Preface

This book, like others in the SUMS series, is designed to be suitable for undergraduate courses. While many institutions may not offer such courses in algebraic number theory, some may instead offer the possibility for students to take reading courses, or to write projects, in more diverse areas of pure mathematics. It is my hope that this book is suitable for any of these options.

Outline of the Book

Let us now summarise the content of the book. The first chapter begins with a review of the Euclidean algorithm and its importance in the proof of the Fundamental Theorem of Arithmetic, which states that every integer can be uniquely factorised into prime numbers. We then consider some questions about the integers which can be addressed by working with the Gaussian integers $\mathbb{Z}[i]$, and for which analogues of unique factorisation are essential to the proof.

Motivated by the need to consider larger sets than $\mathbb{Z}$, the second chapter defines algebraic numbers, and number fields and their rings of integers. These are the sets which are going to generalise the rational numbers and the integers and in which we are going to be studying arithmetic throughout the rest of the book. The third chapter continues this theme, studying natural questions about rings of integers in number fields. Some of these further questions are of a harder nature than those in Chap. 2, and the reader (or instructor) may wish to omit some of this material on a first reading.

Unique factorisation forms the topic of the next two chapters; we would like to know whether the ring of integers in a given number field has unique factorisation or not, in order to deduce interesting results such as those at the end of the first chapter. Although unique factorisation does not always hold (indeed, it's quite rare!), Kummer suggested a way to recover it, by adding "ideal numbers". Later, Dedekind reformulated this to give a definition of ideals in the rings of integers, and Chap. 4 considers properties of ideals. Prime ideals, analogues of prime numbers, are studied in the fifth chapter, whose main result is the uniqueness of factorisation of ideals into prime ideals. The chapter also introduces the class number and class group, which measure the failure of unique factorisation of elements.

Chapter 6 considers the case of imaginary quadratic fields, which is probably the simplest family of worked examples. After considering problems such as finding the imaginary quadratic fields with unique factorisation, the relation with the theory of positive definite quadratic forms is explained, which gives a convenient way to make computations of class numbers of imaginary quadratic fields.

Before considering further examples, we develop some theory in Chap. 7. This chapter studies geometry of numbers and the class group, proving some useful general theoretical results, which then get illustrated in Chap. 8, which focuses on other classes of fields with small degree. To treat the case of real quadratic fields, we introduce Pell's equation, and its solution via continued fractions. Next, Chap. 9 considers number fields generated by roots of unity, and in particular, Kummer's work on Fermat's Last Theorem.

These nine chapters are already more than enough to form a full one-semester course in a typical UK University. But this is just the start of the theory, almost all understood by the mid-nineteenth century. I have also included additional chapters, which could form the basis for further reading, or for student projects. These concern explicit class number formulae, and the number field sieve. The first chapter, on analytic methods, considers the Riemann zeta function, and zeta functions of number fields, culminating in the analytic class number formula, and a brief discussion of p-adic numbers, of great importance for modern number theorists. The advent of the computer has led to increased interest in the problem of factorisation of integers, through the RSA cryptosystem, and the current method of choice, which uses many techniques of algebraic number theory, is the number field sieve. But today the field is extremely active, and has expanded far beyond the contents of this book. I am very conscious that there are topics which might have been treated as part of this list which have been omitted: the relation to Galois Theory, further ramification theory, class field theory, p-adic methods and transcendence theory, amongst others.

A Note for Instructors

There are many possible combinations of topics that could form a suitable course. A basic one-semester course at an undergraduate level at a typical UK University might review Chap. 1 quickly, spend quite a lot of time on Chap. 2, briefly touch on some of the topics in Chap. 3 and cover Chaps. 4 and 5 fairly fully, with examples taken from parts of Chaps. 6 and 8. Any remaining time might be spent on additional topics from some of the later chapters, such as quadratic forms (from Chap. 6), the finiteness of the class number (from Chap. 7), or roots of unity and Fermat's Last Theorem (from Chap. 9). The relationship between class numbers of imaginary quadratic fields and quadratic forms (Chap. 6), analytic methods (Chap. 10) and the number field sieve (Chap. 11) are more likely to be suitable for undergraduate project work. Some of this material is also likely to be suitable for beginning graduate students.

Prerequisites

I have tried to keep the prerequisites to a minimum. Nevertheless, there are a number of topics which might be useful, and which most readers will have met in their previous studies. It is my intention that readers should be able to read most of the text without previous courses in these topics, but it is inevitably true that previous acquaintance with them will be helpful, and readers without this knowledge may occasionally need to consult additional sources for this background. These topics include: elementary number theory (here [7] is an excellent source), a first course in linear algebra (including vector spaces over fields), a first course in group theory (little beyond Lagrange's Theorem is required) and some basic understanding of rings and fields. Even here, it should be possible for a reader without this knowledge to follow the material, with the understanding that a ring is just a set in which one can add, subtract and multiply, in such a way that all the algebraic properties of $\mathbb{Z}$ are satisfied (in particular, all our rings are commutative and have a multiplicative identity). Slightly more advanced concepts such as ideals and quotient rings are an essential part of algebraic number theory (and were, in fact, motivated by the theory, as we will see), and they are introduced from scratch. Similarly, I hope that readers would be able to follow the text with the idea that a field is just a set in which one can add, subtract, multiply and divide by non-zero elements, in such a way that all the algebraic properties satisfied by $\mathbb{Q}$ continue to hold.

A Note on Computer Packages

It was a difficult decision to exclude explicit mention of computer packages within the text. There is considerable scope for using computer packages to study algebraic number theory; many have been written and new ones continue to appear; had I written the book 5 years ago, I might well have written examples with a different package to my package of choice today, and 10 years ago I might have preferred a different choice again.

But it would seem to be a mistake to write an undergraduate text with no mention of resources available for students to study the subject further, or to develop understanding by finding interesting examples with the aid of a computer package. Partly to make amends, here is a brief guide to available resources at the time of writing.

An excellent list of packages and online tables of examples can be found at the *Number Theory Web*; see http://www.numbertheory.org/ntw/N1.html. All the packages listed here are linked to from this page.

Algebraic number theory is a relatively specialist area, and is not so well served by well-known general-purpose computer packages such as Maple or Mathematica, although both have their uses. The MAGMA Computational Algebra System (http://www.magma.maths.usyd.edu.au/magma/) has the best treatment of algebraic number theory of the major packages; however, it is comparatively expensive, and less likely to be installed on University computer systems.

However, there are free alternatives which have been particularly developed for use in algebraic number theory. (Of course, the disadvantage of such programs is that there may be little in the way of documentation or support.)

One such program is PARI-GP (http://www.pari.math.u-bordeaux.fr/), developed originally by Henri Cohen (Bordeaux) and a team of co-workers. Cohen has also written several nice textbooks on computational number theory.

More recently, William Stein has been heading the SAGE project to develop an open-source equivalent to Maple, Mathematica and MAGMA. It can be downloaded from http://www.sagemath.org/; the project incorporates parts of PARI-GP.

http://www.springer.com/978-3-319-07544-0

Algebraic Number Theory
Jarvis, F.
2014, XIII, 292 p. 3 illus., Softcover

ISBN: 978-3-319-07544-0