Kenneth Ireland
Michael Rosen

A Classical Introduction to Modern Number Theory

Second Edition

Springer

Contents

Preface to the Second Edition v
Preface vii

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 $\Sigma\, 1/p$ 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 $ax \equiv b(m)$ 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 nth 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

CHAPTER 19
The Mordell–Weil Theorem 319

§1 The Addition Law and Several Identities 320
§2 The Group $E/2E$ 323
§3 The Weak Dirichlet Unit Theorem 326
§4 The Weak Mordell–Weil Theorem 328
§5 The Descent Argument 330

CHAPTER 20
New Progress in Arithmetic Geometry 339

§1 The Mordell Conjecture 340
§2 Elliptic Curves 343
§3 Modular Curves 345
§4 Heights and the Height Regulator 348
§5 New Results on the Birch–Swinnerton-Dyer Conjecture 353
§6 Applications to Gauss's Class Number Conjecture 358

Selected Hints for the Exercises 367

Bibliography 375

Index 385