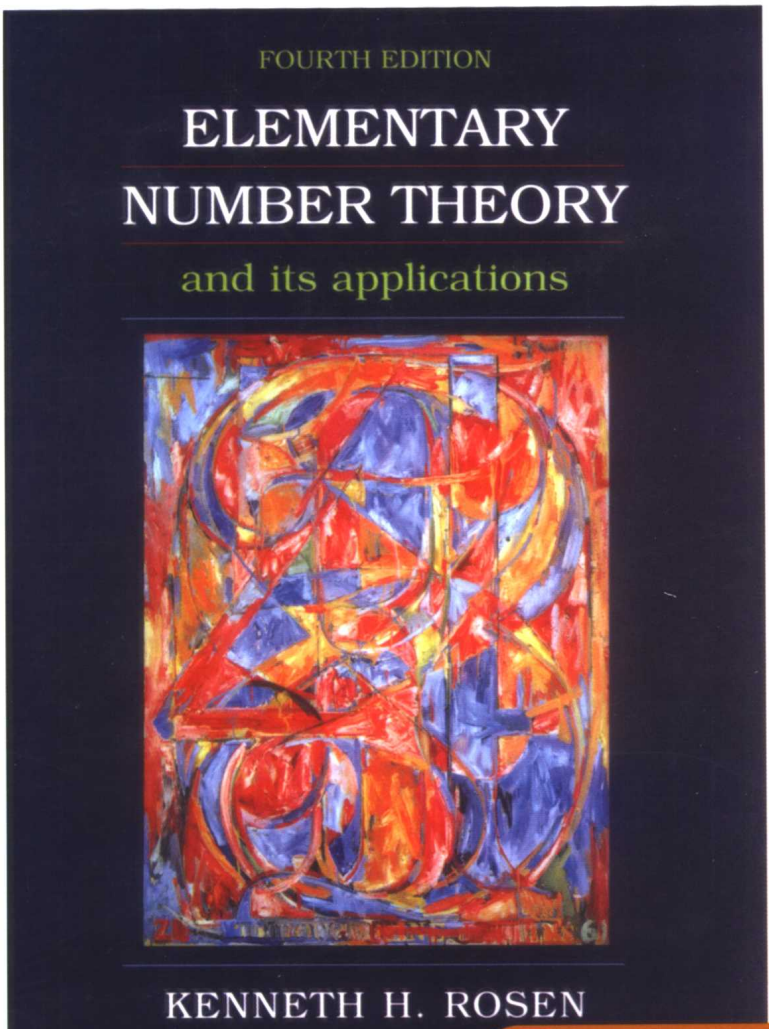
HZ BOOKS

PEARSON Addison Wesley

经 典 原 版 书 库

初等数论及其应用

（英文版 · 第4版）



（美）Kenneth H. Rosen 著

机械工业出版社
China Machine Press

Pearson Education

经典原版书库

初等数论及其应用

（英文版·第4版）

Elementary Number Theory and Its Applications (Fourth Edition)

