Graduate Texts in Mathematics

Kenneth Ireland
Michael Rosen

A Classical Introduction to Modern Number Theory

Second Edition

现代数论经典引论 第2版

Springer-Verlag
世界图书出版公司

Kenneth Ireland
Michael Rosen

A Classical Introduction to Modern Number Theory

Second Edition

Springer

书　　名：A Classical Introduction to Modern Number Theory 2nd ed.
作　　者：K. Ireland, M. Rosen
中 译 名：现代数论经典引论　第 2 版
出 版 者：世界图书出版公司北京公司
印 刷 者：北京世图印刷厂
发　　行：世界图书出版公司北京公司 (北京朝内大街 137 号　100010)
联系电话：010-64015659, 64038347
电子信箱：kjsk@vip.sina.com
开　　本：24　　印　张：17
出版年代：2003 年 6 月
书　　号：7-5062-6015-8/ O • 404
版权登记：图字: 01-2003-3763
定　　价：38.00 元

Graduate Texts in Mathematics 84

Springer
New York
Berlin
Heidelberg
Hong Kong
London
Milan
Paris
Tokyo

Graduate Texts in Mathematics

1 TAKEUTI/ZARING. Introduction to Axiomatic Set Theory. 2nd ed.
2 OXTOBY. Measure and Category. 2nd ed.
3 SCHAEFER. Topological Vector Spaces. 2nd ed.
4 HILTON/STAMMBACH. A Course in Homological Algebra. 2nd ed.
5 MAC LANE. Categories for the Working Mathematician. 2nd ed.
6 HUGHES/PIPER. Projective Planes.
7 J.-P. SERRE. A Course in Arithmetic.
8 TAKEUTI/ZARING. Axiomatic Set Theory.
9 HUMPHREYS. Introduction to Lie Algebras and Representation Theory.
10 COHEN. A Course in Simple Homotopy Theory.
11 CONWAY. Functions of One Complex Variable I. 2nd ed.
12 BEALS. Advanced Mathematical Analysis.
13 ANDERSON/FULLER. Rings and Categories of Modules. 2nd ed.
14 GOLUBITSKY/GUILLEMIN. Stable Mappings and Their Singularities.
15 BERBERIAN. Lectures in Functional Analysis and Operator Theory.
16 WINTER. The Structure of Fields.
17 ROSENBLATT. Random Processes. 2nd ed.
18 HALMOS. Measure Theory.
19 HALMOS. A Hilbert Space Problem Book. 2nd ed.
20 HUSEMOLLER. Fibre Bundles. 3rd ed.
21 HUMPHREYS. Linear Algebraic Groups.
22 BARNES/MACK. An Algebraic Introduction to Mathematical Logic.
23 GREUB. Linear Algebra. 4th ed.
24 HOLMES. Geometric Functional Analysis and Its Applications.
25 HEWITT/STROMBERG. Real and Abstract Analysis.
26 MANES. Algebraic Theories.
27 KELLEY. General Topology.
28 ZARISKI/SAMUEL. Commutative Algebra. Vol.I.
29 ZARISKI/SAMUEL. Commutative Algebra. Vol.II.
30 JACOBSON. Lectures in Abstract Algebra I. Basic Concepts.
31 JACOBSON. Lectures in Abstract Algebra II. Linear Algebra.
32 JACOBSON. Lectures in Abstract Algebra III. Theory of Fields and Galois Theory.
33 HIRSCH. Differential Topology.
34 SPITZER. Principles of Random Walk. 2nd ed.
35 ALEXANDER/WERMER. Several Complex Variables and Banach Algebras. 3rd ed.
36 KELLEY/NAMIOKA et al. Linear Topological Spaces.
37 MONK. Mathematical Logic.
38 GRAUERT/FRITZSCHE. Several Complex Variables.
39 ARVESON. An Invitation to C^*-Algebras.
40 KEMENY/SNELL/KNAPP. Denumerable Markov Chains. 2nd ed.
41 APOSTOL. Modular Functions and Dirichlet Series in Number Theory. 2nd ed.
42 J.-P. SERRE. Linear Representations of Finite Groups.
43 GILLMAN/JERISON. Rings of Continuous Functions.
44 KENDIG. Elementary Algebraic Geometry.
45 LOÈVE. Probability Theory I. 4th ed.
46 LOÈVE. Probability Theory II. 4th ed.
47 MOISE. Geometric Topology in Dimensions 2 and 3.
48 SACHS/WU. General Relativity for Mathematicians.
49 GRUENBERG/WEIR. Linear Geometry. 2nd ed.
50 EDWARDS. Fermat's Last Theorem.
51 KLINGENBERG. A Course in Differential Geometry.
52 HARTSHORNE. Algebraic Geometry.
53 MANIN. A Course in Mathematical Logic.
54 GRAVER/WATKINS. Combinatorics with Emphasis on the Theory of Graphs.
55 BROWN/PEARCY. Introduction to Operator Theory I: Elements of Functional Analysis.
56 MASSEY. Algebraic Topology: An Introduction.
57 CROWELL/FOX. Introduction to Knot Theory.
58 KOBLITZ. p-adic Numbers, p-adic Analysis, and Zeta-Functions. 2nd ed.
59 LANG. Cyclotomic Fields.
60 ARNOLD. Mathematical Methods in Classical Mechanics. 2nd ed.
61 WHITEHEAD. Elements of Homotopy Theory.
62 KARGAPOLOV/MERLZJAKOV. Fundamentals of the Theory of Groups.
63 BOLLOBAS. Graph Theory.

