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