HZ BOOKS
华章教育

PEARSON

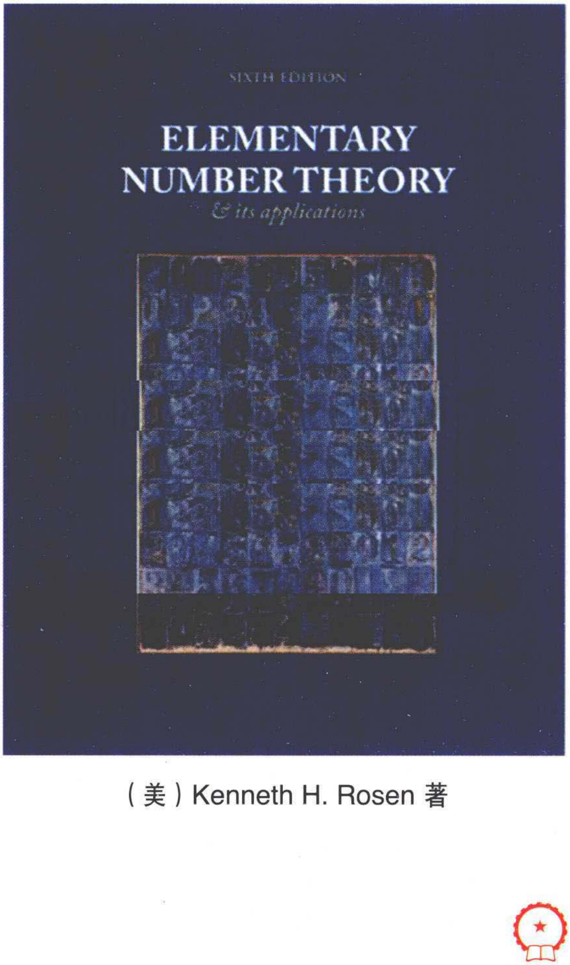
华章数学·统计学原版精品系列

初等数论及其应用

Elementary Number Theory and Its Applications

(Sixth Edition)

（英文版·第6版）



（美）Kenneth H. Rosen 著

机械工业出版社
China Machine Press

华章数学·统计学原版精品系列

初等数论及其应用

Elementary Number Theory and Its Applications

(Sixth Edition)

（英文版·第6版）

（美）Kenneth H. Rosen 著

机械工业出版社
China Machine Press

本书版权登记号：图字：01-2010-5015

图书在版编目（CIP）数据

初等数论及其应用（英文版·第6版）/（美）罗森（Rosen, K. H.）著. —北京：机械工业出版社，2010.9
（华章数学·统计学原版精品系列）
书名原文：Elementary Number Theory and Its Applications, Sixth Edition

ISBN 978-7-111-31798-2

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（2010）第 175152 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：李俊竹
北京京北印刷有限公司印刷
2010年9月第1版第1次印刷
170mm×242mm · 48.25 印张
标准书号：ISBN 978-7-111-31798-2
定价：89.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88378991；88361066
购书热线：（010）68326294；88379649；68995259
投稿热线：（010）88379604
读者信箱：hzjsj@hzbook.com

Preface

My goal in writing this text has been to write an accessible and inviting introduction to number theory. Foremost, I wanted to create an effective tool for teaching and learning. I hoped to capture the richness and beauty of the subject and its unexpected usefulness. Number theory is both classical and modern, and, at the same time, both pure and applied. In this text, I have strived to capture these contrasting aspects of number theory. I have worked hard to integrate these aspects into one cohesive text.

This book is ideal for an undergraduate number theory course at any level. No formal prerequisites beyond college algebra are needed for most of the material, other than some level of mathematical maturity. This book is also designed to be a source book for elementary number theory; it can serve as a useful supplement for computer science courses and as a primer for those interested in new developments in number theory and cryptography. Because it is comprehensive, it is designed to serve both as a textbook and as a lifetime reference for elementary number theory and its wide-ranging applications.