（美）Kenneth H. Rosen 著

机械工业出版社
China Machine Press

本书版权登记号：图字：01-2004-0503

图书在版编目（CIP）数据

初等数论及其应用（英文版·第4版）/（美）罗森（Rosen, K. H.）著. -北京：机械工业出版社，2004.2

（经典原版书库）

书名原文：Elementary Number Theory and Its Applications, Fourth Edition

ISBN 7-111-13815-5

Ⅰ.初… Ⅱ.罗… Ⅲ.初等数论-英文 Ⅳ.O156.1

中国版本图书馆CIP数据核字（2004）第001386号

机械工业出版社（北京市西城区百万庄大街22号 邮政编码 100037）

责任编辑：迟振春

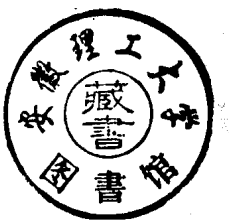
北京瑞德印刷有限公司印刷·新华书店北京发行所发行

2004年2月第1版第1次印刷

787mm × 1092mm 1/16 · 41.25印张

印数：0 001-2 000 册

定价：59.00元



Preface

In olden times (well, before 1970) number theory had the reputation as the purest part of mathematics. It was studied for its long and rich history, its wealth of easily accessible and fascinating questions, and its intellectual appeal. But, in the past few years, people have looked at number theory in a new way. Today, people study number theory both for the traditional reasons and for the compelling reason that number theory has become essential for cryptography. The first edition of this book was the first text to integrate the modern applications of elementary number theory with traditional topics. This fourth edition builds on the basic approach of the original text. No other number theory text presents elementary number theory and its applications in as thoughtful a fashion as this book does. Instructors will be pleasantly surprised to see how modern applications can be seamlessly woven into their number theory course when they use this text.

This book is designed as a text for an undergraduate number theory course at any level. No formal prerequisites are needed for most of the material, other than some level of mathematical maturity. This book is also designed to be a useful supplement for computer science courses and as a number theory primer for people interested in learning about new developments in number theory and cryptography.

This fourth edition has been designed to preserve the strengths of previous editions while providing substantial enhancements and improvements. Instructors familiar with previous editions will be comfortable with this new edition. Those examining this book for the first time will see a text suitable for the new millennium, integrating gems of number theory dating back thousands of years with developments less than ten years old. Those familiar with previous editions will find that this book has become more flexible, easier to each from, and more interesting and compelling. They will also find that additional emphasis has also been placed on the historical context of results and on the experimental side of number theory.

CHANGES IN THE FOURTH EDITION

Extensive enhancements have been made to the third edition of this text to produce this new and improved fourth edition. Many changes have been made at the request of users and reviewers. The fourth edition should be easier to teach from, easier to read, and more effective in conveying both the beauty and utility of number theory. Noteworthy changes include:

- ***A more flexible initial set of chapters***

The initial chapter has been streamlined. Material covered in this chapter has been reorganized. Coverage of axioms for the integers and the binomial theorem, previously in Chapter 1, is now in the Appendix. Coverage of integer representations and integer operations and their complexity is now presented in a separate chapter (Chapter 2). Primes and greatest common divisors are covered in Chapter 3; previously primes were introduced in Chapter 1.

- ***Chapter introductions***

Each chapter now begins with an introduction describing what the chapter covers and why this material is important. These introductions are designed to provide perspective to students.

- ***Updated and expanded coverage of cryptography***

The chapter on cryptology has been revised and updated. Expanded coverage of block ciphers and new coverage of stream ciphers is provided. In particular, Vernam and autokey ciphers are covered and a discussion of the DES cryptosystem is included. The material in this chapter has been reorganized so that material related to cryptographic protocols is now in a separate section. The ElGamal cryptosystem is now covered (in Chapter 10). Cryptographic terminology has also been updated.

- ***Up-to-date discoveries***

The latest discoveries in number theory have been reflected in the text, including theoretical discoveries such as the fact that Andrew Wiles has proved Fermat's last theorem. Also, computational discoveries, such as the six new Mersenne primes discovered since the third edition was published, are described throughout the text. Web links are provided where updates to discoveries made subsequent to the publication of, and reprinting of, this book can be found

- ***Web resources***

You can access the Web site for this book by visiting the Addison Wesley Longman site at `www.awlonline.com/rosen`. It includes links for sites that provide up-to-date information about recent discoveries, tutorials, historical and biographical material, software to download, and other resources.

A special icon (🕸) marks the locations in the text where material related to these links is covered. Furthermore, an appendix listing the top Web links for number theory is now provided.

