Graduate Texts in Mathematics 84

Kenneth Ireland
Michael Rosen

A Classical Introduction to Modern Number Theory

With 1 Illustration

Springer Science+Business Media, LLC

Kenneth Ireland
Department of Mathematics
University of New Brunswick
Fredericton
New Brunswick E3B 5A3
Canada

Michael Rosen
Department of Mathematics
Brown University
Providence, RI 02906
U.S.A.

AMS Subject Classifications (1980): 10-01, 12-01

Library of Congress Cataloging in Publication Data

Ireland, Kenneth F.
A classical introduction to modern number theory.
(Graduate texts in mathematics; 84)
Bibliography: p.
Includes index.
1. Numbers, Theory of. I. Rosen, Michael I.
II. Title. III. Series.
QA241.I667 512'.7 81-23265
AACR2

"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.

Originally published by Springer-Verlag New York Inc. in 1972 and 1982
Softcover reprint of the hardcover 1st edition 1982

9 8 7 6 5 4 3 2 1

ISBN 978-1-4757-1781-5 ISBN 978-1-4757-1779-2 (eBook)
DOI 10.1007/978-1-4757-1779-2

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