17} = c_{13}$ and so forth). ◊

**Exercise 12.4.5.** For each prime $p$ and element $c$ of $\mathbb{F}_p$, calculate enough terms of the suborder sequence of $c$ modulo $p$ in order to determine $\text{sub}_p(c)$. Use the results to calculate as many other values of the suborder function modulo $p$ as possible.

(a) $p = 61$ and $c = 4$.

(b) $p = 61$ and $c = 5$.

(c) $p = 67$ and $c = 3$.

(d) $p = 67$ and $c = 5$.

**Exercise 12.4.6.** In each part, find the suborder of the quadratic sequence $r_n$ modulo the given prime $p$ by direct calculation. If $f(x)$ is the characteristic polynomial of $r_n$, find the value of $c = c_p(f)$ as defined in Theorem 12.3.3, and use Table 12.1 to verify that $\text{sub}_p(r_n) = \text{sub}_p(c)$.

(a) $r_n = 2r_{n-1} + r_{n-2}$, with $p = 29$.

(b) $r_n = 2r_{n-1} + r_{n-2}$, with $p = 31$.

(c) $r_n = 2r_{n-1} + r_{n-2}$, with $p = 37$.

(d) $r_n = 2r_{n-1} + r_{n-2}$, with $p = 41$.

(e) $r_n = 2r_{n-1} + r_{n-2}$, with $p = 43$.

(f) $r_n = 2r_{n-1} + r_{n-2}$, with $p = 47$.

If we are interested in computing $\text{sub}_p(c)$ for just one $c$ in $\mathbb{F}_p$, we have an alternative to calculating the entire suborder sequence of $c$ modulo $p$.

**Lemma 12.4.4.** *Let $p$ be an odd prime, let $c$ be an element of $\mathbb{F}_p$, and let $m = \text{sub}_p(c)$. Then $\text{sub}_p(c^2 - 2) = \frac{m}{2}$ if $m$ is even, while $\text{sub}_p(c^2 - 2) = m$ if $m$ is odd.*

*Proof.* Part (5) of Theorem 12.4.1 and Corollary 12.4.2 show that the suborder of $c^2 - 2$ is given by $\frac{m}{\gcd(m,2)}$, which equals $\frac{m}{2}$ if $m$ is even, and equals $m$ if $m$ is odd. □

**Theorem 12.4.5.** *Let $p$ be an odd prime and let $c$ be an element of $\mathbb{F}_p$. Consider a sequence $d_n$ of elements of $\mathbb{F}_p$ defined recursively by $d_0 = c$ and $d_n = d_{n-1}^2 - 2$ for $n > 0$. Then there is a smallest positive integer $\ell$ so that $d_\ell = d_k$ for some $k$ with $0 \le k < \ell$. In this case, if $m = \text{sub}_p(c)$, then $k = e_2(m)$. If $m' = \frac{m}{2^k}$, then $t = \ell - k$ is the smallest positive integer with $2^t \equiv \pm 1 \pmod{m'}$.*

*Proof.* If $c_n$ is defined for $n \ge 0$ as in Corollary 12.4.2, then we see by induction, using part (5) of Theorem 12.4.1, that $d_n = c_{2^n}$ for $n \ge 0$. If we let $m_n = \text{sub}_p(d_n)$ for each $n \ge 0$, then Lemma 12.4.4 shows that $m_{n+1} = \frac{m_n}{2}$ if $m_n$ is even, while $m_{n+1} = m_n$ if $m_n$ is odd. It follows that if $k$ is the exponent of 2 in $m = m_0$, and

$m' = \frac{m}{2^k}$, then $m_n = m'$ for all $n \geq k$. Thus $d_k$ is the first term of this sequence that can possibly equal some later term. Now note that $d_k = d_\ell$ for some $\ell > k$ if and only if $c_{2^k} = c_{2^\ell}$, which by part (2) of Theorem 12.4.1 is true if and only if $2^\ell \equiv 2^k \pmod{m}$ or $2^\ell \equiv -2^k \pmod{m}$. Since $2^k$ divides all terms in these congruences, this is equivalent to saying that $2^{\ell-k} \equiv \pm 1 \pmod{m'}$. □

We refer to the sequence $d_n$ defined in Theorem 12.4.5 as the *suborder subsequence* of $c$ modulo a prime $p$.

**Example.** Let $p = 71$ and $c = -5$. The subsequence $d_n$ defined in Theorem 12.4.5 begins

$$-5, 23, 30, -25, -16, -30, -25, -16, \ldots,$$

so that $k = 3$ and $\ell = 6$ is the smallest pair for which $d_k = d_\ell$. Thus $2^k = 8$ divides $m = \text{sub}_p(c)$, and we can be sure that $m$ divides $p + 1 = 72$ rather than $p - 1 = 70$. Now $m' = \frac{m}{8}$ could equal 1, 3, or 9, but we know that $t = \ell - k = 3$ is the smallest positive integer for which $2^t \equiv \pm 1 \pmod{m'}$. Since $2^1 \equiv 1 \pmod{1}$ and $2^2 \equiv 1 \pmod{3}$, we conclude that $m'$ must equal 9. Therefore $m = \text{sub}_{71}(-5) = 72$. The calculations in this example also show that $\text{sub}_{71}(23) = 36$, $\text{sub}_{71}(30) = 18$, and $\text{sub}_{71}(b) = 9$ for $b = -25, -16$, and $-30$. ◊

**Exercise 12.4.7.** Use Corollary 12.4.3 to calculate $\text{sub}_p(c)$ for each of the following primes $p$ and integers $c$. Verify that your answers are consistent with the claims of Theorem 12.4.5.

(a) $p = 53$ and $c = 3$.

(b) $p = 53$ and $c = 8$.

(c) $p = 59$ and $c = 6$.

(d) $p = 59$ and $c = 7$.

(e) $p = 61$ and $c = 3$.

(f) $p = 61$ and $c = 4$.

We conclude this section with a formula for the number of elements of a field $\mathbb{F}_p$ having a particular suborder.

**Lemma 12.4.6.** *Let $p$ be an odd prime, with $\mathbb{F}_p$ a field with $p$ elements and $\mathbb{E}$ a quadratic extension field of $\mathbb{F}_p$. Let $w$ be a generator of $\mathbb{E}^\times$ and let $z = w^k$ for some $k$. Then $z + z^{-1}$ is an element of $\mathbb{F}_p$ if and only if $k$ is a multiple of $p - 1$ or of $p + 1$.*

*Proof.* We noted in §12.2 that the function $\psi : \mathbb{E} \to \mathbb{E}$ defined by $\psi(x) = x^p$ is an automorphism of $E$, and that $\psi(v) = v$ if and only if $v$ is an element of $\mathbb{F}_p$. Note that

$$\psi(z + z^{-1}) = \psi(z) + \psi(z^{-1}) = z^p + z^{-p} = z + z^{-1}$$

if and only if $0 = z^p - z - z^{-1} + z^{-p} = (z^p - z)(1 - z^{-1}z^{-p})$, so that $z^p = z$ or $z^p = z^{-1}$. If $z = w^k$, the first case implies that $z^{p-1} = w^{(p-1)k} = 1$, and the second case implies that $z^{p+1} = w^{(p+1)k} = 1$. Since $w$ has order $p^2 - 1 = (p-1)(p+1)$, the first case occurs if and only if $p + 1$ divides $k$ and the second occurs if and only if $p - 1$ divides $k$. □

If $m$ is a positive integer, denote by $\phi(m)$ (the *Euler totient function* applied to $m$) the number of integers $n$ with $0 \leq n < m$ and $\gcd(n, m) = 1$.

**Proposition 12.4.7.** *Let $p$ be an odd prime. If $m$ divides $p - 1$ or $m$ divides $p + 1$, but not both, then there are precisely $\frac{\phi(m)}{2}$ elements $c$ in $\mathbb{F}_p$ for which $\mathrm{sub}_p(c) = m$.*

The only common divisors of $p-1$ and $p+1$ are 1 and 2. As we have seen, $\mathbb{F}_p$ always contains a unique element of suborder 1 and a unique element of suborder 2. (These elements are congruent to 2 and $-2$, respectively modulo $p$.)

*Proof.* Let $\mathbb{E}$ be a quadratic extension field of $\mathbb{F}_p$ and let $w$ be a generator of $\mathbb{E}^\times$. If $z = w^{p+1}$, then $z$ has order $p-1$ in $\mathbb{E}^\times$, and $c = z+z^{-1}$ is an element of $\mathbb{F}_p$ with suborder $p-1$ by Lemma 12.4.6. For $0 < k < \frac{p-1}{2}$, the elements $c_k = z^k + z^{-k}$ are distinct in $\mathbb{F}_p$, by part (2) of Theorem 12.4.1, with $\mathrm{sub}_p(c_k) = \frac{p-1}{\gcd(k,p-1)}$. For each divisor $m$ of $p-1$ other than 1 and 2, we find that there are $\frac{\phi(m)}{2}$ such values of $k$. Similarly, if we let $z = w^{p-1}$, we find $\frac{\phi(m)}{2}$ values of $c_k$ for which $\mathrm{sub}_p(c_k) = m$, if $m$ is a divisor of $p + 1$ other than 1 or 2. For every positive integer $n$, the sum of $\phi(d)$, taken over all positive divisors $d$ of $n$, equals $n$. Using this fact, we find that all $p$ elements of $\mathbb{F}_p$ are accounted for in these lists. □

We illustrate the final claim of this proof with the following example.