- ***New and expanded topic coverage***

Sections devoted to solving polynomial congruences, Möbius inversion, and the El-Gamal cryptosystem have been added. The Pocklington and Proth primality tests are now covered. New material on integer sequences and figurate numbers can be found in Chapter 1. A new section on Fibonacci numbers is found in Chapter 1, expanding the coverage of Fibonacci numbers in the third edition. The algebraic and transcendental numbers are now discussed in Chapters 1 and 12. Countability is now covered in Chapter 1.

- ***Enhanced examples and proofs***

Many proofs have been enhanced by adding more motivation, clearer explanations, and by breaking up some long, complicated proofs through the use of lemmas. New examples have been added at key places in the text.

- ***Enhanced exercises***

Many new exercises have been added, including both routine and challenging exercises. Answers to the odd-numbered exercises have been checked and rechecked. Additional computational exercises designed to be solved using a computational system such as Maple or *Mathematica* have been added. These are segregated from the exercises designed for solution by hand.

- ***Stress on historical context***

More attention has been paid to the history and context of the key ideas of number theory. For example, the genesis of the prime number theorem is covered. The history and importance of the law of quadratic reciprocity receives more coverage in this edition. Euler's version of the law of quadratic reciprocity is now described in the text. Several different proofs of the law of quadratic reciprocity are now outlined in the exercises. A comprehensive history of the discovery of all currently known Mersenne primes is also provided.

- ***Additional biographies***

More than 25 new biographies have been added, including those of early mathematicians from India and China and of twentieth century mathematicians and computer scientists. Biographies from the third edition have been improved. Photographs or illustrations accompany many of these biographies. An index of biographies is also provided.

- ***Support for Maple® and* Mathematica®**

A new appendix describes the number theory commands in Maple, *Mathematica*, and their add-on packages. It also provides pointers for finding out more about using these systems for calculations in number theory

- ***Student's Solutions Manual***

A Student's Solutions Manual is now available. This guide includes worked solutions to all the odd-numbered exercises in the text and contains other useful material, such as guidance with some of the computational exercises found at the end of each section of the text.

FEATURES

A Development of Classical Number Theory

The core of this book presents classical elementary number theory in a comprehensive and compelling manner. The historical context and importance of key results is noted. The basic material on each topic is developed carefully, followed by more sophisticated results on the same topic.

Applications

A key strength of this book is how applications of number theory are covered. Once the requisite theory has been developed, applications are woven into the text in a flexible way. These applications are designed to motivate the coverage of the theory and illustrate the usefulness of different aspects of elementary number theory. Extensive coverage is devoted to applications of number theory to cryptography. Classical ciphers, block and stream ciphers, public key cryptosystems, and cryptographic protocols are all covered. Other applications to computer science include fast multiplication of integers, pseudorandom numbers, and check digits. Applications to many other areas, such as scheduling, telephony, entomology, and zoology can also be found in the text.

Unifying Themes

Many concepts from elementary number theory are used in primality testing and factoring. Furthermore, primality testing and factoring play a key role in applications of number theory to cryptography. As such, these topics are used as unifying themes and all returned to repeatedly. Almost every chapter includes material on these topics.

Accessibility

This book has been designed with a minimum of prerequisites. The book is almost entirely self-contained, with only a knowledge of what is generally known as "college algebra" required. There are several places where knowledge of some concepts from calculus is needed (such as in the discussion of the distribution of primes and of big-O

notation). Concepts from discrete mathematics and from linear algebra are needed in a few places. All material that depends on topics more advanced than college algebra are explicitly noted and are optional.

Accuracy

Great effort has been made to ensure the accuracy of this edition. Input from many users of the third edition, reviewers, and proofreaders skilled in mathematics has helped achieve this goal.

Extensive Exercise Sets

The best (and maybe the only) way to learn mathematics is by doing exercises. This text contains an extremely extensive and diverse collection of exercises. Many routine exercises are included to develop basic skills, with care taken so that both odd-numbered and even-numbered exercises of this type are included. A large number of intermediate level exercises help students put several concepts together to form new results. Many other exercises and blocks of exercises are designed to develop new concepts. Challenging exercises are in ample supply and are marked with one star (*) indicating a difficult exercise and two stars (**) indicating an extremely difficult exercise. There are some exercises that contain results used later in the text; these are marked with a chevron (➢). These exercises should be assigned by instructors whenever possible.