(continued after index)

Kenneth Ireland
(deceased)

Michael Rosen
Department of Mathematics
Brown University
Providence, RI 02912
USA

With 1 illustration.

Mathematics Subject Classification (2000): 11-01, 11-02

Library of Congress Cataloging-in-Publication Data
Ireland, Kenneth F.
A classical introduction to modern number theory / Kenneth Ireland, Michael Rosen.—2nd ed.
p. cm.—(Graduate texts in mathematics; 84)
Includes bibliographical references and index.
1. Number theory. I. Rosen, Michael I. II. Title. III. Series.
QA241.I667 1990
512.7—dc20

90-9848

Printed on acid-free paper.

"A Classical Introduction to Modern Number Theory" is a revised and expanded version of "Elements of Number Theory" published in 1972 by Bogden and Quigley, Inc., Publishers.

9 8 7

ISBN 0-387-97329-X
ISBN 3-540-97329-X SPIN 10900505

Springer-Verlag New York Berlin Heidelberg
A member of BertelsmannSpringer Science+Business Media GmbH

Preface to the Second Edition

It is now 10 years since the first edition of this book appeared in 1980. The intervening decade has seen tremendous advances take place in mathematics generally, and in number theory in particular. It would seem desirable to treat some of these advances, and with the addition of two new chapters, we are able to cover some portion of this new material.

As examples of important new work that we have not included, we mention the following two results:

(1) The first case of Fermat's last theorem is true for infinitely many prime exponents p. This means that, for infinitely many primes p, the equation $x^p + y^p = z^p$ has no solutions in nonzero integers with $p \nmid xyz$. This was proved by L.M. Adelman and D.R. Heath-Brown and independently by E. Fouvry. An overview of the proof is given by Heath-Brown in the *Mathematical Intelligencer* (Vol. 7, No. 6, 1985).

(2) Let p_1, p_2, and p_3 be three distinct primes. Then at least one of them is a primitive root for infinitely many primes q. Recall that E. Artin conjectured that, if $a \in \mathbb{Z}$ is not 0, 1, -1, or a square, then there are infinitely many primes q such that a is a primitive root modulo q. The theorem we have stated was proved in a weaker form by R. Gupta and M.R. Murty, and then strengthened by the combined efforts of R. Gupta, M.R. Murty, V.K. Murty, and D.R. Heath-Brown. An exposition of this result, as well as an analogue on elliptic curves, is given by M.R. Murty in the *Mathematical Intelligencer* (Vol. 10, No. 4, 1988).

