Preface

Number theory has a rich history. For many years it was one of the purest areas of pure mathematics, studied because of the intellectual fascination with properties of integers. More recently, it has been an area that also has important applications to subjects such as cryptography. The goal of this book is to present both sides of the picture, giving a selection of topics that we find exciting.

The book is designed to be used at several levels. It should fit well with an undergraduate course in number theory, but the book has also been used in a course for advanced high school students. It could also be used for independent study. We have included several topics beyond the standard ones covered in classes in order to open up new vistas to interested students.

The main thing to remember is number theory is supposed to be fun. We hope you enjoy the book.

The Chapters. The flowchart (following this preface) gives the dependencies of the chapters. When a section number occurs with an arrow, it means that only that section is needed for the chapter at the end of the arrow. For example, only the statement of quadratic reciprocity (Section 9.1) from Chapter 9 is needed in Chapter 10.

The core material is Chapters 1, 2, 4, 7, along with Sections 6.1 and 9.1. These should be covered if at all possible. At this point, there are several possibilities. It is highly recommended that some sections of Chapters 3, 5, and 8 be covered. These present some of the exciting applications of number theory to various problems, especially in cryptography. If time permits, some of the more advanced topics from Chapters 9 through 16 can be covered. These chapters are mostly independent of one another, so the choices depend on the interests of the audience.

We have tried to keep the prerequisites to a minimum. Appendix A treats some topics such as induction and the binomial theorem.

Our experience is that many students have seen these topics but that a review is worthwhile. The appendix also treats Fibonacci numbers since they occur as examples in various places throughout the book.

Notes to the reader. At the end of each chapter, we have a short list of Chapter Highlights. We were tempted to use the label "If you don't know these, no one will believe you read the chapter." In other words, when you finish a chapter, make sure you thoroughly know the highlights. (Of course, there is more that is worth knowing.) At the end of several sections, there are problems labeled "CHECK YOUR UNDERSTANDING." These are problems that check whether you have learned some basic ideas. The solutions to these are given at the ends of the chapters. You should not leave a topic until you can do these problems easily.

Problems. At the end of every chapter, there are problems to solve. The *Exercises* are intended to give practice with the concepts and sometimes to introduce interesting ideas related to the chapter's topics. The *Projects* are more substantial problems. Often, they consist of several steps that develop ideas more extensively. Although there are exceptions, generally they should take much longer to complete. Several could be worked on in groups. Computations have had a great influence on number theory and the *Computer Explorations* introduce this type of experimentation. Sometimes they ask for specific data, sometimes they are more open-ended. But they represent the type of exploration that number theorists often do in their research.

Appendix B contains answers or hints for the odd-numbered problems. For the problems where the answer is a number, the answer is given. When the exercise asks for a proof, usually a sketch or a key step is given.