An extensive collection of computer projects is also provided. Each section includes computations and explorations designed to be done with a computational program such as Maple or *Mathematica*, or using programs written by instructors and/or students. There are some routine exercises of this sort that students should do to learn how to apply basic commands from Maple or *Mathematica* (as describe in Appendix D), as well as more open-ended questions designed for experimentation and creativity. Each section also includes a set of programming projects designed to be done by students using a programming language of their choice, such as the programming languages included with Maple and *Mathematica*, or another programming language of their choice.

Exercise Answers

The answers to all odd-numbered exercises are provided at the end of the text. More complete solutions to these exercises can be found in the Student's Solutions Manual that accompanies this text. All solutions have been careful checked and rechecked to ensure accuracy.

Discovery via Empirical Evidence

In many places in the text numerical evidence is examined to help motivate key results. This gives an opportunity to students to come up with a conjecture much as the people who originally developed number theory did.

Extensive Examples

This book includes examples that illustrates each important concept. These examples are designed to illustrate the definitions, algorithms, and proofs in the text. They are also designed to help students work many of the exercises found at the end of sections.

Carefully Motivated Proofs

Many proofs in this book are motivated with examples that precede the formal proof and illustrate the key ideas of the proof. The proofs themselves are presented in a careful, rigorous, and fully explained manner. The proofs are designed so that students can understand each step and the flow of logic. Numerical examples illustrating the steps of the proof are often provided following the formal proof as well.

Algorithmic Reasoning

The algorithmic aspects of elementary number theory are thoroughly covered in this text. Not only are many algorithms described, but their complexity is also analyzed. Among the algorithms described in this book are those for computing greatest common divisors in many different ways and for primality testing and factoring. The coverage of the complexity of algorithms has been included so that instructors can choose whether they want to include this material in their course.

Biographies and Historical Notes

More than 50 biographies of contributors to number theory are included in this edition. Contributors included lived in ancient times, the Middle Ages, the sixteenth through eighteenth centuries, the nineteenth century, and the twentieth century, and lived in the East and in the West. These biographies are designed to give students an appreciation of contributors as unique individuals who often led (or are leading) interesting lives.

Open Questions

Many open questions in number theory are described throughout the book. Some are described in the text itself and others are found in exercise sets. These questions show that the subject of number theory is a work in progress. Readers should be aware that attempting to solve such problems can often be time-consuming and futile. However, it would be surprising if some of these questions were not settled in the next few years.

Up-to-Date Content

The latest discoveries in number theory are included in this book. The current status of many open questions is described, as are new theoretical results. Discoveries of new primes and factorizations made as late as November 1999 are included with the first printing of this edition. These discoveries will help readers understand that number theory is an extremely active area of study. They may even see how they may participate in the search for new primes.

Bibliography

An extensive bibliography is provided for this book. This bibliography lists key printed number theory resources including both books and papers. Many useful number texts are listed, as are books dealing with the history of number theory and with particular aspects of the subject. Many original sources are included, as is material covering cryptography.

Maple and *Mathematica* Support

An appendix has been provided which lists the commands in both Maple and *Mathematica* for carrying out computations in number theory. These commands are listed according to the chapter of the text relevant to these commands.

Web Resources

The Web site for this book includes a Web guide to number theory that is keyed to this text, as well as other resources. To access this site go to `www.awlonline.com/rosen`. For convenience, the most important number theory Web sites are highlighted in Appendix D.

Tables

A set of five tables is included to help students with their computations and experimentation. Looking at these tables can help students search for patterns and formulate conjectures. The use of a computational software package, such as Maple or *Mathematica* is recommended when these tables are insufficient.

