

Graduate Texts in Mathematics 84

Editorial Board

F. W. Gehring P. R. Halmos (Managing Editor)

C. C. Moore

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.

Editorial Board

P. R. Halmos
Managing Editor
Indiana University
Department of
Mathematics
Bloomington, IN 47401
U.S.A.

F. W. Gehring
University of Michigan
Department of
Mathematics
Ann Arbor, MI 48104
U.S.A.

C. C. Moore
University of California
at Berkeley
Department of Mathematics
Berkeley, CA 94720
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.

I. 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.

© 1982 by Springer Science+Business Media New York

Originally published by Springer-Verlag New York Inc. in 1972 and 1982

Softcover reprint of the hardcover 1st edition 1982

All rights reserved. No part of this book may be translated or reproduced in any form without written permission from Springer Science+Business Media, LLC.

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 it 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 Oisín McGuinness 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	1
1 Unique Factorization in \mathbb{Z}	1
2 Unique Factorization in $k[x]$	6
3 Unique Factorization in a Principal Ideal Domain	8
4 The Rings $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$	12
CHAPTER 2	
Applications of Unique Factorization	17
1 Infinitely Many Primes in \mathbb{Z}	17
2 Some Arithmetic Functions	18
3 $\sum 1/p$ Diverges	21
4 The Growth of $\pi(x)$	22
CHAPTER 3	
Congruence	28
1 Elementary Observations	28
2 Congruence in \mathbb{Z}	29
3 The Congruence $ax \equiv b \pmod{m}$	31
4 The Chinese Remainder Theorem	34

CHAPTER 4	
The Structure of $U(\mathbb{Z}/n\mathbb{Z})$	39
1 Primitive Roots and the Group Structure of $U(\mathbb{Z}/n\mathbb{Z})$	39
2 n th Power Residues	45
CHAPTER 5	
Quadratic Reciprocity	50
1 Quadratic Residues	50
2 Law of Quadratic Reciprocity	53
3 A Proof of the Law of Quadratic Reciprocity	58
CHAPTER 6	
Quadratic Gauss Sums	66
1 Algebraic Numbers and Algebraic Integers	66
2 The Quadratic Character of 2	69
3 Quadratic Gauss Sums	70
4 The Sign of the Quadratic Gauss Sum	73
CHAPTER 7	
Finite Fields	79
1 Basic Properties of Finite Fields	79
2 The Existence of Finite Fields	83
3 An Application to Quadratic Residues	85
CHAPTER 8	
Gauss and Jacobi Sums	88
1 Multiplicative Characters	88
2 Gauss Sums	91
3 Jacobi Sums	92
4 The Equation $x^n + y^n = 1$ in F_p	97
5 More on Jacobi Sums	98
6 Applications	101
7 A General Theorem	102
CHAPTER 9	
Cubic and Biquadratic Reciprocity	108
1 The Ring $\mathbb{Z}[\omega]$	109
2 Residue Class Rings	111
3 Cubic Residue Character	112

4 Proof of the Law of Cubic Reciprocity	115
5 Another Proof of the Law of Cubic Reciprocity	117
6 The Cubic Character of 2	118
7 Biquadratic Reciprocity: Preliminaries	119
8 The Quartic Residue Symbol	121
9 The Law of Biquadratic Reciprocity	123
10 Rational Biquadratic Reciprocity	127
11 The Constructibility of Regular Polygons	130
12 Cubic Gauss Sums and the Problem of Kummer	131

CHAPTER 10

Equations over Finite Fields 138

1 Affine Space, Projective Space, and Polynomials	138
2 Chevalley's Theorem	143
3 Gauss and Jacobi Sums over Finite Fields	145

CHAPTER 11

The Zeta Function 151

1 The Zeta Function of a Projective Hypersurface	151
2 Trace and Norm in Finite Fields	158
3 The Rationality of the Zeta Function Associated to $a_0x_0^m + a_1x_1^m + \cdots + a_nx_n^m$	161
4 A Proof of the Hasse–Davenport Relation	163
5 The Last Entry	166

CHAPTER 12

Algebraic Number Theory 172

1 Algebraic Preliminaries	172
2 Unique Factorization in Algebraic Number Fields	174
3 Ramification and Degree	181

CHAPTER 13

Quadratic and Cyclotomic Fields 188

1 Quadratic Number Fields	188
2 Cyclotomic Fields	193
3 Quadratic Reciprocity Revisited	199

CHAPTER 14

The Stickelberger Relation and the Eisenstein Reciprocity Law 203

- | | |
|---|-----|
| 1 The Norm of an Ideal | 203 |
| 2 The Power Residue Symbol | 204 |
| 3 The Stickelberger Relation | 207 |
| 4 The Proof of the Stickelberger Relation | 209 |
| 5 The Proof of the Eisenstein Reciprocity Law | 215 |
| 6 Three Applications | 220 |

CHAPTER 15

Bernoulli Numbers 228

- | | |
|---|-----|
| 1 Bernoulli Numbers; Definitions and Applications | 228 |
| 2 Congruences Involving Bernoulli Numbers | 234 |
| 3 Herbrand's Theorem | 241 |

CHAPTER 16

Dirichlet L -functions 249

- | | |
|--|-----|
| 1 The Zeta Function | 249 |
| 2 A Special Case | 251 |
| 3 Dirichlet Characters | 253 |
| 4 Dirichlet L -functions | 255 |
| 5 The Key Step | 257 |
| 6 Evaluating $L(s, \chi)$ at Negative Integers | 261 |

CHAPTER 17

Diophantine Equations 269

- | | |
|---|-----|
| 1 Generalities and First Examples | 269 |
| 2 The Method of Descent | 271 |
| 3 Legendre's Theorem | 272 |
| 4 Sophie Germain's Theorem | 275 |
| 5 Pell's Equation | 276 |
| 6 Sums of Two Squares | 278 |
| 7 Sums of Four Squares | 280 |
| 8 The Fermat Equation: Exponent 3 | 284 |
| 9 Cubic Curves with Infinitely Many Rational Points | 287 |
| 10 The Equation $y^2 = x^3 + k$ | 288 |
| 11 The First Case of Fermat's Conjecture for Regular Exponent | 290 |
| 12 Diophantine Equations and Diophantine Approximation | 292 |

CHAPTER 18	
Elliptic Curves	297
1 Generalities	297
2 Local and Global Zeta Functions of an Elliptic Curve	301
3 $y^2 = x^3 + D$, the Local Case	304
4 $y^2 = x^3 - Dx$, the Local Case	306
5 Hecke L -functions	307
6 $y^2 = x^3 - Dx$, the Global Case	310
7 $y^2 = x^3 + D$, the Global Case	312
8 Final Remarks	314
Selected Hints for the Exercises	319
Bibliography	327
Index	337