**Example.** If $p = 41$, then possible suborders of elements of $\mathbb{F}_p$ are divisors of $p - 1 = 40$ or $p + 1 = 42$. Each such divisor $m > 2$ is listed below, along with $\frac{\phi(m)}{2}$ for each one.

| $m$ | 4 | 5 | 8 | 10 | 20 | 40 | 3 | 6 | 7 | 14 | 21 | 42 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\phi(m)/2$ | 1 | 2 | 2 | 2 | 4 | 8 | 1 | 1 | 3 | 3 | 6 | 6 |

Adding in one element of suborder 1, and one element of suborder 2, we see that the sum of the number of elements in this list is 41. ◊

**Exercise 12.4.8.** Verify that Proposition 12.4.7 is correct for each of the following primes $p$.

(a) $p = 17$.

(b) $p = 19$.

(c) $p = 29$.

(d) $p = 31$.

(e) $p = 37$.

(f) $p = 43$.

(g) $p = 47$.

## Properties of Recursive Sequences—Review

In this chapter, we considered sequences defined by

$$r_0 = 0, \quad r_1 = 1, \quad \text{and} \quad r_n = sr_{n-1} + tr_{n-2} \quad \text{for} \quad n \geq 2,$$

where $s$ and $t$ are integers, $t \neq 0$. We noted several connections between terms in a *quadratic recursive sequence* of this type and roots of its *characteristic polynomial* $f(x) = x^2 - sx - t$, either in the complex numbers or in a field with $p^2$ elements for some prime $p$. We summarize our main results as follows.

(1) If $\upsilon$ is a root of $f(x) = x^2 - sx - t$, then $\upsilon^n = r_n\upsilon + tr_{n-1}$ for every $n \geq 1$. Using this fact, we can determine a formula for the $n$-th term of the quadratic recursive sequence with characteristic polynomial $f(x)$ (Theorem 12.1.2). We can also describe divisibility properties of a quadratic sequence, such as which terms in the sequence divide other terms or, in some cases, calculating the greatest common divisor of a pair of terms in such a sequence.

(2) We can consider patterns in a quadratic sequence $r_n$ when its terms are reduced modulo a fixed prime $p$ or, equivalently, consider $r_n$ as defined by a polynomial $f(x) = x^2 - sx - t$ in a field $\mathbb{F}_p$ with $p$ elements. This sequence is periodic modulo $p$ if and only if $t \neq 0$ in $\mathbb{F}_p$, that is, $p$ does not divide $t$. We can place restrictions on the *suborder* of $r_n$ modulo $p$ (the smallest positive $m$ for which $r_m \equiv 0 \pmod{p}$) and the *order* of $r_n$ modulo $p$ (the smallest $m > 0$ for which $r_m \equiv 0 \pmod{p}$ and $r_{m+1} \equiv 1 \pmod{p}$) based on how $f(x)$ factors in a field $\mathbb{E}$ with $p^2$ elements.

(3) We can further describe the suborder of a quadratic sequence modulo an odd prime $p$ via *suborder functions*, $\text{sub}_p(c)$, which we define on the field $\mathbb{F}_p$ when $p$ is an odd prime. We can associate an element $c$ of $\mathbb{F}_p$ to the polynomial $f(x) = x^2 - sx - t$, and then show that the suborder of $r_n$ modulo $p$ is determined by the value of $\text{sub}_p(c)$. In §12.3 and §12.4, we compiled several properties of

these suborder functions, and saw some practical methods of computing $\text{sub}_p(c)$ for an individual $c$ or for all elements $c$ in $\mathbb{F}_p$.

Thus in this chapter we have established some close connections between recursive sequences defined by a polynomial $f(x) = x^2 - sx - t$ and the roots of $f(x)$, which are quadratic integers. In Chapter 13, we will apply these results to further describe some properties of quadratic forms and quadratic domains.

# 13

# Applications of Quadratic Recursive Sequences

In our final chapter, we consider several applications of the results on quadratic recursive sequences in Chapter 12 to calculations with indefinite quadratic forms and to properties of quadratic domains of positive discriminant. We begin in §13.1 by showing that the automorphs of a particular type of quadratic form of discriminant $\Delta > 0$ can be computed using terms of a corresponding quadratic sequence. We will see in §13.2 that we can then apply our results about suborders of quadratic sequences modulo primes to calculation of the fundamental solution of $x^2 - dy^2 = 1$ when $d$ is not squarefree. In §13.3, we likewise apply these results to descriptions of the class group of a quadratic subdomain of positive discriminant.

## 13.1 Recursive Sequences and Automorphs

Let $\phi(x)$ be the principal polynomial of some positive discriminant $\Delta$, and for a fixed integer $k$, consider the following quadratic form in $\mathcal{Q}_\Delta$:

$$f = (1 : k) = x^2 + bxy + cy^2, \quad \text{where } c = \phi(k) \text{ and } b = \phi'(k). \tag{13.1.1}$$

Recall that a unimodular matrix $U$ is an automorph of $f$ if $f \circ U = f$.

**Proposition 13.1.1.** *Let $f$ be the quadratic form defined as in* (13.1.1)*. Then $U = \begin{bmatrix} q & s \\ r & t \end{bmatrix}$ is an automorph of $f$ if and only if $q$ and $r$ are integers for which $f(q, r) = 1$, with $s = -cr$ and $t = q + br$.*

*Proof.* Since the coefficient of $x^2$ in $f$ is 1, this is an immediate consequence of Proposition 4.3.4. □

Proposition 13.1.1 implies that automorphs of $f$ are in one-to-one correspondence with solutions of $f(q,r) = 1$. By Theorem 11.1.1, we know that all such solutions (in positive integers) arise as convergents in the continued fraction expansion of $\upsilon = \frac{-b+\sqrt{\Delta}}{2}$, which we can find via the quadratic continued fraction algorithm applied with $a_0 = 1$ and $k_0 = k$.

**Example.** Let $\Delta = 29$ and $k = 0$, so that $f(x,y) = x^2 + xy - 7y^2$. From the following values of the principal polynomial $\phi(x) = x^2 + x - 7$ of discriminant 29,

| $x$ | $-3,2$ | $-2,1$ | $-1,0$ |
|---|---|---|---|
| $\phi(x)$ | $-1$ | $-5$ | $-7$ |

we can apply the quadratic continued fraction algorithm with $a_0 = 1$ and $k_0 = 0$, obtaining the following data.

| $i$ | 0 | 1 | 2 |
|---|---|---|---|
| $a$ | 1 | 1 | 1 |
| $k$ | 0 | $-3$ | $-3$ |
| $q$ | 2 | 5 | 5 |
| $m$ | 2 | 11 | |
| $n$ | 1 | 5 | |

Here $\langle 2, \overline{5} \rangle$ is the continued fraction of $\upsilon = \frac{-1+\sqrt{29}}{2}$. Note that $f(2,1) = -1$, but that $(q,r) = (11,5)$ is the smallest positive integer pair with $f(q,r) = 1$. With $s = -cr = 35$ and $t = q + br = 16$, then

$$U = \begin{bmatrix} 11 & 35 \\ 5 & 16 \end{bmatrix}$$

is an automorph of $f$, and the group of automorphs of $f$ consists of $\pm U^n$ with $n$ an arbitrary integer. ◊

If $f$ is the quadratic form of positive discriminant $\Delta$ given in equation (13.1.1), we can connect all positive integer solutions of $f(x,y) = 1$, and so all automorphs of $f$, to the terms in a particular quadratic recursive sequence, defined in the following theorem.

**Theorem 13.1.2.** *Let $\phi(x)$ be the principal polynomial of some positive discriminant $\Delta$, and let $f(x,y) = x^2 + bxy + cy^2$, where $c = \phi(k)$ and $b = \phi'(k)$ for some integer $k$. Let $q$ and $r$ be the smallest pair of positive integers so that $f(q,r) = 1$. Let $a_n$ be defined for all $n \geq 0$ by*

$$a_n = (2q + br)a_{n-1} - a_{n-2} \quad \textit{with} \quad a_0 = 0 \quad \textit{and} \quad a_1 = 1. \tag{13.1.2}$$

*Then all solutions of $f(x,y) = 1$ in positive integers are given by*

$$x = a_n q - a_{n-1} \quad \textit{and} \quad y = a_n r,$$

*with $n \geq 1$. If $U = \begin{bmatrix} q & -cr \\ r & q+br \end{bmatrix}$ and $I$ is the $2 \times 2$ identity matrix, then $U^n = a_n U - a_{n-1} I$ for all $n \geq 1$.*