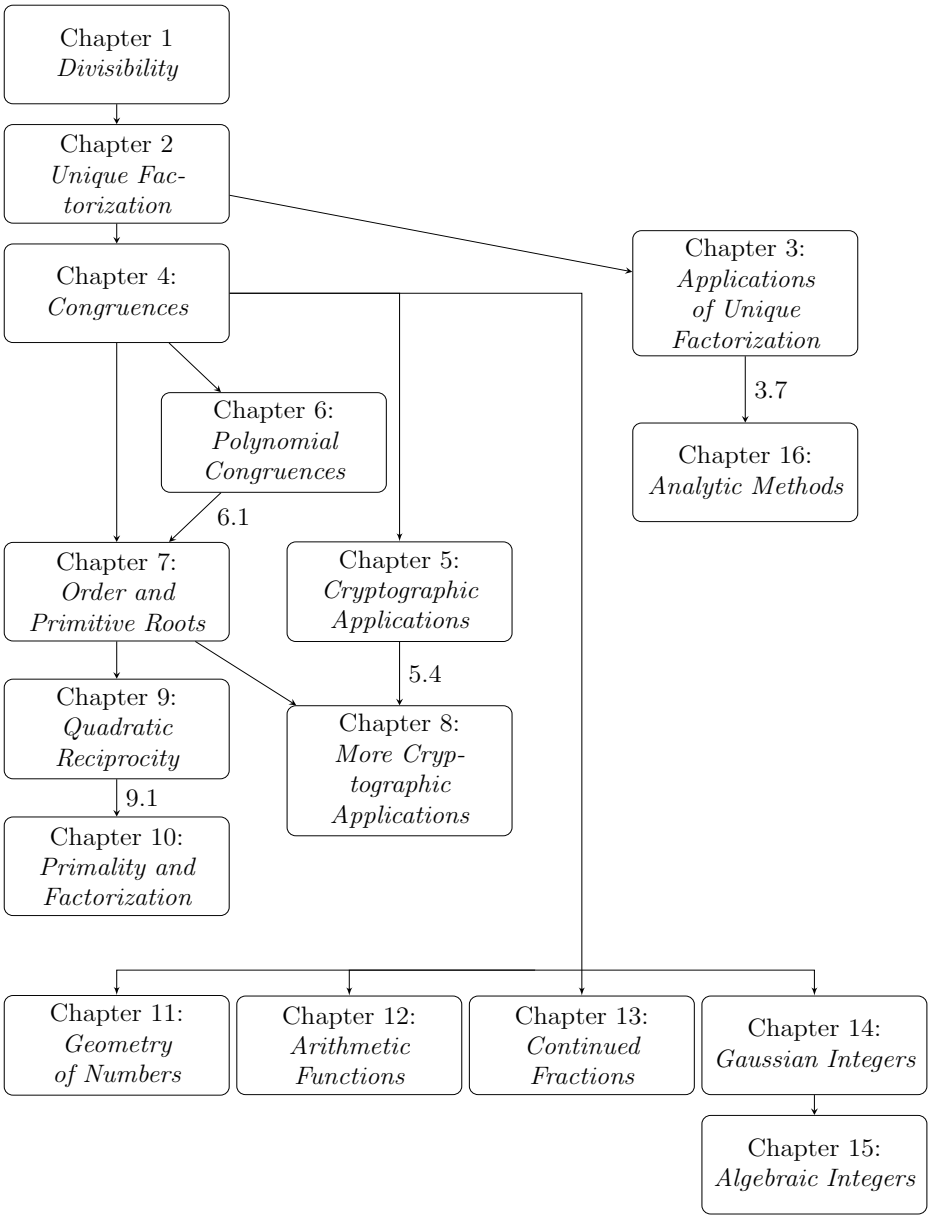
Computers. Many students are familiar with computers these days and many have access to software packages such as Mathematica©, Maple©, Matlab©, Sage, or Pari that perform number theoretical calculations with ease. Some of the exercises (the ones that use numbers of five or more digits) are intended to be used in conjunction with a computer. Many can probably be done with an advanced calculator. The Computer Explorations definitely are designed for students with computer skills.

Acknowledgments. Jim Kraft wants to thank the Gilman School for its generous support during the writing of this book and his students Rishi Bedi, John Chirikjian, Anthony Kim, and John Lee, whose comments helped make this a better book. Many thanks are also due to Manjit Bhatia, who made many very useful suggestions. We both want to thank our many students over the years who have taught us while we have taught them. This book would not have been possible without them.

We welcome comments, corrections, and suggestions. Corrections and related matter will be listed on the web site for the book (www.math.umd.edu/∼lcw/numbertheory.html).

James S. Kraft
Gilman School
jkraft@gilman.edu

Lawrence C. Washington
University of Maryland
lcw@math.umd.edu


Chapter 1
Divisibility
Chapter 2
Unique Factorization
Chapter 4:
Congruences
Chapter 3:
Applications of Unique Factorization
3.7
Chapter 16:
Analytic Methods
Chapter 6:
Polynomial Congruences
6.1
Chapter 7:
Order and Primitive Roots
Chapter 5:
Cryptographic Applications
5.4
Chapter 9:
Quadratic Reciprocity
Chapter 8:
More Cryptographic Applications
9.1
Chapter 10:
Primality and Factorization
Chapter 11:
Geometry of Numbers
Chapter 12:
Arithmetic Functions
Chapter 13:
Continued Fractions
Chapter 14:
Gaussian Integers
Chapter 15:
Algebraic Integers