The new material that we have added falls principally within the framework of arithmetic geometry. In Chapter 19 we give a complete proof of L.J. Mordell's fundamental theorem, which asserts that the group of rational points on an elliptic curve, defined over the rational numbers, is finitely generated. In keeping with the spirit of the book, the proof (due in essence to A. Weil) is elementary. It makes no use of cohomology groups or any other advanced machinery. It does use finiteness of class number and a weak form of the Dirichlet unit theorem; both results are proved in the text.

The second new chapter, Chapter 20, is an overview of G. Faltings's proof of the Mordell conjecture and recent progress on the arithmetic of

elliptic curves, especially the work of B. Gross, V.A. Kolyvagin, K. Rubin, and D. Zagier. Some of this work has surprising applications to other areas of number theory. We discuss one application to Fermat's last theorem, due to G. Frey, J.P. Serre, and K. Ribet. Another important application is the solution of an old problem due to K.F. Gauss about class numbers of imaginary quadratic number fields. This comes about by combining the work of B. Gross and D. Zagier with a result of D. Goldfeld. This chapter contains few proofs. Its main purpose is to give an informative survey in the hope that the reader will be inspired to learn the background necessary to a better understanding and appreciation of these important new developments.

The rest of the book is essentially unchanged. An attempt has been made to correct errors and misprints. In an effort to keep confusion to a minimum, we have not changed the bibliography at the end of the book. New references for the two new chapters, Chapters 19 and 20, will be found at the end of those chapters. We would like to thank Toru Nakahara and others for submitting a list of misprints from the first edition. Also, we thank Linda Guthrie for typing portions of the final chapters.

We have both been very pleased with the warm reception that the first edition of this book received. It is our hope that the new edition will continue to entice readers to delve deeper into the mysteries of this ancient, beautiful, and still vital subject.

February 1990

Kenneth Ireland
Michael Rosen

Addendum to Second Edition, Second Corrected Printing

The second printing of the second edition is unchanged except for corrections and the addition of a few clarifying comments. I would like to thank K. Conrad, M. Jastrzebski, F. Lemmermeyer and others who took the trouble to send us detailed lists of misprints.

November 1992

Michael Rosen

Notes for the Second Edition, Fifth Corrected Printing

In 1995 Andrew Wiles published a paper in the Annals of Mathematics which proved the Taniyama-Shimura-Weil conjecture is true for semi-stable elliptic curves over the rational numbers. Together with earlier results, principally the theorem of Ken Ribet mentioned on page 347, this proved Fermat's Last Theorem. The most famous conjecture in elementary number theory is finally a theorem!!!

April 1998

Michael Rosen

Preface

This book is a revised and greatly expanded version of our book *Elements of Number Theory* published in 1972. As with the first book the primary audience we envisage consists of upper level undergraduate mathematics majors and graduate students. We have assumed some familiarity with the material in a standard undergraduate course in abstract algebra. A large portion of Chapters 1–11 can be read even without such background with the aid of a small amount of supplementary reading. The later chapters assume some knowledge of Galois theory, and in Chapters 16 and 18 an acquaintance with the theory of complex variables is necessary.

Number theory is an ancient subject and its content is vast. Any introductory book must, of necessity, make a very limited selection from the fascinating array of possible topics. Our focus is on topics which point in the direction of algebraic number theory and arithmetic algebraic geometry. By a careful selection of subject matter we have found it possible to exposit some rather advanced material without requiring very much in the way of technical background. Most of this material is classical in the sense that is was discovered during the nineteenth century and earlier, but it is also modern because it is intimately related to important research going on at the present time.

In Chapters 1–5 we discuss prime numbers, unique factorization, arithmetic functions, congruences, and the law of quadratic reciprocity. Very little is demanded in the way of background. Nevertheless it is remarkable how a modicum of group and ring theory introduces unexpected order into the subject. For example, many scattered results turn out to be parts of the answer to a natural question: What is the structure of the group of units in the ring $\mathbb{Z}/n\mathbb{Z}$?