**Example.** For $f(x,y) = x^2 + xy - 7y^2$ of discriminant $\Delta = 29$, we found that $(q,r) = (11,5)$ is the smallest positive solution of $f(x,y) = 1$. So $2q+br = 27$, and we consider the quadratic recursive sequence $a_n = 27a_{n-1} - a_{n-2}$ with $a_0 = 0$ and $a_1 = 1$, which begins $0, 1, 27, 728, \ldots$. Theorem 13.1.2 implies that the next two smallest positive solutions of $f(x,y) = 1$ are

$$(27 \cdot 11 - 1, 27 \cdot 5) = (296, 135) \quad \text{and} \quad (728 \cdot 11 - 27, 728 \cdot 5) = (7981, 3640),$$

claims that we can verify using the continued fraction of $\upsilon = \frac{-1+\sqrt{29}}{2}$ calculated in the preceding example. Likewise,

$$U^2 = 27\begin{bmatrix} 11 & 35 \\ 5 & 16 \end{bmatrix} - \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 296 & 945 \\ 135 & 431 \end{bmatrix}$$

and

$$U^3 = 728\begin{bmatrix} 11 & 35 \\ 5 & 16 \end{bmatrix} - 27\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 7981 & 25480 \\ 3640 & 11621 \end{bmatrix},$$

as we can confirm by matrix multiplication. ◊

*Proof.* Let $f(x,y) = x^2 + bxy + cy^2$ be a quadratic form of positive discriminant $\Delta$ as in (13.1.1), and let $\upsilon = \frac{-b+\sqrt{\Delta}}{2}$. All parts of Theorem 11.1.1 apply to $f$ since $\upsilon + \lfloor -\overline{\upsilon} \rfloor > \sqrt{\Delta} - 1 > 1$ and $\upsilon + \overline{\upsilon} = -b$ is an integer. In particular, if $(q,r)$ is the smallest pair of positive integers for which $f(q,r) = 1$, and we let $w = q - r\upsilon$, then parts (2), (3), and (5) of Theorem 11.1.1 imply that all solutions of $f(x,y) = 1$ are given by $(x,y) = (q_n, r_n)$, where $w^n = q_n - r_n\upsilon$. Now note that

$$w + \overline{w} = (q - r\upsilon) + (q - r\overline{\upsilon}) = 2q - r(\upsilon + \overline{\upsilon}) = 2q + br$$

and

$$w\overline{w} = (q - r\upsilon)(q - r\overline{\upsilon}) = q^2 - qr(\upsilon + \overline{\upsilon}) + r^2\upsilon\overline{\upsilon} = q^2 + bqr + cr^2 = 1,$$

since $\upsilon + \overline{\upsilon} = -b$ and $\upsilon\overline{\upsilon} = \frac{b^2-\Delta}{4} = c$. Thus $w$ is a root of $x^2 - (2q + br)x + 1$. But now if $a_n$ is defined for $n \geq 0$ as in equation (13.1.2), then Theorem 12.1.1 implies that $w^n = a_n w - a_{n-1}$ for all $n \geq 1$. That is,

$$q_n - r_n\upsilon = a_n(q - r\upsilon) - a_{n-1} = (a_n q - a_{n-1}) - a_n r\upsilon,$$

so that $q_n = a_n q - a_{n-1}$ and $r_n = a_n r$.

Now let $U$ be the automorph of $f$ with entries $q$ and $r$ in its first column, and let $s = -cr$ and $t = q + br$. Note that

$$U^2 = \begin{bmatrix} q^2 + rs & (q+t)s \\ (q+t)r & rs + t^2 \end{bmatrix} \quad \text{while} \quad a_2U - a_1I = \begin{bmatrix} a_2q - 1 & a_2s \\ a_2r & a_2t - 1 \end{bmatrix},$$

with $a_2 = 2q + br$. Using the calculation of $q_n$ and $r_n$ above, we then find that

$$q_2 = a_2q - a_1 = a_2q - 1 = (2q + br)q - (q^2 + bqr + cr^2) = q^2 - cr^2 = q^2 + rs$$

and

$$r_2 = a_2r = (2q + br)r = (q + t)r.$$

Then note that $a_2s = -c(a_2r) = -cr_2$ and $a_2t - 1 = a_2(q+br) - 1 = (a_2q - 1) + b(a_2r) = q_2 + br_2$. This implies that $a_2U - a_1I$ is an automorph of $f$ by Proposition 13.1.1. Since $U^2$ is also an automorph of $f$, with the same first column as $a_2U - a_1I$, we conclude that $U^2 = a_2U - a_1I$. Now under the inductive hypothesis that $U^k = a_kU - a_{k-1}I$ for some $k \geq 1$, we find that

$$\begin{aligned} U^{k+1} = U \cdot U^k &= a_kU^2 - a_{k-1}U \\ &= a_k(a_2U - a_1I) - a_{k-1}U = (a_2a_k - a_{k-1})U - (a_1a_k)I. \end{aligned}$$

But since $a_1 = 1$ and $a_2 = 2q + br$, we conclude that $U^{k+1} = a_{k+1}U - a_kI$, and therefore $U^n = a_nU - a_{n-1}I$ for all $n \geq 1$. □

The quadratic sequence defined in (13.1.2) depends only on the discriminant $\Delta$, as we can see by the following proposition.

**Proposition 13.1.3.** *Let $\phi = (1 : 0) = x^2 + \varepsilon xy + \frac{\varepsilon^2 - \Delta}{4}y^2$ be the principal form of some discriminant $\Delta$. Let $f = (1 : k) = x^2 + bxy + cy^2$ for some integer $k$, with $f$ also of discriminant $\Delta$. Then $\phi(q, r) = f(q - kr, r)$ for every pair of integers $q$ and $r$.*

*Proof.* Note that $b = \phi'(k) = 2k + \varepsilon$ and $c = \phi(k) = k^2 + \varepsilon k + \frac{\varepsilon^2 - \Delta}{4}$ (here with $\phi(x)$ the principal polynomial of discriminant $\Delta$). Then

$$\begin{aligned} f(q - kr, r) = (q - kr)^2 + (2k + \varepsilon)(q - kr)r + \left(k^2 + \varepsilon k + \frac{\varepsilon^2 - \Delta}{4}\right)r^2 \\ = q^2 + \varepsilon qr + \frac{\varepsilon^2 - \Delta}{4}r^2 = \phi(q, r) \end{aligned}$$

by direct calculation. □

Thus if $(q, r)$ is the smallest pair of positive integers for which $\phi(q, r) = 1$, so that $(q - kr, r)$ is likewise the smallest positive solution of $f(x, y) = 1$, then

$$2q + \varepsilon r = 2(q - kr) + (2k + \varepsilon)r = 2(q - kr) + br.$$

**Exercise 13.1.1.** For each discriminant $\Delta$ below, find the smallest solution $(q, r)$ in positive integers of the equation $f(x, y) = 1$, where $f = (1 : 0)$ is the principal form of discriminant $\Delta$. Calculate the terms in the quadratic sequence $a_n$ defined as in equation (13.1.2), and the corresponding solutions $(q_n, r_n)$ of $f(x, y) = 1$, for $n \leq 4$.

(a) $\Delta = 8$.

(b) $\Delta = 12$.

(c) $\Delta = 13$.

(d) $\Delta = 17$.

(e) $\Delta = 21$.

(f) $\Delta = 24$.

(g) $\Delta = 28$.

(h) $\Delta = 33$.

(i) $\Delta = 37$.

(j) $\Delta = 40$.

(k) $\Delta = 41$.

## 13.2 An Application to Pell's Equation

If $d$ is a positive integer, not a square, there is a smallest pair of positive integers $q$ and $r$ for which $q^2 - dr^2 = 1$, and we say that the pair $(q, r)$, or the corresponding real number $\upsilon = q + r\sqrt{d}$, is the *fundamental solution* of Pell's equation, $x^2 - dy^2 = 1$. We saw in §9.2 that if $\upsilon^m$ is written as $q_m + r_m\sqrt{d}$, then all solutions of $x^2 - dy^2 = 1$ in positive integers are given by $(q_m, r_m)$ with $m$ positive. In this case, if $n$ is a positive integer, and $m$ is the smallest positive integer for which $n$ divides $r_m$, then $q_m + \frac{r_m}{n}\sqrt{n^2 d}$ is the fundamental solution of $x^2 - (n^2 d)y^2 = 1$. In this section, we apply our results about quadratic recursive sequences to the problem of describing the fundamental solution of $x^2 - (n^2 d)y^2 = 1$ from that of $x^2 - dy^2 = 1$. We begin with the following observation, a special case of Theorem 13.1.2.

If $\upsilon = q + r\sqrt{d}$ is the fundamental solution of $x^2 - dy^2 = 1$, and $\overline{\upsilon} = q - r\sqrt{d}$, then $\upsilon$ is a root of

$$(x - \upsilon)(x - \overline{\upsilon}) = x^2 - (\upsilon + \overline{\upsilon})x + \upsilon\overline{\upsilon} = x^2 - 2qx + 1,$$

here using the fact that $v\overline{v} = q^2 - dr^2 = 1$. If we let $a_m = 2q \cdot a_{m-1} - a_{m-2}$, with $a_0 = 0$ and $a_1 = 1$, then Theorem 12.1.1 shows that

$$v^m = a_m v - a_{m-1} = (qa_m - a_{m-1}) + (ra_m)\sqrt{d}.$$

So $(q_m, r_m) = (qa_m - a_{m-1}, ra_m)$ is a solution of $x^2 - dy^2 = 1$. If we assume that $\gcd(r, n) = 1$, then $n$ divides $ra_m$ if and only if $n$ divides $a_m$. By definition, the smallest positive integer $m$ for which this is true is the *suborder* of this quadratic sequence modulo $n$.

