This book studies when a prime p can be written in the form $x^2 + ny^2$. It begins at an elementary level with results of Fermat and Euler and then discusses the work of Lagrange, Legendre and Gauss on quadratic reciprocity and the genus theory of quadratic forms. After exploring cubic and biquadratic reciprocity, the pace quickens with the introduction of algebraic number fields and class field theory. This leads to the concept of ring class field and a complete but abstract solution of $p = x^2 + ny^2$. To make things more concrete, the book introduces complex multiplication and modular functions to give a constructive solution. The book ends with a discussion of elliptic curves and Shimura reciprocity. Along the way the reader will encounter some compelling history and marvelous formulas, together with a complete solution of the class number one problem for imaginary quadratic fields. The book is accessible to readers with modest backgrounds in number theory. In the third edition, the numerous exercises have been thoroughly checked and revised, and as a special feature, complete solutions are included. This makes the book especially attractive to readers who want to get an active knowledge of this wonderful part of mathematics.

ISBN 978-1-4704-7028-9

9 781470 470289

CHEL/387

For additional information
and updates on this book, visit
www.ams.org/bookpages/chel-387

AMS
www.ams.org

Contents

Preface ix

First Edition ix

Second Edition ix

Third Edition with Solutions x

Notation xiii

Introduction 1

Chapter 1. From Fermat to Gauss 7

§1. Fermat, Euler and Quadratic Reciprocity 7

A. Fermat 7

B. Euler 8

C. $p = x^2 + ny^2$ and Quadratic Reciprocity 11

D. Beyond Quadratic Reciprocity 16

E. Exercises 17

§2. Lagrange, Legendre and Quadratic Forms 20

A. Quadratic Forms 20

B. $p = x^2 + ny^2$ and Quadratic Forms 25

C. Elementary Genus Theory 27

D. Lagrange and Legendre 31

E. Exercises 35

§3. Gauss, Composition and Genera 38

A. Composition and the Class Group 38

B. Genus Theory 43

C. $p = x^2 + ny^2$ and Euler's Convenient Numbers 48

D. Disquisitiones Arithmeticae 51

E. Exercises 53

§4. Cubic and Biquadratic Reciprocity 60

A. $\mathbb{Z}[\omega]$ and Cubic Reciprocity 60

B. $\mathbb{Z}[i]$ and Biquadratic Reciprocity 65

C. Gauss and Higher Reciprocity 67

D. Exercises 71

Chapter 2. Class Field Theory 77

§5. The Hilbert Class Field and $p = x^2 + ny^2$ 77

A. Number Fields 77

B. Quadratic Fields 81

C. The Hilbert Class Field 83

D. Solution of $p = x^2 + ny^2$ for Infinitely Many n 86
E. Exercises 91
§6. The Hilbert Class Field and Genus Theory 95
A. Genus Theory for Field Discriminants 95
B. Applications to the Hilbert Class Field 100
C. Exercises 101
§7. Orders in Imaginary Quadratic Fields 104
A. Orders in Quadratic Fields 105
B. Orders and Quadratic Forms 108
C. Ideals Prime to the Conductor 113
D. The Class Number 115
E. Exercises 118
§8. Class Field Theory and the Čebotarev Density Theorem 125
A. The Theorems of Class Field Theory 126
B. The Čebotarev Density Theorem 133
C. Norms and Ideles 136
D. Exercises 137
§9. Ring Class Fields and $p = x^2 + ny^2$ 141
A. Solution of $p = x^2 + ny^2$ for All n 142
B. The Ring Class Fields of $\mathbb{Z}[\sqrt{-27}]$ and $\mathbb{Z}[\sqrt{-64}]$ 145
C. Primes Represented by Positive Definite Quadratic Forms 148
D. Ring Class Fields and Generalized Dihedral Extensions 150
E. Exercises 152

Chapter 3. Complex Multiplication 157
§10. Elliptic Functions and Complex Multiplication 157
A. Elliptic Functions and the Weierstrass $\wp$-Function 157
B. The j-Invariant of a Lattice 162
C. Complex Multiplication 164
D. Exercises 170
§11. Modular Functions and Ring Class Fields 173
A. The j-Function 173
B. Modular Functions for $\Gamma_0(m)$ 177
C. The Modular Equation $\Phi_m(X, Y)$ 181
D. Complex Multiplication and Ring Class Fields 185
E. Exercises 190
§12. Modular Functions and Singular j-Invariants 195
A. The Cube Root of the j-Function 195
B. The Weber Functions 201
C. j-Invariants of Orders of Class Number 1 205
D. Weber's Computation of $j(\sqrt{-14})$ 207
E. Imaginary Quadratic Fields of Class Number 1 213
F. Exercises 216
§13. The Class Equation 225
A. Computing the Class Equation 225
B. Computing the Modular Equation 231
C. Theorems of Deuring, Gross and Zagier 235
D. Exercises 238

Chapter 4. Additional Topics 243
§14. Elliptic Curves 243
A. Elliptic Curves and Weierstrass Equations 243
B. Complex Multiplication and Elliptic Curves 246
C. Elliptic Curves over Finite Fields 249
D. Elliptic Curve Primality Tests 255
E. Exercises 261
§15. Shimura Reciprocity 265
A. Modular Functions 265
B. The Shimura Reciprocity Theorem 269
C. Extended Ring Class Fields 272
D. Shimura Reciprocity for Extended Ring Class Fields 274
E. Shimura Reciprocity for Ring Class Fields 278
F. Class Field Theory 284
G. Exercises 291

Solutions by Roger Lipsett and David Cox 297
Solutions to Exercises in §1 298
Solutions to Exercises in §2 306
Solutions to Exercises in §3 320
Solutions to Exercises in §4 340
Solutions to Exercises in §5 354
Solutions to Exercises in §6 367
Solutions to Exercises in §7 378
Solutions to Exercises in §8 397
Solutions to Exercises in §9 406
Solutions to Exercises in §10 421
Solutions to Exercises in §11 432
Solutions to Exercises in §12 445
Solutions to Exercises in §13 473
Solutions to Exercises in §14 486
Solutions to Exercises in §15 496

References 517

Further Reading 523

Index 525