List of Symbols

A list of symbols used in the text and where they are defined is included on the inside front cover of this book.

ANCILLARIES

Student's Solutions Manual (ISBN 0-201-43723-6)

The Student's Solutions Manual contains worked solutions to all the odd-numbered exercises in the text and other helpful material, including some tips on using Maple and *Mathematica* to explore number theory.

Instructor's Manual (ISBN 0-201-43722-8)

The Instructor's Manual contains solutions to all exercises in the text. It also contains advice on planning which sections to cover. Sample tests are also provided.

Web Site

The Web site for this book contains a guide providing annotated links to a large number of Web sites relevant to number theory. These sites are keyed to the page in the book

where relevant material is discussed. These locations are marked with an icon (✱) in the text.

How to Use this Book

This text is designed to be extremely flexible. The essential, core material for a number theory course can be found in Section 1.4, which covers divisibility; Chapter 3, which covers primes, factoring, and greatest common divisors; Sections 4.1–4.3, which cover congruences; and Chapter 6, which covers important congruences including Fermat's little theorem. Instructors can design their own courses by supplementing core material with other content of their own choice. To help instructors decide which sections to cover, a brief description of the different parts of the book follows.

The material in Sections 1.1, 1.2, and 1.3 is optional. Section 1.1 covers the basic concepts about different types of numbers, integer sequences (including countability), and sums and products. Section 1.2 provides a concise introduction to mathematical induction, which students may already have studied elsewhere. (Additional foundational material on integer axioms and the binomial theorem can be found in the Appendices.) Section 1.3 introduces the Fibonacci numbers, which students may have studied in a course in discrete mathematics. (As stated previously, Section 1.4 presents core material on divisibility of integers.)

Chapter 2 is optional; it covers base b representations of integers, integer arithmetic, and the complexity of integer operations. Big-O notation is introduced in Section 2.3. This is important for students who have not seen this notation elsewhere, especially when the instructor wants to stress the complexity of computations in number theory.

As previously stated, Chapter 3 and Section 4.1–4.3 present core material. Section 4.4, which deals with solving polynomial congruences modulo powers of primes is optional; it is important to development of p-adic number theory. Section 4.5 requires some background in linear algebra; the material in this section is used in Section 8.2; these sections may be omitted if desired. Section 4.6 introduces a particular factorization method (the Pollard rho method) and can be omitted.

Chapter 5 is optional. Instructors can pick and choose from a variety of applications of number theory. Section 5.1 introduces divisibility tests; Section 5.2 covers the perpetual calendar; Section 5.3 discusses scheduling round-robin tournaments; Section 5.4 shows how congruences can be used in hashing functions; and Section 5.5 describes how check digits are found and used. As mentioned previously, Chapter 6 presents core material.

Chapter 7 covers multiplicative functions. Section 7.1 should be covered; it introduces the basic concept of a multiplicative function and studies the Euler phi-function. The sum and number of divisors functions are studied in Section 7.2; this section is recommended for all instructors. All instructors will probably want to cover Section 7.3, which introduces the concept of a perfect number and describes the search for Mersenne primes.

Chapter 8 covers the applications of number theory to cryptology. It is highly recommended since this is such an important topic and one that students find extremely interesting. Section 8.1 introduces the basic terminology of this subject and some classical character ciphers; instructors who plan to cover cryptography in their course should be sure to include this section. Section 8.2 introduces block and stream ciphers, two important families of ciphers, and provides examples of these types of cipher that are based on number theory. Section 8.3 covers a particular type of block cipher based on modular exponentiation. Section 8.4 should be covered by all instructors. It introduces the fundamental concept of public-key cryptography and illustrates this with the RSA cryptosystem. Section 8.5 discuss knapsack ciphers; it is an optional section. Section 8.6 provides an introduction to cryptographic protocols and is highly recommended for instructors interested in modern cryptographic applications. (Additional topics from cryptography are covered in Chapters 9,10, and 11.)