**Example.** Suppose we have found that $v = 8 + 3\sqrt{7}$ is the fundamental solution of $x^2 - 7y^2 = 1$, and that we are interested in finding the fundamental solution of $x^2 - 847y^2 = 1$, where $847 = 11^2 \cdot 7$. Consider $a_m$ defined for $m \geq 0$ by $a_m = 16a_{m-1} - a_{m-2}$, with $a_0 = 0$ and $a_1 = 1$. We can easily calculate the first terms of this sequence modulo 11 as $0, 1, 5, 2, 5, 1, 0, \ldots$, so that $m = 6$ is the smallest positive integer for which 11 divides $a_m$. Direct calculation shows that $v^6 = 8193151 + 3096720\sqrt{7}$, and we confirm that $3096720 = 11 \cdot 281520$, so that $(8193151, 281520)$ is the fundamental solution of $x^2 - 847y^2 = 1$. ◊

**Exercise 13.2.1.** Verify the claim of the preceding example by applying the algorithm for Pell's equation of Theorem 9.2.2 directly to $d = 847$.

**Theorem 13.2.1.** *Let $d$ be a positive integer, not a square, and let $v = q + r\sqrt{d}$ be the fundamental solution of $x^2 - dy^2 = 1$. Let $v^m = q_m + r_m\sqrt{d}$ for each positive integer $m$. Let $p$ be a prime number that does not divide $r$, and let $m_p$ be the smallest positive integer for which $p$ divides $r_{m_p}$. Then the following statements are true.*

(1) *If $p$ divides $d$, then $m_p = p$.*

(2) *If $p$ divides $q$, then $m_p = 2$.*

(3) *If $p$ does not divide $q$ and $\left(\frac{d}{p}\right) = 1$, then $m_p$ divides $\frac{p-1}{2}$.*

(4) *If $p$ does not divide $q$ and $\left(\frac{d}{p}\right) = -1$, then $m_p$ divides $\frac{p+1}{2}$.*

Note that if $q^2 - dr^2 = 1$ and $r$ is odd, then either $q$ or $d$ must be even. So if $p = 2$, then one of the first two cases listed above must be true. Since $v^2 = (q^2 + dr^2) + 2qr\sqrt{d}$, then $m_p = p = 2$ in either situation. So in the following proof, we can assume that $p$ is an odd prime.

*Proof.* Let $a_n$ be the quadratic recursive sequence with characteristic polynomial $f(x) = x^2 - 2qx + 1$, so that $v^m = (qa_m - a_{m-1}) + (ra_m)\sqrt{d}$ for all $m \geq 1$.

The discriminant of $f$ is $\Delta = 4q^2-4 = (2r)^2 d$ since we are given that $q^2-dr^2 = 1$. Let $p$ be an odd prime, and let

$$c = c_p(f) = (2q)^2(1)^{-1} - 2 = 4q^2 - 2$$

in $\mathbb{F}_p$, the suborder number of $f(x)$ modulo $p$ as defined in §12.3. Note that $c = 2$ if and only if $q^2 = 1$ in $\mathbb{F}_p$, and since $p$ does not divide $r$, this occurs if and only if $p$ divides $d$. We saw in Theorem 12.3.3 that when $c = 2$, then the suborder of the sequence $a_n$ modulo $p$ equals $p$. This establishes case (1).

Now suppose that $c \neq 2$, so that $\mathrm{sub}_p(a_n) = \mathrm{sub}_p(c)$ by Theorem 12.3.3. Note that $c = -2$ if and only if $q = 0$ in $\mathbb{F}_p$, that is, $p$ divides $q$. In this case, $\mathrm{sub}_p(c) = 2 = \mathrm{sub}_p(a_n)$, from the observation that $v^2 = (q^2 + dr^2) + 2qr\sqrt{d}$. This establishes case (2).

Finally we can assume that $c \neq \pm 2$, in which case Theorem 12.3.5 applies to $m = m_p = \mathrm{sub}_p(c)$. Note that $c + 2 = (2q)^2$ and $c - 2 = 4q^2 - 4 = (2r)^2 d$, so that $\left(\frac{c+2}{p}\right) = 1$ and $\left(\frac{c-2}{p}\right) = \left(\frac{d}{p}\right)$. If $\left(\frac{d}{p}\right) = 1$, then $m$ divides $p-1$, but $e_2(m) < e_2(p-1)$. If $\left(\frac{d}{p}\right) = -1$, then $m$ divides $p+1$, but $e_2(m) < e_2(p+1)$. Cases (3) and (4) of this theorem follow. □

**Example.** The following table lists the first sixteen powers of $v = 2 + \sqrt{3}$, the fundamental solution of $x^2 - 3y^2 = 1$. (Here we can use direct calculation or the formula in Theorem 13.1.2.)

| $i$ | $v^i$ | $i$ | $v^i$ |
|---|---|---|---|
| 1 | $2 + \sqrt{3}$ | 9 | $70226 + 40545\sqrt{3}$ |
| 2 | $7 + 4\sqrt{3}$ | 10 | $262087 + 151316\sqrt{3}$ |
| 3 | $26 + 15\sqrt{3}$ | 11 | $978122 + 564719\sqrt{3}$ |
| 4 | $97 + 56\sqrt{3}$ | 12 | $3650401 + 2107560\sqrt{3}$ |
| 5 | $362 + 209\sqrt{3}$ | 13 | $13623482 + 7865521\sqrt{3}$ |
| 6 | $1351 + 780\sqrt{3}$ | 14 | $50843527 + 29354524\sqrt{3}$ |
| 7 | $5042 + 2911\sqrt{3}$ | 15 | $189750626 + 109552575\sqrt{3}$ |
| 8 | $18817 + 10864\sqrt{3}$ | 16 | $708158977 + 408855776\sqrt{3}$ |

Let $r_m$ be the coefficient of $\sqrt{3}$ in $v^m$. In the following table, we list each prime $p$ that divides some $r_m$ with $m \leq 16$, and the smallest such $m$ (that is, $m_p$ in the notation of Theorem 13.2.1) in each case.

| $p$ | 2 | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $m$ | 2 | 3 | 3 | 4 | 5 | 6 | 9 | 5 | 11 | 15 | 16 |

| $p$ | 41 | 43 | 53 | 71 | 97 | 181 | 193 | 571 | 607 | 2131 | 2521 | 3691 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $m$ | 7 | 11 | 9 | 7 | 8 | 10 | 12 | 11 | 16 | 13 | 14 | 13 |

We leave it to the reader to verify that these results are consistent with the claims of Theorem 13.2.1. We can also check that these results are as predicted by values of the suborder function in Table 12.1. Here with $q = 2$ and $r = 1$ in the smallest solution of $x^2 - dy^2 = 1$, we consider the quadratic recursive sequence defined by $f(x) = x^2 - 4x + 1$. The suborder number of this polynomial is $c_p(f) = 4^2 \cdot (1)^{-1} - 2 = 14$ for every prime $p$. If 14 is not congruent to 2 modulo $p$, then $\text{sub}_p(14) = m$ is the smallest value so that $p$ divides $r_m$. For instance, if $p = 11$, with $14 \equiv 3 \pmod{11}$, we verify from Table 12.1 that $m = 5$, while if $p = 53$, then $m = 9$. These values are as calculated above. ◊

**Example.** Let $v = 6 + \sqrt{35}$, the fundamental solution of $x^2 - 35y^2 = 1$. To illustrate the application of Theorem 13.2.1, we find the fundamental solution of $x^2 - (35n^2)y^2 = 1$ for several prime and composite values of $n$.

(1) Let $n = 7$. Since 7 is prime and divides $d = 35$, then $m = 7$ is the smallest positive integer for which 7 divides the coefficient of $\sqrt{35}$ in $v^m$. We calculate that $v^7 = 17057046 + 2883167\sqrt{35}$, with $2883167 = 7 \cdot 411881$, and conclude that

$$17057046 + 411881\sqrt{1715}$$

is the fundamental solution of $x^2 - 1715y^2 = 1$, where $1715 = 35 \cdot 7^2$.

(2) Let $n = 9$. Here $p = 3$ divides $q = 6$, and so $p$ divides the coefficient of $\sqrt{35}$ in $v^2 = 71 + 12\sqrt{35} = 71 + 4\sqrt{315}$. Now we can apply Theorem 13.2.1 to $71+4\sqrt{315}$ with $p = 3$. Since $p$ does not divide 4 but does divide 315, we conclude that $m = 3$ is the smallest positive integer for which $p$ divides the coefficient of $\sqrt{315}$ in $(71 + 4\sqrt{315})^m$. That is, $v^6$ is the smallest power of the original solution that we can use. Here $v^6 = 1431431 + 241956\sqrt{35}$ with $241956 = 9 \cdot 26884$, and we conclude that

$$1431431 + 26884\sqrt{2835}$$

is the fundamental solution of $x^2 - 2835y^2 = 1$, where $2835 = 35 \cdot 9^2$.

(3) Let $n = 15$. As above, 3 divides the coefficient of $\sqrt{35}$ in $v^2 = 71 + 12\sqrt{35} = 71 + 4\sqrt{315}$. Since 5 divides 315, then 5 divides the coefficient of $\sqrt{315}$ in $(v^2)^5 = v^{10} = 28860511751 + 4878316860\sqrt{35}$. With $4878316860 = 15 \cdot 325221124$, we conclude that

$$28860511751 + 325221124\sqrt{7875}$$

is the fundamental solution of $x^2 - 7875y^2 = 1$, where $7875 = 35 \cdot 15^2$.