Reciprocity laws constitute a major theme in the later chapters. The law of quadratic reciprocity, beautiful in itself, is the first of a series of reciprocity laws which lead ultimately to the Artin reciprocity law, one of the major achievements of algebraic number theory. We travel along the road beyond quadratic reciprocity by formulating and proving the laws of cubic and biquadratic reciprocity. In preparation for this many of the techniques of algebraic number theory are introduced; algebraic numbers and algebraic integers, finite fields, splitting of primes, etc. Another important tool in this

investigation (and in others!) is the theory of Gauss and Jacobi sums. This material is covered in Chapters 6–9. Later in the book we formulate and prove the more advanced partial generalization of these results, the Eisenstein reciprocity law.

A second major theme is that of diophantine equations, at first over finite fields and later over the rational numbers. The discussion of polynomial equations over finite fields is begun in Chapters 8 and 10 and culminates in Chapter 11 with an exposition of a portion of the paper "Number of solutions of equations over finite fields" by A. Weil. This paper, published in 1948, has been very influential in the recent development of both algebraic geometry and number theory. In Chapters 17 and 18 we consider diophantine equations over the rational numbers. Chapter 17 covers many standard topics from sums of squares to Fermat's Last Theorem. However, because of material developed earlier we are able to treat a number of these topics from a novel point of view. Chapter 18 is about the arithmetic of elliptic curves. It differs from the earlier chapters in that it is primarily an overview with many definitions and statements of results but few proofs. Nevertheless, by concentrating on some important special cases we hope to convey to the reader something of the beauty of the accomplishments in this area where much work is being done and many mysteries remain.

The third, and final, major theme is that of zeta functions. In Chapter 11 we discuss the congruence zeta function associated to varieties defined over finite fields. In Chapter 16 we discuss the Riemann zeta function and the Dirichlet L-functions. In Chapter 18 we discuss the zeta function associated to an algebraic curve defined over the rational numbers and Hecke L-functions. Zeta functions compress a large amount of arithmetic information into a single function and make possible the application of the powerful methods of analysis to number theory.

Throughout the book we place considerable emphasis on the history of our subject. In the notes at the end of each chapter we give a brief historical sketch and provide references to the literature. The bibliography is extensive containing many items both classical and modern. Our aim has been to provide the reader with a wealth of material for further study.

There are many exercises, some routine, some challenging. Some of the exercises supplement the text by providing a step by step guide through the proofs of important results. In the later chapters a number of exercises have been adapted from results which have appeared in the recent literature. We hope that working through the exercises will be a source of enjoyment as well as instruction.

In the writing of this book we have been helped immensely by the interest and assistance of many mathematical friends and acquaintances. We thank them all. In particular we would like to thank Henry Pohlmann who insisted we follow certain themes to their logical conclusion, David Goss for allowing us to incorporate some of his work into Chapter 16, and Oisin McGuiness for his invaluable assistance in the preparation of Chapter 18. We would

like to thank Dale Cavanaugh, Janice Phillips, and especially Carol Ferreira, for their patience and expertise in typing large portions of the manuscript. Finally, the second author wishes to express his gratitude to the Vaughn Foundation Fund for financial support during his sabbatical year in Berkeley, California (1979/80).

July 25, 1981

Kenneth Ireland
Michael Rosen

Contents

Chapter 1

Unique Factorization

The notion of prime number is fundamental in number theory. The first part of this chapter is devoted to proving that every integer can be written as a product of primes in an essentially unique way.

After that, we shall prove an analogous theorem in the ring of polynomials over a field.

On a more abstract plane, the general idea of unique factorization is treated for principal ideal domains.

Finally, returning from the abstract to the concrete, the general theory is applied to two special rings that will be important later in the book.