Chapter 9 deals with the concept of the order of an integer, primitive roots, and index arithmetic. Sections 9.1–9.4 should be covered if possible. Section 9.5, which discusses how the concepts of this chapter are used in primality testing presents partial converses of Fermat's little theorem. Section 9.6 on universal exponents is optional; it contains some interesting results about Carmichael numbers.

Chapter 10 introduces some applications that use the material from Chapter 9. The three sections that cover pseudorandom numbers, the ElGamal cryptosystem, and schemes for splicing telephone cable are optional. Instructors stressing cryptographic applications will especially want to cover Section 10.2.

Sections 11.1 and 11.2, which cover quadratic residues and quadratic reciprocity, a key result of number theory, should be covered whenever possible. Sections 11.3 and 11.4 deal with Jacobi symbols and Euler pseudoprimes and are optional. Section 11.5 covers zero-knowledge proofs; instructors interested in cryptography will want to cover this section if possible.

Section 12.1, which covers decimal fractions, will be covered by many instructors. Instructors with an interest in continued fractions will want to cover Sections 12.2–12.4, which establish the basic results about finite and periodic continued fractions. Section 12.5, which deals with factoring using continued fractions, is optional.

Most instructors will want to cover Sections 13.1 and 13.2, which deal with Pythagorean triples and Fermat's last theorem, respectively. Section 13.3, which covers sums of squares and Section 13.4, which discuss the solution of Pell's equation and which uses continued fractions, are optional sections.

ACKNOWLEDGMENTS

I wish to thank my management at AT&T Laboratories Research for their support in the preparation of this edition and for providing a stimulating professional environment.

Special thanks go to Jerry Grossman and Bart Goddard for their help reviewing the manuscript for accuracy and for their assistance with the solutions of the exercises in this text and for checking and rechecking the answers and solutions to these exercises.

Thanks go to Carolyn Lee-Davis, the editor of this edition, for her support and enthusiasm and to all the other editors of previous editions of this book at Addison-Wesley, going back to Wayne Yuhasz who endorsed the original concept of this book and his colleague Jeff Pepper who also recognized its appeal in an era when publishers were avoiding number theory books like the plague. My appreciation also goes to Karen Guardino, who managed the production of this book, and the rest of the Addison-Wesley team, including Greg Tobin, Michael Boezi, Barbara Atkinson, and RoseAnne Johnson.

I have benefitted from the thoughtful reviews and suggestions from users of previous editions of this book. Many of their ideas have been incorporated in this edition. My profound thanks go to the following reviewers of this and previous editions of this text.

David Bressoud, *Pennsylvania State University*
Sydney Bulman-Fleming, *Wilfred Laurier University*
Richard Bumby, *Rutgers University*
Charles Cook, *University of South Carolina, Sumter*
Christopher Cotter, *University of Northern Colorado*
Euda Dean, *Tarleton State University*
Daniel Drucker, *Wayne State University*
Bob Gold, *Ohio State University*
Fernando Gouvea, *Colby College*
Jennifer Johnson, *University of Utah*
Roy Jordan, *Monmouth College*
Herbert Kasube, *Bradley University*
Neil Koblitz, *University of Washington*
Steven Leonhardi, *Winona State University*
Charles Lewis, *Monmouth College*
James McKay, *Oakland University*
John Mairhuber, *University of Maine–Orono*
Alexsandrs Mihailovs, *University of Pennsylvania*
Rudolf Najar, *California State University, Fresno*
Carl Pomerance, *University of Georgia*
Sinai Robins, *Temple University*
Tom Shemanske, *Dartmouth College*
Leslie Vaaler, *University of Texas, Austin*
Evelyn Bender Vaskas, *Clark University*
Samuel Wagstaff, *Purdue University*
Edward Wang, *Wilfred Laurier University*
Betsey Whitman, *Framingham State University*
David Wright, *Oklahoma State*
Paul Zwier, *Calvin College*

Finally, I thank in advance all those who send me suggestions and corrections in the future. You may send such material to me care of Addison-Wesley at `math@awl.com`.