(4) Let $n = 17$. With $q = 6$ in the fundamental solution of $x^2 - 35y^2 = 1$, we find that $c = 4q^2 - 2 = 142$ is the suborder number of $f(x) = x^2 - 2qx + 1$, as in the proof of Theorem 13.2.1. Since $142 \equiv 6 \pmod{17}$, we can read from Table 12.1 that $\text{sub}_{17}(142) = 8$. We calculate that $v^8 = 203253121 + 34356048\sqrt{35}$, with

$34356048 = 17 \cdot 2020944$, and so

$$203253121 + 2020944\sqrt{10115}$$

is the fundamental solution of $x^2 - 10115y^2 = 1$, where $10115 = 35 \cdot 17^2$.

(5) Let $n = 33$. As we have seen, 3 divides the coefficient of $\sqrt{35}$ in $v^2$, and we find that 11 divides the coefficient of $\sqrt{35}$ in $v^3$. (Since $\left(\frac{35}{11}\right) = \left(\frac{2}{11}\right) = -1$, this power of $v$ must divide $\frac{11+1}{2} = 6$.) It follows that 33 divides the coefficient of $\sqrt{35}$ in $v^6 = 1431431 + 241956\sqrt{35}$. We verify that $241956 = 33 \cdot 7332$, and conclude that

$$1431431 + 7332\sqrt{38115}$$

is the fundamental solution of $x^2 - 38115y^2 = 1$, where $38115 = 35 \cdot 33^2$.

(6) Let $n = 47$. Here $142 \equiv 1 \pmod{47}$, and so $\mathrm{sub}_{47}(142) = 6$ by Proposition 12.3.2. We find that $v^6 = 1431431 + 241956\sqrt{35}$ with $241956 = 47 \cdot 5148$, and we conclude that

$$1431431 + 5148\sqrt{77315}$$

is the fundamental solution of $x^2 - 77315y^2 = 1$, where $77315 = 35 \cdot 47^2$. ◊

**Exercise 13.2.2.** Use the method of Theorem 13.2.1 to find the fundamental solution of $x^2 - dy^2 = 1$ for the given value of $d$. Verify the results by applying the algorithm of Theorem 9.2.2 directly to each $d$.

(a) $d = 18 = 2 \cdot 3^2$.

(b) $d = 50 = 2 \cdot 5^2$.

(c) $d = 98 = 2 \cdot 7^2$.

(d) $d = 242 = 2 \cdot 11^2$.

(e) $d = 450 = 2 \cdot 15^2$.

(f) $d = 20 = 5 \cdot 2^2$.

(g) $d = 45 = 5 \cdot 3^2$.

(h) $d = 180 = 5 \cdot 6^2$.

(i) $d = 63 = 7 \cdot 3^2$.

(j) $d = 90 = 10 \cdot 3^2$.

## 13.3 Quadratic Subdomains of Positive Discriminant

As a final application of quadratic recursive sequences, we return to the question considered in Chapter 8. Let $\Delta$ be a discriminant, let $p$ be a prime number, and let $G_p$ be the form class group $\mathcal{F}_{p^2\Delta}$. In §8.1, we saw that elements of $G_p$ can be computed as products (or compositions) of elements of two of its subsets, $S_p$ and $K_p$, which can be listed in practice. The subset $S_p$ always has the same number of elements as the class group $\mathcal{F}_\Delta$, and there is an upper bound on the number of elements in $K_p$. In §8.2, we found that $K_p = K(\Delta, p)$ is the kernel of a projection homomorphism $\psi$ from $\mathcal{F}_{p^2\Delta}$ onto $\mathcal{F}_\Delta$, and in §8.3, we related the number of elements in $K_p$ to $\mathrm{Aut}(\phi)$, the group of automorphs of $\phi(x, y)$, the principal form of discriminant $\Delta$. This group is finite when $\Delta$ is negative, and we found a complete formula for $|K(\Delta, p)|$ in that case. On the other hand, $\mathrm{Aut}(\phi)$ is infinite when $\Delta$ is positive, making the general description of the kernel of a projection homomorphism somewhat more difficult in that case. In §13.1, however, we related these automorphs to terms in a particular quadratic recursive sequence. We will see in this section that this gives us a practical method of determining the kernel of a projection homomorphism. We begin with the statement of our main result.

**Theorem 13.3.1.** *Let $\phi = (1 : 0) = x^2 + \varepsilon xy + \frac{\varepsilon^2 - \Delta}{4} y^2$ be the principal form of some positive discriminant $\Delta$. Let $(q, r)$ be the smallest pair of positive integers for which $\phi(q, r) = 1$, and consider the quadratic recursive sequence $a_n$ with characteristic polynomial $f(x) = x^2 - (2q + \varepsilon r)x + 1$, that is,*

$$a_0 = 0, \quad a_1 = 1, \quad \text{and} \quad a_n = (2q + \varepsilon r)a_{n-1} - a_{n-2} \quad \text{for} \quad n \geq 2. \tag{13.3.1}$$

*For each prime number $p$, let $K(\Delta, p)$ be the kernel of the projection homomorphism from $\mathcal{F}_{p^2\Delta}$ to $\mathcal{F}_\Delta$, and let $s_p$ be the smallest positive integer so that $p$ divides $ra_{s_p}$. Then*

$$|K(\Delta, p)| = \frac{p - \left(\frac{\Delta}{p}\right)}{s_p} \tag{13.3.2}$$

*for every prime number $p$.*

Notice that $s_p = 1$ if $p$ divides $r$. Otherwise, $s_p$ is by definition the suborder of the $a_n$ sequence modulo $p$. In the proof of Theorem 13.3.1, we will use properties of the $p$-matrix group $G(\Delta, p)$ and the homomorphism $\chi_p : \mathrm{Aut}(\phi) \to G(\Delta, p)$, which were introduced for the proof of Theorem 8.1.3, a similar formula for $|K(\Delta, p)|$ when $\Delta$ is negative. We refer to §8.3 for all details.

*Proof.* Let $\phi = (1 : 0)$ be the principal form of some positive discriminant $\Delta$. If $p$ is a prime number, then the kernel of $\chi_p : \mathrm{Aut}(\phi) \to G(\Delta, p)$ is $\mathrm{Aut}(\phi) \cap \Gamma_p$, that is, the set of automorphs of $\phi$ for which $p$ divides the lower left-hand entry.

Theorem 8.3.6 implies that if $H(\Delta, p)$ is the image of $\mathrm{Aut}(\phi)$ under $\chi_p$, then

$$|K(\Delta, p)| = \frac{|G(\Delta, p)|}{|H(\Delta, p)|}.$$

Let $(q, r)$ be the smallest pair of positive integers with $\phi(q, r) = 1$, so that there is an automorph

$$U = \begin{bmatrix} q & s \\ r & t \end{bmatrix}$$

of $\phi$, and $\mathrm{Aut}(\phi) = \{\pm U^n \mid n \in \mathbb{Z}\}$. Let $a_n$ be the quadratic recursive sequence defined as in (13.3.1). Then Theorem 13.1.2 implies that $U^n = a_n U - a_{n-1} I$ is an element of $\Gamma_p$ if and only if $p$ divides $r a_n$. It follows that $s_p$, as defined in Theorem 13.3.1, is the number of distinct cosets of $\mathrm{Aut}(\phi) \cap \Gamma_p$ in $\mathrm{Aut}(\phi)$. But then $|H(\Delta, p)| = s_p$ as an application of the Fundamental Homomorphism Theorem (see Appendix C). Therefore, when $p$ is an odd prime, then

$$|K(\Delta, p)| = \frac{|G(\Delta, p)|}{|H(\Delta, p)|} = \frac{p - \left(\frac{\Delta}{p}\right)}{s_p},$$

using an expression for $|G(\Delta, p)|$ from the proof of Theorem 8.1.3. □

We illustrate Theorem 13.3.1 with an extended example, which also touches on other topics that we have considered in the latter part of this text.

**Example.** Let $\Delta = 29$, so that $\phi(x, y) = x^2 + xy - 7y^2$. We leave it to the reader to verify that the form class group of discriminant 29 has order one—the calculations necessary to establish this appear in the first example in §13.1. It follows that the order of $\mathcal{F}_{29p^2}$ is the same as the order of $K_p = K(29, p)$, the kernel of the projection homomorphism from $\mathcal{F}_{29p^2}$ to $\mathcal{F}_{29}$. As noted in Theorem 13.3.1, this order is, in most cases, determined by the suborder of a particular quadratic sequence.

In the first example in §13.1, we also saw that $(q, r) = (11, 5)$ is the smallest positive solution of $\phi(x, y) = 1$. Let $f(x) = x^2 - (2q + \varepsilon r)x + 1 = x^2 - 27x + 1$, the characteristic polynomial of the quadratic recursive sequence with

$$a_0 = 0, \quad a_1 = 1, \quad \text{and} \quad a_n = 27a_{n-1} - a_{n-2} \quad \text{for} \quad n \geq 2.$$

Here $s_5 = 1$ and $|K_5| = 5 - \left(\frac{29}{5}\right) = 4$, since $p = 5$ divides $r$. On the other hand, $s_p$ is the suborder of $a_n$ modulo $p$ for all other primes $p$. When $p = 2$ for instance, the sequence $a_n \bmod 2$ begins $0, 1, 1, 0, \ldots$, so that $s_2 = 3$. With $29 \equiv 5 \pmod 8$, the Kronecker symbol $\left(\frac{29}{2}\right)$ is $-1$, and equation (13.3.2) implies that $|K_2| = 1$.