This edition celebrates the silver anniversary of this book. Over the past 25 years, close to 100,000 students worldwide have studied number theory from previous editions. Each successive edition of this book has benefited from feedback and suggestions from many instructors, students, and reviewers. This new edition follows the same basic approach as all previous editions, but with many improvements and enhancements. I invite instructors unfamiliar with this book, or who have not looked at a recent edition, to carefully examine the sixth edition. I have confidence that you will appreciate the rich exercise sets, the fascinating biographical and historical notes, the up-to-date coverage, careful and rigorous proofs, the many helpful examples, the rich applications, the support for computational engines such as Maple and *Mathematica,* and the many resources available on the Web.

Changes in the Sixth Edition

The changes in the sixth edition have been designed to make the book easier to teach and learn from, more interesting and inviting, and as up-to-date as possible. Many of these changes were suggested by users and reviewers of the fifth edition. The following list highlights some of the more important changes in this edition.

- ***New discoveries***

This edition tracks recent discoveries of both a numerical and a theoretical nature. Among the new computational discoveries reflected in the sixth edition are four Mersenne primes and the latest evidence supporting many open conjectures. The Tao-Green theorem proving the existence of arbitrarily long arithmetic progressions of primes is one of the recent theoretical discoveries described in this edition.

- ***Biographies and historical notes***

Biographies of Terence Tao, Etienne Bezout, Norman MacLeod Ferrers, Clifford Cocks, and Wacław Sierpiński supplement the already extensive collection of biographies in the book. Surprising information about secret British cryptographic discoveries predating the work of Rivest, Shamir, and Adleman has been added.

- ***Conjectures***

The treatment of conjectures throughout elementary number theory has been expanded, particularly those about prime numbers and diophantine equations. Both resolved and open conjectures are addressed.

- ***Combinatorial number theory***

A new section of the book covers partitions, a fascinating and accessible topic in combinatorial number theory. This new section introduces such important topics as Ferrers diagrams, partition identies, and Ramanujan's work on congruences. In this section, partition identities, including Euler's important results, are proved using both generating functions and bijections.

- ***Congruent numbers and elliptic curves***

A new section is devoted to the famous congruent number problem, which asks which positive integers are the area of a right triangle with rational side lengths. This section contains a brief introduction to elliptic curves and relates the congruent number problem to finding rational points on certain elliptic curves. Also, this section relates the congruent number problem to arithmetic progressions of three squares.

- ***Geometric reasoning***

This edition introduces the use of geometric reasoning in the study of diophantine problems. In particular, new material shows that finding rational points on the unit circle is equivalent to finding Pythgaorean triples, and that finding rational triangles with a given integer as area is equivalent to finding rational points on an associated elliptic curve.

- ***Cryptography***

This edition eliminates the unnecessary restriction that when the RSA cryptosystem is used to encrypt a plaintext message this message needs to be relatively prime to the modulus in the key.

- ***Greatest common divisors***

Greatest common divisors are now defined in the first chapter, as is what it means for two integers to be relatively prime. The term *Bezout coefficients* is now introduced and used in the book.

- ***Jacobi symbols***

More motivation is provided for the usefulness of Jacobi symbols. In particular, an expanded discussion on the usefulness of the Jacobi symbol in evaluating Legendre symbols is now provided.

- ***Enhanced exercise sets***

Extensive work has been done to improve exercise sets even farther. Several hundred new exercises, ranging from routine to challenging, have been added. Moreover, new computational and exploratory exercises can be found in this new edition.

- ***Accurancy***

More attention than ever before has been paid to ensuring the accuracy of this edition. Two independent accuracy checkers have examined the entire text and the answers to exercises.

