Preface

Note to the Instructor

This book presents material suitable for an undergraduate course in elementary number theory from a computational perspective. It seeks to not only introduce students to the standard topics in elementary number theory, but also to the formulation of conjectures from experimental data. Each topic is motivated by a question to be answered, followed by some experimental data and, eventually, a statement and proof of a theorem. There are numerous opportunities throughout the chapters and exercises for the students to engage in (guided) open-ended exploration. The goal of this exploration is for students to engage with examples, deepen understanding, notice patterns, and formulate conjectures. To be effective as a learning mechanism, it is important that these explorations culminate in clear mathematical statements of what has been discovered. It is my hope that at the end of their course the students will understand how mathematics is developed from asking questions, to gathering data, to formulating and proving theorems.

There is a heavy emphasis on computation throughout the book, including several investigations within each chapter guiding the student through experimental investigations related to the material. At the end of each chapter, the exercises are divided into three sections: computational exercises, theoretical (proof-based) exercises, and explorations. The computational exercises range from simple calculations to more difficult algorithms, with an emphasis on working with explicit examples of the concepts described in the chapter. The ones marked with ✍ are meant to be done with paper and pencil, the rest with a computer algebra system. The theoretical exercises are more like the "standard" exercises you would see in any number theory textbook, where students are asked to prove some additional concepts related to those in the chapter. As with the computational exercises, the difficulty varies, but the emphasis is on developing rigorous proofs of the statements. The explorations are meant to be treated as open-ended projects, where students put into practice the following methodology:

(a) Ask a question.
(b) Generate data.
(c) Formulate conjectures.
(d) Test your conjectures.
(e) Try to prove your conjectures.

Many of the exploration topics are areas of current research. However, the student is provided with guiding questions that ensure they will be able to make progress on a subset of the problem. These explorations also serve as mathematical writing exercises, where the student must describe the problem, their steps toward gathering data, and their conclusions in the form of conjectures.

The mathematical prerequisites for this book are few. A basic understanding of functions from first semester calculus is sufficient. However, it is assumed that students have some familiarity with proof techniques. The level of the book is geared toward a junior-level mathematics student, but it could easily be adapted to a lower or higher level. Modest experience with a computer algebra system would be helpful, but a willingness to learn to use one is all that is required. What is most important is to approach this book in the proper frame of mind. This is a subject for exploration and experimentation. Students use the computer algebra system to gather data from which to formulate new conjectures. The definitions and main theorems are presented and proven, but the more the reader wanders down interesting side paths, the more he or she will get out of this book. The exercises present many such side paths, especially the in-chapter investigations and end-of-chapter exploration exercises.

The book is not tied into any one computer algebra system, and there are several freely available. The systems SageMath and PARI/GP are two excellent freely available systems. Similarly, Mathematica, Maple, or other commercial software could also be used. Because there are many excellent tutorials for each of these systems freely available, they will not be presented in this book.

Organization

This book contains more than can be typically covered in a standard semester. The typical material of a first semester number theory course is covered in Chapters 1–8. The remaining chapters, 9–11, represent more specialized topics. Various sections can be omitted from the core chapters to allow more time for other topics. For example, Chapter 4 and Sections 3.2, 3.3, 5.3, and 5.4 are used only lightly, if at all, in later chapters.

Chapters 1 and 2 cover the standard topics in divisibility and modular arithmetic and are prerequisites for every other chapter. Chapter 3 covers Quadratic Reciprocity and primitive roots. Chapter 4 is a brief side journey into cryptography. Chapter 5 investigates a few arithmetic functions, while Chapters 6 and 7 cover height functions, partial fractions, algebraic numbers, and Diophantine approximation. Chapter 8 is an introduction to solving Diophantine equations by examining several standard Diophantine problems. Chapter 9 treats the specific Diophantine equations that are called elliptic curves, with an emphasis on points of finite order.

Chapter 10 examines dynamical systems from a number theoretic perspective by studying rational preperiodic points for iterated systems. Finally, Chapter 11 introduces the notion of number theory with polynomials, that is, an introduction to number theory on function fields.

The following table gives an idea of the dependencies.

Chapter/Section	Dependencies
Chapter 1	–
Chapter 2	Chapter 1
Chapter 3	Chapters 1 and 2
Chapter 4	Chapters 1 and 2
Chapter 5	Chapter 1
Chapter 6 Section 6.4	Chapter 1 Additionally Chapter 2 and Section 3.1
Chapter 7	Chapters 1 and 6
Chapter 8 Section 8.5	Chapters 1, 2, and Section 3.1 Additionally Section 7.4
Chapter 9 Section 9.6	Chapters 1 and 2 Additionally Section 8.3
Chapter 10	Chapters 1, 2, Section 5.2
Chapter 11 Section 11.4	Chapters 1, 2, Section 5.1, Chapter 6 Additionally Chapter 8

Acknowledgments

As with any work of this sort, the author owes a great debt to those who came before. The written sources consulted can be found in the references. Additionally, there are many people over the course of many years that fostered my interest in number theory and computation, from my first number theory course as a freshman at Duke University taught by William Pardon, to my PhD advisor Joseph Silverman at Brown University, and all the professors and textbook authors in between. Particular thanks to Joe for always offering astute advice on everything from mathematics to publishers and for being a great role model by writing such excellent books.

There are many people who read early versions of the text and provided feedback. Stephen Kennedy provided detailed feedback on an early version and several helpful discussions about publishing in general. Steven J. Miller and his number theory class at Williams College provided helpful feedback and identified several errors in the text. The spring 2013 number theory class at the Florida Institute of Technology and the spring 2017 number theory class at Saint Louis University also showed remarkable patience using an early version of this text and providing useful feedback.

Special thanks goes to my mom Linda Pesante for bravely reading every page despite having to treat much of the technical material as a foreign language. Without her, grammatical errors and simply bad writing would be much more prevalent in text.

Benjamin Hutz
July 2017