For an odd prime $p$, we can apply the suborder function as defined in §12.3. The suborder number of $f(x)$ is $c = c_p(f) = 27^2(1)^{-1} - 2 = 727$ for all primes $p$. Here $c \equiv 2 \pmod p$ only for $p = 5$ and $p = 29$ (since $c - 2 = 725 = 5^2 \cdot 29$). We

have already noted that $|K_5| = 4$. On the other hand, the suborder of $a_n$ modulo $p = 29$ is 29, and so $|K_{29}| = 1$ by equation (13.3.2). For all other odd primes $p$, the same equation implies that

$$|K_p| = \frac{p - \left(\frac{29}{p}\right)}{\mathrm{sub}_p(727)}.$$

Using Table 12.1, along with Propositions 12.3.2 and 12.3.4 as needed, we can compile the following values of $|K_p|$. (Here $c = 727$ in $\mathbb{F}_p$ and $s = \mathrm{sub}_p(c)$.)

| $p$ | 3 | 7 | 11 | 13 | 17 | 19 | 23 | 31 | 37 | 41 | 43 | 47 | 53 | 59 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $c$ | 1 | $-1$ | 1 | $-1$ | $-4$ | 5 | $-9$ | 14 | $-13$ | $-11$ | $-4$ | 22 | $-15$ | 19 |
| $s$ | 2 | 3 | 6 | 3 | 9 | 10 | 11 | 16 | 19 | 7 | 22 | 24 | 13 | 29 |
| $\lvert K\rvert$ | 2 | 2 | 2 | 4 | 2 | 2 | 2 | 2 | 2 | 6 | 2 | 2 | 4 | 2 |

We will use the methods of Chapter 10 to confirm our claims directly for $p = 2$, $p = 3$, and $p = 5$.

(1) Let $p = 2$, and consider $G_2 = \mathcal{F}_{2^2 \cdot 29} = \mathcal{F}_{116}$. Here $u_{116} = \left\lfloor \sqrt{116/4} \right\rfloor = 5$, and the principal polynomial of discriminant $\Delta(29, 2) = 116$ is

$$\phi_2(x) = x^2 + 2x - 28.$$

Using a table listing $\phi_2(x)$ for $-6 \le x \le 4$ (omitted), we determine the following possible representatives of all classes of primitive quadratic forms in $\mathcal{Q}_{116}$:

$$(\pm 1 : -6), \quad (\pm 4 : -6), \quad (\pm 4 : -4), \quad (\pm 5 : -4), \quad (\pm 5 : -3).$$

(The forms $(\pm 2 : -6)$ are not primitive.) But when we apply the equivalence algorithm to one of these forms, such as $(1 : -6)$ in the following table, we find that all of these forms are equivalent.

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| $a$ | 1 | 4 | 5 | 5 | 4 | 1 |
| $k$ | $-6$ | $-6$ | $-4$ | $-3$ | $-4$ | $-6$ |

So $\mathcal{F}_{116}$ has only one element, confirming the claim that $|K_2| = 1$.

(2) If $p = 3$, then $u_{261} = 8$ and $\phi_3(x) = x^2 + 3x - 63$ is the principal polynomial of discriminant $\Delta(29, 3) = 261$. We find the following potential representatives of primitive forms $(a : k)$ with $|a| \le 8$:

$$(\pm 1 : -9), \quad (\pm 5 : -7), \quad (\pm 5 : -6), \quad (\pm 7 : -7), \quad (\pm 7 : -3).$$

We apply the equivalence algorithm to $(1 : -9)$ as follows.

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| $a$ | 1 | 9 | 7 | 5 | 9 | 5 | 7 | 9 | 1 |
| $k$ | $-9$ | $-9$ | $-3$ | $-7$ | $-6$ | $-6$ | $-7$ | $-3$ | $-9$ |

This time we find that

$$(1 : -9) \sim (-5 : -7) \sim (-5 : -6) \sim (7 : -7) \sim (7 : -3)$$

and

$$(-1 : -9) \sim (5 : -7) \sim (5 : -6) \sim (-7 : -7) \sim (-7 : -3).$$

But since the period length is even, $(1 : -9)$ is not equivalent to $(-1 : -9)$. Thus $\mathcal{F}_{261}$ has two elements, confirming the previous calculation of $|K_3|$. (Notice in this example that the ideal class group $\mathcal{C}_{261}$ has only one element, since $[1 : -9] = [-1 : -9]$.)

(3) If $p = 5$, then $u_{725} = 13$ and $\phi_5(x) = x^2 + 5x - 175$ is the principal polynomial of discriminant $\Delta(29, 5) = 725$. Here we find the following primitive forms as potential representatives of $\mathcal{F}_{725}$:

$$(\pm 1 : -15), \quad (\pm 7 : -14), \quad (\pm 7 : -12), \quad (\pm 13 : -12), \quad (\pm 13 : -6).$$

But now the equivalence algorithm produces the following data on two of these forms.

| $i$ | 0 | 1 | 2 |
|---|---|---|---|
| $a$ | 1 | 25 | 1 |
| $k$ | $-15$ | $-15$ | $-15$ |

| $i$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| $a$ | 7 | 13 | 13 | 7 | 7 |
| $k$ | $-14$ | $-12$ | $-6$ | $-12$ | $-14$ |

We conclude that there are four distinct classes of primitive quadratic forms of discriminant 725, with $(1 : -15)$, $(-1 : -15)$, $(7 : -14)$, and $(-7 : -14)$ as representatives. This confirms the previous calculation of $|K_5|$.

As an alternative test, recall that, in one characterization of the kernel, $K_p = K(\Delta, p)$ consists of the distinct classes, in $\mathcal{Q}_{p^2\Delta}$, of the quadratic forms $(1 : 0)$ and $(\phi(k) : pk)$, where $\phi(x)$ is the principal polynomial of discriminant $\Delta$ and $p$ does not divide $\phi(k)$. There is a maximum of $p - \left(\frac{\Delta}{p}\right)$ distinct classes in $K_p$, since it is always true that $(\phi(k) : pk) \sim (\phi(\ell) : p\ell)$ if $k \equiv \ell \pmod{p}$. But typically other equivalences exist when $\Delta$ is positive.

For example, consider $p = 17$ with $\Delta = 29$ as above. Here from the following values of $\phi(x) = x^2 + x - 7$,

| $x$ | $0, -1$ | $1, -2$ | $2, -3$ | $3, -4$ | $4, -5$ | $5, -6$ | $6, -7$ | $7, -8$ | $8, -9$ |
|---|---|---|---|---|---|---|---|---|---|
| $\phi(x)$ | $-7$ | $-5$ | $-1$ | 5 | 13 | 23 | 35 | 49 | 65 |

we find a list of eighteen potentially distinct elements in $K = K(29, 17)$:

$$(1 : 0), (-7 : 0), (-7 : -17), \ldots, (49 : 119), (49 : -136), (65 : 136).$$

Applying the equivalence algorithm to one of these forms, such as $(5 : -68) \sim (5 : -53)$ (the latter expression qualifying as a candidate form of discriminant

$\Delta_p = 29 \cdot 17^2$, in the terminology of §10.1),

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| $a$ | 5 | 5 | 23 | 65 | 7 | 29 | 7 | 65 | 23 | 5 |
| $k$ | −53 | −54 | −53 | −33 | −49 | −52 | −52 | −49 | −33 | −53 |

we find that nine of these eighteen forms are equivalent. (In this table, we use calculations of $\phi_p(x) = x^2 - 17x - 2023$, which are omitted.) We likewise find that the other nine forms are equivalent by applying the equivalence algorithm to $(1 : 0) \sim (1 : -54)$. So in fact $K_{17}$ contains only two distinct elements, as claimed in our previous calculations. ◊

**Exercise 13.3.1.** For each discriminant $\Delta$ below, find the integer $s_p$ as defined in Theorem 13.3.1, and find the order of the kernel, $K(\Delta, p)$, of the projection homomorphism from $\mathcal{F}_{p^2\Delta}$ to $\mathcal{F}_\Delta$ for each prime $p < 20$. (Note that these values of $\Delta$ are the same as those in Exercise 13.1.1.)

(a) $\Delta = 8$.

(b) $\Delta = 12$.

(c) $\Delta = 13$.

(d) $\Delta = 17$.

(e) $\Delta = 21$.

(f) $\Delta = 24$.

(g) $\Delta = 28$.

(h) $\Delta = 33$.

(i) $\Delta = 37$.

(j) $\Delta = 40$.

(k) $\Delta = 41$.

Finally, we note a consequence of Theorem 13.3.1, illustrated by the preceding example.

**Corollary 13.3.2.** *Let $\phi = (1 : 0) = x^2 + \varepsilon xy + \frac{\varepsilon^2 - \Delta}{4} y^2$ be the principal form of some positive discriminant $\Delta$, and let $(q, r)$ be the smallest pair of positive integers for which $\phi(q, r) = 1$. Let $p$ be an odd prime number that does not divide $\Delta$, $r$, or $2q + \varepsilon r$. Let $K_p$ be the kernel of the projection homomorphism from $\mathcal{F}_{p^2\Delta}$ to $\mathcal{F}_\Delta$. Then $|K_p|$ is even.*

*Proof.* Let $a_n$ be the quadratic recursive sequence with characteristic polynomial

$$f(x) = x^2 - (2q + \varepsilon r)x + 1.$$

Note that the discriminant of $f$ is

$$\Delta(f) = (2q + \varepsilon r)^2 - 4 = 4\left(q^2 + \varepsilon qr + \frac{\varepsilon^2 - \Delta}{4} r^2\right) - 4 + \Delta r^2 = \Delta r^2,$$

since $\phi(q, r) = 1$. The suborder number of $f(x)$ is

$$c = c_p(x) = (2q + \varepsilon r)^2 (1)^{-1} - 2 = (2q + \varepsilon r)^2 - 2$$

for every odd prime $p$. Thus $c + 2 = (2q + \varepsilon r)^2$ and $c - 2 = \Delta r^2$.