- ***Web Site, www.pearsonhighered.com/rosen***

The Web site for this edition has been considerably expanded. Students and instructors will find many new resources they can use in conjunction with the book. Among the new features are an expanded collection of applets, a manual for using comptutional engines to explore number theory, and a Web page devoted to number theory news.

Exercise Sets

Because exercises are so important, a large percentage of my writing and revision work has been devoted to the exercise sets. Students should keep in mind that the best way to learn mathematics is to work as many exercises as possible. I will briefly describe the types of exercises found in this book and where to find answers and solutions.

- ***Standard 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.

- ***Exercise Legend***

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 arrow symbol (➢). These exercises should be assigned by instructors whenever possible.

- ***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 can be found on the Web site for this book. All solutions have been carefully checked and rechecked to ensure accuracy.

- ***Computational Exercises***

Each section includes computations and explorations designed to be done with a computational program, such as Maple, *Mathematica*, PARI/GP, or Sage, or using programs written by instructors and/or students. There are routine computational exercises students can do to learn how to apply basic commands (as described in Appendix D for Maple and *Mathematica* and on the Web site for PARI/GP and Sage), 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 or the computational program of their choice. The *Student's Manual to Computations and Explorations* on the Web site provides answers, hints, and guidance that will help students use computational tools to attack these exercises.

Web Site

Students and instructors will find a comprehensive collection of resources on this book's Web site. Students (as well as instructors) can find a wide range of resources at www.pearsonhighered.com/rosen. Resources intended for only instructor use can be accessed at www.pearsonhighered.com/irc; instructors can obtain their password for these resources from Pearson.

- ***External Links***

The Web site for this book contains a guide providing annotated links to many 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 in the book with the icon ○. For convenience, a list of the most important Web sites related to number theory is provided in Appendix D.

- ***Number Theory News***

The Web site also contains a section highlighting the latest discoveries in number theory.

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

Worked-out solutions to all the odd-numbered exercises in the text and sample exams can be found in the online *Student's Solution Manual.*

- ***Student's Manual for Computations and Explorations***

A manual providing resources supporting the computations and explorations can be found on the Web site for this book. This manual provides worked-out solutions or partial solutions to many of these computational and exploratory exercises, as well as hints and guidance for attacking others. This manual will support, to varying degrees, different comptutional environments, including Maple, *Mathematica*, and PARI/GP.

- ***Applets***

An extensive collection of applets are provided on the Web site. These applets can be used by students for some common computations in number theory and to help understand concepts and explore conjectures. Besides algorithms for comptutions in number theory, a collection of cryptographic applets is also provided. These include applets for encyrption, decryption, cryptanalysis, and cryptographic protocols, adderssing both classical ciphers and the RSA cryptosystem. These cryptographic applets can be used for individual, group, and classroom activities.

- ***Suggested Projects***

A useful collection of suggested projects can also be found on the Web site for this book. These projects can serve as final projects for students and for groups of students.

- ***Instructor's Manual***

Worked solutions to all exercises in the text, including the even-numbered execises, and a variety of other resources can be found on the Web site for instructors (which is not available to students). Among these other resources are sample syllabi, advice on planning which sections to cover, and a test bank.

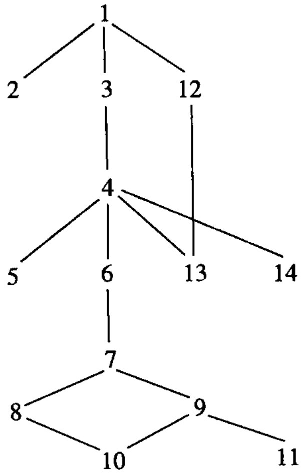
How to Design a Course Using this Book

This book can serve as the text for elementary number theory courses with many different slants and at many different levels. Consequently, instructors will have a great deal of flexibility designing their syllabi with this text. Most instructors will want to cover the core material in Chapter 1 (as needed), Section 2.1 (as needed), Chapter 3, Sections 4.1–4.3, Chapter 6, Sections 7.1–7.3, and Sections 9.1–9.2.