Kenneth H. Rosen
Middletown, New Jersey

Contents

What is Number Theory? 1

1 The Integers 5

1.1 Numbers, Sequences, and Sums 6
1.2 Mathematical Induction 18
1.3 The Fibonacci Numbers 24
1.4 Divisibility 31

2 Integer Representations and Operations 39

2.1 Representations of Integers 39
2.2 Computer Operations with Integers 49
2.3 Complexity of Integer Operations 56

3 Primes and Greatest Common Divisors 65

3.1 Prime Numbers 66
3.2 Greatest Common Divisors 80
3.3 The Euclidean Algorithm 86
3.4 The Fundamental Theorem of Arithmetic 97
3.5 Factorization Methods and the Fermat Numbers 109
3.6 Linear Diophantine Equations 119

4 Congruences 127

4.1 Introduction to Congruences 127
4.2 Linear Congruences 139
4.3 The Chinese Remainder Theorem 143
4.4 Solving Polynomial Congruences 153
4.5 Systems of Linear Congruences 160
4.6 Factoring Using the Pollard Rho Method 170

5 Applications of Congruences 173

5.1 Divisibility Tests 173
5.2 The Perpetual Calendar 179
5.3 Round-Robin Tournaments 184
5.4 Hashing Functions 186
5.5 Check Digits 191

6 Some Special Congruences 197

6.1 Wilson's Theorem and Fermat's Little Theorem 197
6.2 Pseudoprimes 205
6.3 Euler's Theorem 215

7 Multiplicative Functions 221

7.1 The Euler Phi-function 222
7.2 The Sum and Number of Divisors 232
7.3 Perfect Numbers and Mersenne Primes 239
7.4 Möbius Inversion 251

8 Cryptology 259

8.1 Character Ciphers 260
8.2 Block and Stream Ciphers 268
8.3 Exponentiation Ciphers 282
8.4 Public-Key Cryptography 285
8.5 Knapsack Ciphers 292
8.6 Cryptographic Protocols and Applications 299

9 Primitive Roots 307

9.1 The Order of an Integer and Primitive Roots 308
9.2 Primitive Roots for Primes 315
9.3 The Existence of Primitive Roots 321
9.4 Index Arithmetic 329
9.5 Primality Tests Using Orders of Integers and Primitive Roots 339
9.6 Universal Exponents 346

10 Applications of Primitive Roots and the Order of an Integer 353

10.1 Pseudorandom Numbers 353
10.2 The ElGamal Cryptosystem 363
10.3 An Application to the Splicing of Telephone Cables 368

11 Quadratic Residues 375

11.1 Quadratic Residues and Nonresidues 376
11.2 The Law of Quadratic Reciprocity 392
11.3 The Jacobi Symbol 404
11.4 Euler Pseudoprimes 412
11.5 Zero-Knowledge Proofs 421

12 Decimal Fractions and Continued Fractions 429

12.1 Decimal Fractions 429
12.2 Finite Continued Fractions 442
12.3 Infinite Continued Fractions 452
12.4 Periodic Continued Fractions 463
12.5 Factoring Using Continued Fractions 477

13 Some Nonlinear Diophantine Equations 481

13.1 Pythagorean Triples 482
13.2 Fermat's Last Theorem 487
13.3 Sums of Squares 495
13.4 Pell's Equation 505

Appendix A Axioms for the Set of Integers 515

Appendix B Binomial Coefficients 519

Appendix C Using Maple and *Mathematica* for Number Theory 527

C.1 Using Maple for Number Theory 527
C.2 Using Mathematica for Number Theory 530

Appendix D Number Theory Web Links 535

Appendix E Tables 537

Answers to Odd-Numbered Exercises 553

Bibliography 611

Index of Biographies 623

Index 625

Photo Credits 638