Now suppose that $p$ is an odd prime and does not divide $\Delta$, $r$, or $2q + \varepsilon r$. Then $c$ is not congruent to $\pm 2$ modulo $p$, so that $\left(\frac{c+2}{p}\right) = 1$ and $\left(\frac{c-2}{p}\right) = \left(\frac{\Delta}{p}\right)$. Theorem 12.3.5 applies, and we can conclude the following.

(1) If $\left(\frac{\Delta}{p}\right) = 1$, then $\text{sub}_p(c)$ divides $\frac{p-1}{2}$.

(2) If $\left(\frac{\Delta}{p}\right) = -1$, then $\text{sub}_p(c)$ divides $\frac{p+1}{2}$.

That is, $\text{sub}_p(c)$ divides $\frac{1}{2}\left(p - \left(\frac{\Delta}{p}\right)\right)$ in all such cases. But now equation (13.3.2) shows that $|K_p|$ is an integer, and must be even. □

## Applications of Quadratic Recursive Sequences—Review

If $\phi(x, y)$ is the principal form of some positive discriminant $\Delta$, then there is a smallest pair of positive integers $(q, r)$ for which $\phi(q, r) = 1$. We can use this solution to define a quadratic recursive sequence $a_n$ with characteristic polynomial $f(x) = x^2 - (2q + \varepsilon r)x + 1$ (where $\varepsilon = \varepsilon_\Delta$). In this chapter, we looked at several applications of this quadratic sequence to arithmetic problems concerning quadratic forms and quadratic domains of positive discriminant.

(1) All solutions in positive integers of $\phi(x, y) = 1$ have the form

$$(q_n, r_n) = (a_n q - a_{n-1}, a_n r)$$

with $n \geq 1$. There is a similar expression for all automorphs of $\phi$. (See Theorem 13.1.2.)

(2) If we know the fundamental solution of Pell's equation, $x^2 - dy^2 = 1$, where $d$ is squarefree, then we can determine the fundamental solution of $x^2 - (m^2 d)y = 1$ in terms of this associated quadratic sequence $a_n$. When $m = p$ is prime, we can use the suborder of $a_n$ modulo $p$ to help calculate this solution. We can apply properties of the suborder function on $\mathbb{F}_p$ to limit the possibilities for where this solution may occur.

(3) Using the automorphs of the principal polynomial of a positive discriminant $\Delta$, we can establish a formula for the order of the kernel of a projection homomorphism $\psi : \mathcal{F}_{p^2\Delta} \to \mathcal{F}_\Delta$ for every prime $p$. This formula involves the suborder of the associated quadratic recursive sequence, $a_n$. Again, properties of the suborder function give us information about possibilities for the order of the kernel. In theory then, it suffices to consider the form class group $\mathcal{F}_\Delta$ for every *primitive* positive discriminant $\Delta$, as we saw was the case for negative discriminants in Chapter 8.

# Concluding Remarks

In this book, we have seen how attempts to answer arithmetic questions, particularly about sums of two squares and similar representations by quadratic forms, can lead us to larger sets of numbers, such as the Gaussian integers and other quadratic domains. Questions about properties of these domains can, in turn, inspire consideration of the algebraic structure of these and related sets. In particular, we found that class groups of ideals help us to categorize and compute representations of integers by corresponding quadratic forms.

A key aspect of our approach has been the introduction of several new computational techniques with these objects, via "ideal number" expressions for elements and ideals of quadratic domains, and similar ideal notation for binary quadratic forms. Using this notation, we developed systematic methods of determining distinct classes of ideals for an arbitrary discriminant. Algebraic properties of the resulting class groups typically give us information about which integers are properly represented by various quadratic forms of a fixed discriminant. We demonstrated a reduction process whereby an arbitrary quadratic form can be replaced by an equivalent class representative, and we saw how this method also allows us to construct representations of integers by one of a fixed collection of quadratic forms, when those expressions are known to exist.

We hope that readers, whether new to algebraic number theory or with some expertise in that field, have found the computational focus of this work to be both enlightening and provocative of further questions. We fully acknowledge, however, that our scope has been deliberately narrow from the algebraic standpoint, as we have essentially restricted our attention to quadratic extension fields of the rational numbers, and their subdomains of integers. There are many other directions that a study of number theory can take.

(1) Even if one wishes to maintain a focus on representations by binary quadratic forms, a more complete study would inevitably lead beyond quadratic extensions of the rational numbers. For example, in §7.3, we found that consideration of the ideal class group $\mathcal{C}_{-56}$ gave us a criterion for an integer to be represented by $x^2 + 14y^2$ *or* by $2x^2 + 7y^2$. To distinguish between those quadratic forms requires a degree-two extension of $\mathbb{Q}(\sqrt{-14})$. We are then led to classify

integers, units, irreducible elements, and so forth in arbitrary finite extensions of the rational numbers.

(2) There is, of course, no need to restrict our attention to quadratic expressions. Among many other possibilities, one could consider *elliptic curves*, which can be expressed in one form as $y^2 = f(x)$, where $f(x)$ is a *cubic* polynomial with distinct roots in the complex numbers. A study of these objects leads to algebraic questions of a different type, as solutions of these equations exhibit a group structure under an operation defined geometrically. As another example, *Fermat's Last Theorem*, the claim that $x^n + y^n = z^n$ has no nonzero solutions in integers when $n > 2$, was an important impetus in the development of algebraic methods in number theory.

(3) In a completely different direction, one could consider questions about the distribution of prime numbers in the integers. Questions of this type have been approached most often using techniques of complex analysis, and comprise the field of *analytic number theory*. Important results in this direction include Dirichlet's Theorem on the existence of prime numbers in arithmetic progressions, and the Prime Number Theorem describing the asymptotic behavior of proportion of prime number among all positive integers less than a given value.

## References and Suggested Reading

To conclude, we mention some sources for further study. There is no shortage of works on algebraic number theory, particularly at the graduate level. Here we will list some of the more accessible treatments, and we make no claim to be comprehensive on that score.

Two highly recommended classical works are *Lectures on Number Theory* by P. G. L. Dirichlet, originally published in 1863 with supplements by Dedekind, and Dedekind's own treatise *Theory of Algebraic Integers* (1877). Dirichlet's text contains an extensive development of binary quadratic forms which, although with slightly different definitions, includes many of the key results of our text. As we have already noted on occasion, Dedekind's work describes the development of ideals from Kummer's original notion of ideal numbers. Both of these books appear in translations by John Stillwell (Dirichlet as a joint publication of the American Mathematical Society and London Mathematical Society (1999) and Dedekind by Cambridge University Press (1996)). Stillwell's introductions to both works are particularly valuable in putting important concepts in historical context.

Two more recent but still classical accounts are *An Introduction to the Theory of Numbers* by G. H. Hardy and E. M. Wright (originally published in 1938, with its sixth edition appearing in Oxford University Press in 2008) and *The Higher*

*Arithmetic* by H. Davenport (1952, with its eighth edition published by Cambridge University Press in 2008). Both works contain much of our background development of continued fractions and quadratic forms.

Among books with a somewhat similar focus to ours, we will recommend two in particular. *Advanced Number Theory* by Harvey Cohn (1980, Dover), originally published as *A Second Course in Number Theory* (1962, Wiley), contains many examples of calculations with ideal classes of quadratic domains, which inspired similar computations (with different notation) in this text. Cohn's work also includes many important details on connections between quadratic forms and ideals of quadratic domains. As its title suggests, *Primes of the Form* $x^2 + ny^2$ by David A. Cox (1989, Wiley) concentrates on a particular question concerning representations by quadratic forms. The first chapter covers the classical approach of composition, equivalence, and genera in the form class group, which we have considered in this text. Later chapters introduce more advanced methods—class field theory and complex multiplication with elliptic functions and elliptic curves—in cases that cannot be answered in full by the first approach. The progression from classical methods to those that require more general calculations with algebraic integers makes Cox's book a useful follow-up to this one, particularly for those interested in more details on integers represented by an arbitrary quadratic form.

Other sources worthy of mention include *Fundamental Number Theory with Applications* (1998, CRC Press) and *Algebraic Number Theory* (1999, CRC Press), both by Richard A. Mollin, from which we adapted many of our computational methods with irrational quadratic numbers, *Algebraic Number Theory and Fermat's Last Theorem* (2002, A K Peters) by Ian Stewart and David Tall, an accessible account of the algebraic concepts behind the recently proved claim of Fermat, and *A Comprehensive Course in Number Theory* (2012, Cambridge University Press) by Alan Baker, which addresses many topics from advanced number theory in a rigorous but concise approach.

Finally, we mention that in the course of our preparation of this text, two new books appeared addressing algebraic number theory at an undergraduate level, *Algebraic Number Theory* (2014, Springer Undergraduate Mathematics Series) by Frazer Jarvis, and *A Conversational Introduction to Algebraic Number Theory* (2017, AMS Student Mathematical Library, Volume 84) by Paul Pollack. Pollack's book in particular begins with a consideration of quadratic extensions of the rational numbers, which is then generalized to more arbitrary algebraic extensions. As such, this work would be a natural follow-up to our text.