To fill out their syllabi, instructors can add material on topics of interest. Generally, topics can be broadly classified as pure versus applied. Pure topics include Möbius inversion (Section 7.4), integer partitions (Section 7.5), primitive roots (Chapter 9), continued fractions (Chapter 12), diophantine equations (Chapter 13), and Guassian integers (Chapter 14).

Some instructors will want to cover accessible applications such as divisibility tests, the perpetual calendar, and check digits (Chapter 5). Those instructors who want to stress computer applications and cryptography should cover Chapter 2 and Chapter 8. They may also want to include Sections 9.3 and 9.4, Chapter 10, and Section 11.5.

After deciding which topics to cover, instructors may wish to consult the following figure displaying the dependency of chapters:



Although Chapter 2 may be omitted if desired, it does explain the big-O notation used throughout the text to describe the complexity of algorithms. Chapter 12 depends only on Chapter 1, as shown, except for Theorem 12.4, which depends on material from Chapter 9. Section 13.4 is the only part of Chapter 13 that depends on Chapter 12. Chapter 11 can be studied without covering Chapter 9 if the optional comments involving primitive roots in Section 9.1 are omitted. Section 14.3 should also be covered in conjunction with Section 13.3.

For further assistance, instructors can consult the suggested syllabi for courses with different emphases provided in the *Instructor's Resource Guide* on the Web site.

Acknowledgments

I appreciate the continued strong support and enthusiam of Bill Hoffman, my editor at Pearson and Addison-Wesley far longer than any of the many editors who have preceded him, and Greg Tobin, president of the mathematics division of Pearson. My special gratitude goes to Caroline Celano, associate editor, for all her assistance with development and production of the new edition. My appreciation also goes to the production, marketing, and media team behind this book, including Beth Houston (Production Project Manager), Maureen Raymond (Photo Researcher), Carl Cottrell (Media Producer), Jeff Weidenaar (Executive Marketing Manager), Kendra Bassi (Marketing Assistant), and Beth Paquin (Designer) at Pearson, and Paul Anagnostopoulos (project manager), Jacqui Scarlott (composition), Rick Camp (copyeditor and proofreader), and Laurel Muller (artist) at Windfall Software. I also want to reiterate my thanks to all those who supported my work on the first five editions of this book, including the multitude of my previous editors at Addison Wesley and my management at AT&T Bell Laboratories (and its various incarnations).

Special thanks go to Bart Goddard who has prepared the solutions of all exercises in this book, including those found at the end of the book and on the Web site, and who has reviewed the entire book. I am also grateful to Jean-Claude Evard and Roger Lipsett for their help checking and rechecking the entire manuscript, including the answers to exercises. I would also like to thank David Wright for his many contributions to the Web site for this book, including material on PARI/GP, number theory and cryptography applets, the computation and exploration manual, and the suggested projects. Thanks also goes to Larry Washington and Keith Conrad for their helpful suggestions concerning congruent numbers and elliptic curves.

Reviewers

I have benefited from the thoughtful reviews and suggestions from users of previous editions, to all of whom I offer heartfelt thanks. Many of their ideas have been incorporated in this edition. My profound thanks go to the reviewers who helped me prepare the sixth edition:

Jennifer Beineke, *Western New England College*
David Bradley, *University of Maine-Orono*
Flavia Colonna, *George Mason University*
Keith Conrad, *University of Connecticut*
Pavel Guerzhoy, *University of Hawaii*
Paul E. Gunnells, *University of Massachusetts-Amherst*
Charles Parry, *Virginia Polytechnic Institute and State University*
Holly Swisher, *Oregon State University*
Lawrence Sze, *California State Polytechnic University, Pomona*

I also wish to thank again the approximately 50 reviewers of previous editions of this book. They have helped improve this book throughout its life. Finally, I thank in advance all those who send me suggestions and corrections in the future. You may send such material to me in care of Pearson at math@pearson.com.

