CONTENTS

PREFACE ix

NOTATION xi

INTRODUCTION 1

CHAPTER ONE: FROM FERMAT TO GAUSS

§1. FERMAT, EULER AND QUADRATIC RECIPROCITY 7

A. Fermat 8
B. Euler 9
C. $p = x^2 + ny^2$ and Quadratic Reciprocity 12
D. Beyond Quadratic Reciprocity 19
E. Exercises 20

§2. LAGRANGE, LEGENDRE AND QUADRATIC FORMS 23

A. Quadratic Forms 24
B. $p = x^2 + ny^2$ and Quadratic Forms 30
C. Elementary Genus Theory 32
D. Lagrange and Legendre 37
E. Exercises 43

§3. GAUSS, COMPOSITION AND GENERA 47

A. Composition and the Class Group 47
B. Genus Theory 53
C. $p = x^2 + ny^2$ and Euler's Convenient Numbers 59
D. *Disquisitiones Arithmeticae* 63
E. Exercises 66

§4. CUBIC AND BIQUADRATIC RECIPROCITY 74

A. $\mathbf{Z}[\omega]$ and Cubic Reciprocity 75
B. $\mathbf{Z}[i]$ and Biquadratic Reciprocity 81
C. Gauss and Higher Reciprocity 83
D. Exercises 89

CHAPTER TWO: CLASS FIELD THEORY

§5. THE HILBERT CLASS FIELD AND $p = x^2 + ny^2$ 97

A. Number Fields 98
B. Quadratic Fields 103
C. The Hilbert Class Field 105
D. Solution of $p = x^2 + ny^2$ for infinitely many n 110
E. Exercises 115

§6. THE HILBERT CLASS FIELD AND GENUS THEORY 120

A. Genus Theory for Field Discriminants 121
B. Applications to the Hilbert Class Field 127
C. Exercises 128

§7. ORDERS IN IMAGINARY QUADRATIC FIELDS 132

A. Orders in Quadratic Fields 133
B. Orders and Quadratic Forms 137
C. Ideals Prime to the Conductor 143
D. The Class Number 146
E. Exercises 150

§8. CLASS FIELD THEORY AND THE ČEBOTAREV DENSITY THEOREM 159

A. The Theorems of Class Field Theory 159
B. The Čebotarev Density Theorem 168

C. Norms and Ideles 172
D. Exercises 174

§9. RING CLASS FIELDS AND $p = x^2 + ny^2$ 179

A. Solution of $p = x^2 + ny^2$ for all n 179
B. The Ring Class Fields of $\mathbb{Z}[\sqrt{-27}]$ and $\mathbb{Z}[\sqrt{-64}]$ 183
C. Primes Represented by Positive Definite Quadratic Forms 188
D. Ring Class Fields and Generalized Dihedral Extensions 190
E. Exercises 192

CHAPTER THREE: COMPLEX MULTIPLICATION

§10. ELLIPTIC FUNCTIONS AND COMPLEX MULTIPLICATION 199

A. Elliptic Functions and the Weierstrass $\wp$-Function 200
B. The j-Invariant of a Lattice 205
C. Complex Multiplication 208
D. Exercises 216

§11. MODULAR FUNCTIONS AND RING CLASS FIELDS 219

A. The j-Function 220
B. Modular Functions for $\Gamma_0(m)$ 225
C. The Modular Equation $\Phi_m(X,Y)$ 231
D. Complex Multiplication and Ring Class Fields 236
E. Exercises 242

§12. MODULAR FUNCTIONS AND SINGULAR j-INVARIANTS 248

A. The Cube Root of the j-Function 249
B. The Weber Functions 256
C. j-Invariants of Orders of Class Number 1 260
D. Weber's Computation of $j(\sqrt{-14})$ 263
E. Imaginary Quadratic Fields of Class Number 1 271
F. Exercises 274

§13. THE CLASS EQUATION 285

A. Computing the Class Equation 286
B. Computing the Modular Equation 293
C. Theorems of Deuring, Gross and Zagier 298
D. Exercises 303

§14. ELLIPTIC CURVES 308
A. Elliptic Curves and Weierstrass Equations 308
B. Complex Multiplication and Elliptic Curves 312
C. Elliptic Curves over Finite Fields 315
D. Elliptic Curve Primality Tests 323
E. Exercises 330

REFERENCES 335

INDEX 343