§1 Unique Factorization in $\mathbb{Z}$

As a first approximation, number theory may be defined as the study of the natural numbers 1, 2, 3, 4, ... L. Kronecker once remarked (speaking of mathematics generally) that God made the natural numbers and all the rest is the work of man. Although the natural numbers constitute, in some sense, the most elementary mathematical system, the study of their properties has provided generations of mathematicians with problems of unending fascination.

We say that a number a divides a number b if there is a number c such that $b = ac$. If a divides b, we use the notation $a|b$. For example, $2|8$, $3|15$, but $6 \nmid 21$. If we are given a number, it is tempting to factor it again and again until further factorization is impossible. For example, $180 = 18 \times 10 = 2 \times 9 \times 2 \times 5 = 2 \times 3 \times 3 \times 2 \times 5$. Numbers that cannot be factored further are called primes. To be more precise, we say that a number p is a prime if its only divisors are 1 and p. Prime numbers are very important because every number can be written as a product of primes. Moreover, primes are of great interest because there are many problems about them that are easy to state but very hard to prove. Indeed many old problems about primes are unsolved to this day.

The first prime numbers are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, ... One may ask if there are infinitely many prime numbers. The answer is yes. Euclid gave an elegant proof of this fact over 2000 years ago. We shall give his proof and several others in Chapter 2. One can ask other questions

of this nature. Let $\pi(x)$ be the number of primes between 1 and x. What can be said about the function $\pi(x)$? Several mathematicians found by experiment that for large x the function $\pi(x)$ was approximately equal to $x/\ln(x)$. This assertion, known as the prime number theorem, was proved toward the end of the nineteenth century by J. Hadamard and independently by Ch.-J. de la Vallé Poussin. More precisely, they proved

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln(x)} = 1.$$

Even from a small list of primes one can notice that they have a tendency to occur in pairs, for example, 3 and 5, 5 and 7, 11 and 13, 17 and 19. Do there exist infinitely many prime pairs? The answer is unknown.

Another famous unsolved problem is known as the Goldbach conjecture (C. H. Goldbach). Can every even number be written as the sum of two primes? Goldbach came to this conjecture experimentally. Nowadays electronic computers make it possible to experiment with very large numbers. No counterexample to Goldbach's conjecture has ever been found. Great progress toward a proof has been given by I. M. Vinogradov and L. Schnirelmann. In 1937 Vinogradov was able to show that every sufficiently large odd number is the sum of three odd primes.

In this book we shall not study in depth the distribution of prime numbers or "additive" problems about them (such as the Goldbach conjecture). Rather our concern will be about the way primes enter into the multiplicative structure of numbers. The main theorem along these lines goes back essentially to Euclid. It is the theorem of unique factorization. This theorem is sometimes referred to as the fundamental theorem of arithmetic. It deserves the title. In one way or another almost all the results we shall discuss depend on it. The theorem states that every number can be factored into a product of primes in a unique way. What uniqueness means will be explained below.

As an illustration consider the number 180. We have seen that $180 = 2 \times 2 \times 3 \times 3 \times 5 = 2^2 \times 3^2 \times 5$. Uniqueness in this case means that the only primes dividing 180 are 2, 3, and 5 and that the exponents 2, 2, and 1 are uniquely determined by 180.

$\mathbb{Z}$ will denote the ring of integers, i.e., the set $0, \pm 1, \pm 2, \pm 3, \ldots$, together with the usual definition of sum and product. It will be more convenient to work with $\mathbb{Z}$ rather than restricting ourselves to the positive integers. The notion of divisibility carries over with no difficulty to $\mathbb{Z}$. If p is a positive prime, $-p$ will also be a prime. We shall not consider 1 or -1 as primes even though they fit the definition. This is simply a useful convention. Note that 1 and -1 divide everything and that they are the only integers with this property. They are called the units of $\mathbb{Z}$. Notice also that every nonzero integer divides zero. As is usual we shall exclude division by zero.

There are a number of simple properties of division that we shall simply list. The reader may wish to supply the proofs.