Kenneth H. Rosen
Middletown, New Jersey

Contents

What Is Number Theory?

There is a buzz about number theory: Thousands of people work on communal number theory problems over the Internet . . . the solution of a famous problem in number theory is reported on the PBS television series NOVA . . . people study number theory to understand systems for making messages secret . . . What is this subject, and why are so many people interested in it today?

Number theory is the branch of mathematics that studies the properties of, and the relationships between, particular types of numbers. Of the sets of numbers studied in number theory, the most important is the set of positive integers. More specifically, the *primes,* those positive integers with no positive proper factors other than 1, are of special importance. A key result of number theory shows that the primes are the multiplicative building blocks of the positive integers. This result, called the *fundamental theorem of arithmetic,* tells us that every positive integer can be uniquely written as the product of primes in nondecreasing order. Interest in prime numbers goes back at least 2500 years, to the studies of ancient Greek mathematicians. Perhaps the first question about primes that comes to mind is whether there are infinitely many. In *The Elements,* the ancient Greek mathematician Euclid provided a proof, that there are infinitely many primes. This proof is considered to be one of the most beautiful proofs in all of mathematics. Interest in primes was rekindled in the seventeenth and eighteenth centuries, when mathematicians such as Pierre de Fermat and Leonhard Euler proved many important results and conjectured approaches for generating primes. The study of primes progressed substantially in the nineteenth century; results included the infinitude of primes in arithmetic progressions, and sharp estimates for the number of primes not exceeding a positive number x. The last 100 years has seen the development of many powerful techniques for the study of primes, but even with these powerful techniques, many questions remain unresolved. An example of a notorious unsolved question is whether there are infinitely many twin primes, which are pairs of primes that differ by 2. New results will certainly follow in the coming decades, as researchers continue working on the many open questions involving primes.

The development of modern number theory was made possible by the German mathematician Carl Friedrich Gauss, one of the greatest mathematicians in history, who in the early nineteenth century developed the language of *congruences.* We say that two integers a and b are congruent modulo m, where m is a positive integer, if m divides $a - b$. This language makes it easy to work with divisibility relationships in much the same way that we work with equations. Gauss developed many important concepts in number theory; for example, he proved one of its most subtle and beautiful results, the *law of quadratic reciprocity.* This law relates whether a prime p is a perfect square modulo a second prime q to whether q is a perfect square modulo p. Gauss developed many different proofs of this law, some of which have led to whole new areas of number theory.

Distinguishing primes from composite integers is a key problem of number theory. Work on this problem has produced an arsenal of *primality tests*. The simplest primality test is simply to check whether a positive integer is divisible by each prime not exceeding its square root. Unfortunately, this test is too inefficient to use for extremely large positive integers. Many different approaches have been used to determine whether an integer is prime. For example, in the nineteenth century, Pierre de Fermat showed that p divides $2^p - 2$ whenever p is prime. Some mathematicians thought that the converse also was true (that is, that if n divides $2^n - 2$, then n must be prime). However, it is not; by the early nineteenth century, composite integers n, such as 341, were known for which n divides $2^n - 2$. Such integers are called *pseudoprimes*. Though pseudoprimes exist, primality tests based on the fact that most composite integers are not pseudoprimes are now used to quickly find extremely large integers which are are extremely likely to be primes. However, they cannot be used to prove that an integer is prime. Finding an efficient method to prove that an integer is prime was an open question for hundreds of years. In a surprise to the mathematical community, this question was solved in 2002 by three Indian computer scientists, Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. Their algorithms can prove that an integer n is prime in polynomial time (in terms of the number of digits of n).