# List of Notation

| Notation | Description | Page |
|---|---|---|
| $n \bmod m$ | remainder under the division algorithm | 1 |
| $\gcd(a, b)$ | greatest common divisor | 2 |
| $\operatorname{lcm}(a, b)$ | least common multiple | 3 |
| $a \equiv b \pmod{m}$ | congruence modulo an integer | 4 |
| $\mathbb{Z}_m$ | congruence classes modulo an integer | 4 |
| $\operatorname{ord}_m(a)$ | order of an integer with respect to a modulus | 4 |
| $\left(\frac{a}{p}\right)$ | Legendre symbol | 7 |
| $n_m(f)$ | number of solutions of $f(x) \equiv 0 \pmod{m}$ | 12 |
| $e_p(m)$ | exponent of a prime in an integer | 13 |
| $\left(\frac{\Delta}{2}\right)$ | Kronecker symbol | 13 |
| $\left(\frac{a}{q}\right)$ | Jacobi symbol | 14 |
| $\mathbb{Z}[i]$ | Gaussian integers | 25 |
| $\overline{z}$ | conjugate of a complex number | 26 |
| $N(z)$ | norm of a complex number | 26 |
| $g[a : k]$ | ideal form of a Gaussian integer | 32 |
| $\lfloor x \rfloor$ | largest integer $\leq x$ | 50 |
| $\mathbb{Q}(\sqrt{d})$ | quadratic field | 57 |
| $\overline{v}$ | conjugate of a quadratic number | 57 |
| $N(v)$ | norm of a quadratic number | 57 |
| $\Delta(v)$ | discriminant of a quadratic number | 60 |
| $\Delta(d, \gamma)$ | discriminant | 61 |
| $d_\Delta$ | squarefree part of a discriminant | 61 |
| $\gamma_\Delta$ | index of a discriminant | 61 |
| $z_\Delta$ | basis element of a discriminant | 61 |
| $\varepsilon_\Delta$ | basis index of a discriminant | 61 |
| $D_\Delta$ | quadratic domain of a discriminant | 61 |

| | | |
|---|---|---|
| $\phi_\Delta(x, y)$ | principal form of a discriminant | 62 |
| $\phi_\Delta(x)$ | principal polynomial of a discriminant | 62 |
| $g[a : k]$ | ideal form of a quadratic integer | 68 |
| $g[a : k]$ | ideal number | 75 |
| $u_\Delta$ | upper bound of a discriminant | 77 |
| $\langle v, w\rangle$ | ideal of combinations | 94 |
| $\langle v\rangle$ | principal ideal | 94 |
| $[a : k]$ | $\mathbb{Z}$-combinations of $\{a, k + z\}$ | 96 |
| $N(A)$ | norm of an ideal | 97 |
| $v \equiv w \pmod{A}$ | congruence modulo an ideal | 98 |
| $A + B$ | sum of ideals | 101 |
| $\overline{A}$ | conjugate of an ideal | 102 |
| $AB$ | product of ideals | 107 |
| $\gamma(A)$ | index of an ideal | 108 |
| $\Delta(f)$ | discriminant of a quadratic form | 132 |
| $\mathcal{Q}_\Delta$ | quadratic forms of a fixed discriminant | 132 |
| $\gamma(f)$ | index of a quadratic form | 132 |
| $M_f$ | matrix of a quadratic form | 133 |
| $A^T$ | transpose of a matrix | 133 |
| $\overline{A}$ | conjugate of a matrix | 133 |
| $\overline{f}(x, y)$ | conjugate of a quadratic form | 133 |
| $-f(x, y)$ | negative of a quadratic form | 133 |
| $-\overline{f}(x, y)$ | negative conjugate of a quadratic form | 133 |
| $(a : k)$ | ideal notation for a quadratic form | 134 |
| $\Gamma$ | group of unimodular matrices | 136 |
| $f \circ U$ | unimodular matrix applied to a quadratic form | 136 |
| $f \sim g$ | equivalence of quadratic forms | 137 |
| $f \leftrightarrow g$ | involution of a quadratic form | 138 |
| $f \simeq g$ | norm equivalence of quadratic forms | 138 |
| $f \rightarrow_u g$ | translation of a quadratic form | 139 |
| $\mathrm{Aut}(f)$ | automorphs of a quadratic form | 142 |
| $\mathbf{x} \sim_f \mathbf{y}$ | $f$-equivalence of ordered pairs | 143 |
| $\left(\frac{f}{p}\right)$, $\left(\frac{-1}{f}\right)$, etc. | genus symbols of a quadratic form | 147 |
| $f \approx g$ | genus equivalence of quadratic forms | 147 |
| $A_f$ | ideal of a quadratic form | 154 |
| $A \sim B$ | equivalence of ideals | 154 |
| $\{u, v\} \circ U$ | unimodular matrix applied to an ordered basis | 161 |
| $f_S$ | quadratic form of an ordered basis | 161 |
| $f_1 \cdot f_2$ | composition of quadratic forms | 167 |
| $\mathcal{C}_\Delta$ | ideal class group | 172 |

| | | |
|---|---|---|
| $\mathcal{F}_\Delta$ | form class group | 173 |
| $(n_1, n_2, \ldots, n_m)$ | invariant factor type | 178 |
| $\left(\frac{A}{p}\right)$, $\left(\frac{-1}{A}\right)$, etc. | genus symbols of an ideal | 191 |
| $A \approx B$ | genus equivalence of ideals | 191 |
| $[A] \approx [B]$ | genus equivalence of ideal classes | 191 |
| $\mathcal{G}_\Delta$ | principal genus | 192 |
| $G^2$ | subgroup of squares in an abelian group | 193 |
| $g \leftrightarrow_u f$ | involution/translation of quadratic forms | 221 |
| $A \leftrightarrow C$ | involution of ideals | 222 |
| $S_p$ | representatives of $\mathcal{C}_\Delta$ in $\mathcal{C}_{p^2\Delta}$ | 228 |
| $K_p$ | kernel of $\mathcal{C}_{p^2\Delta}$ | 229 |
| $\psi : \mathcal{F}_{p^2\Delta} \to \mathcal{F}_\Delta$ | projection homomorphism | 235 |
| $\Gamma_p$ | $p$-congruence subgroup | 236 |
| $f \sim_p g$ | $p$-equivalence of quadratic forms | 236 |
| $K(\Delta, p)$ | kernel of a projection homomorphism | 238 |
| $GL_2(\mathbb{Z}_p)$ | nonsingular matrices over $\mathbb{Z}_p$ | 240 |
| $G(\Delta, p)$ | $p$-matrix group of discriminant $\Delta$ | 240 |
| $\chi_p$ | $p$-automorph map | 241 |
| $H(\Delta, p)$ | image of a $p$-automorph map | 241 |
| $F_n$ | Fibonacci sequence | 250 |
| $\langle q_0, q_1, \ldots, q_i, w \rangle$ | finite continued fraction | 259 |
| $\langle q_0, q_1, q_2, \ldots \rangle$ | infinite simple continued fraction | 260 |
| $\mathrm{ord}(a)$ | order of an element of a group | 334 |
| $r_n$ | quadratic recursive sequence | 336 |
| $\mathrm{ord}_m(r_n)$ | order of a quadratic sequence | 344 |
| $\mathrm{sub}_m(r_n)$ | suborder of a quadratic sequence | 344 |
| $\mathbb{F}_p$ | field with $p$ elements | 344 |
| $\mathbb{E}_p$ | field with $p^2$ elements | 345 |
| $F[x]$ | polynomials over a field | 345 |
| $F^\times$ | group of units of a field | 348 |
| $\mathrm{sub}_p(c)$ | suborder function on $\mathbb{F}_p$ | 350 |
| $c_p(f)$ | suborder number of a polynomial | 351 |
| $c_n$ | suborder sequence modulo a prime | 357 |
| $d_n$ | suborder subsequence modulo a prime | 361 |
| $\phi(m)$ | Euler totient function | 363 |

# Index

AMS / MAA DOLCIANI MATHEMATICAL EXPOSITIONS

*Quadratic Number Theory* is an introduction to algebraic number theory for readers with a moderate knowledge of elementary number theory and some familiarity with the terminology of abstract algebra. By restricting attention to questions about squares the author achieves the dual goals of making the presentation accessible to undergraduates and reflecting the historical roots of the subject. The representation of integers by quadratic forms is emphasized throughout the text.

Lehman introduces an innovative notation for ideals of a quadratic domain that greatly facilitates computation and he uses this to particular effect. The text has an unusual focus on actual computation. This focus, and this notation, serve the author's historical purpose as well; ideals can be seen as number-like objects, as Kummer and Dedekind conceived of them. The notation can be adapted to quadratic forms and provides insight into the connection between quadratic forms and ideals. The computation of class groups and continued fraction representations are featured—the author's notation makes these computations particularly illuminating.

*Quadratic Number Theory,* with its exceptionally clear prose, hundreds of exercises, and historical motivation, would make an excellent textbook for a second undergraduate course in number theory. The clarity of the exposition would also make it a terrific choice for independent reading. It will be exceptionally useful as a fruitful launching pad for undergraduate research projects in algebraic number theory.

ISBN 978-1-4704-4737-3
9 781470 447373
DOL/52

For additional information and updates on this book, visit
**www.ams.org/bookpages/dol-52**

AMS
www ams org