Factoring a positive integer into primes is another central problem in number theory. The factorization of a positive integer can be found using trial division, but this method is extremely time-consuming. Fermat, Euler, and many other mathematicians devised imaginative factorization algorithms, which have been extended in the past 30 years into a wide array of factoring methods. Using the best-known techniques, we can easily find primes with hundreds or even thousands of digits; factoring integers with the same number of digits, however, is beyond our most powerful computers.

The dichotomy between the time required to find large integers which are almost certainly prime and the time required to factor large integers is the basis of an extremely important secrecy system, the *RSA cryptosystem*. The RSA system is a public key cryptosystem, a security system in which each person has a public key and an associated private key. Messages can be encrypted by anyone using another person's public key, but these messages can be decrypted only by the owner of the private key. Concepts from number theory are essential to understanding the basic workings of the RSA cryptosystem, as well as many other parts of modern cryptography. The overwhelming importance of number theory in cryptography contradicts the earlier belief, held by many mathematicians, that number theory was unimportant for real-world applications. It is ironic that some famous mathematicians, such as G. H. Hardy, took pride in the notion that number theory would never be applied in the way that it is today.

The search for integer solutions of equations is another important part of number theory. An equation with the added proviso that only integer solutions are sought is called *diophantine*, after the ancient Greek mathematician Diophantus. Many different types of diophantine equations have been studied, but the most famous is the *Fermat equation* $x^n + y^n = z^n$. *Fermat's last theorem* states that if n is an integer greater than 2, this equation has no solutions in integers x, y, and z, where $xyz \neq 0$. Fermat conjectured in the seventeenth century that this theorem was true, and mathematicians (and others) searched for proofs for more than three centuries, but it was not until 1995 that the first proof was given by Andrew Wiles.

As Wiles's proof shows, number theory is not a static subject! New discoveries continue steadily to be made, and researchers frequently establish significant theoretical results. The fantastic power available when today's computers are linked over the Internet yields a rapid pace of new computational discoveries in number theory. Everyone can participate in this quest; for instance, you can join the quest for the new *Mersenne primes,* primes of the form $2^p - 1$, where p itself is prime. In August 2008, the first prime with more than 10 million decimal digits was found: the Mersenne prime $2^{43,112,609} - 1$. This discovery qualified for a $100,000 prize from the Electronic Frontier Foundation. A concerted effort is under way to find a prime with more than 100 million digits, with a $150,000 prize offered. After learning about some of the topics covered in this text, you may decide to join the hunt yourself, putting your idle computing resources to good use.

What is elementary number theory? You may wonder why the word "elementary" is part of the title of this book. This book considers only that part of number theory called *elementary number theory,* which is the part not dependent on advanced mathematics, such as the theory of complex variables, abstract algebra, or algebraic geometry. Students who plan to continue the study of mathematics will learn about more advanced areas of number theory, such as analytic number theory (which takes advantage of the theory of complex variables) and algebraic number theory (which uses concepts from abstract algebra to prove interesting results about algebraic number fields).

Some words of advice. As you embark on your study, keep in mind that number theory is a classical subject with results dating back thousands of years, yet is also the most modern of subjects, with new discoveries being made at a rapid pace. It is pure mathematics with the greatest intellectual appeal, yet it is also applied mathematics, with crucial applications to cryptography and other aspects of computer science and electrical engineering. I hope that you find the many facets of number theory as captivating as aficionados who have preceded you, many of whom retained an interest in number theory long after their school days were over.

Experimentation and exploration play a key role in the study of number theory. The results in this book were found by mathematicians who often examined large amounts of numerical evidence, looking for patterns and making conjectures. They worked diligently to prove their conjectures; some of these were proved and became theorems, others were rejected when counterexamples were found, and still others remain unresolved. As you study number theory, I recommend that you examine many examples, look for patterns, and formulate your own conjectures. You can examine small examples by hand, much as the founders of number theory did, but unlike these pioneers, you can also take advantage of today's vast computing power and computational engines. Working through examples, either by hand or with the aid of computers, will help you to learn the subject—and you may even find some new results of your own!