

# Contents

Preface to the Second Edition	v
Preface	vii
<b>CHAPTER 1</b>	
<b>Unique Factorization</b>	<b>1</b>
§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
<b>CHAPTER 2</b>	
<b>Applications of Unique Factorization</b>	<b>17</b>
§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
<b>CHAPTER 3</b>	
<b>Congruence</b>	<b>28</b>
§1 Elementary Observations	28
§2 Congruence in $\mathbb{Z}$	29
§3 The Congruence $ax \equiv b(m)$	31
§4 The Chinese Remainder Theorem	34
<b>CHAPTER 4</b>	
<b>The Structure of <math>U(\mathbb{Z}/n\mathbb{Z})</math></b>	<b>39</b>
§1 Primitive Roots and the Group Structure of $U(\mathbb{Z}/n\mathbb{Z})$	39
§2 $n$ th Power Residues	45
<b>CHAPTER 5</b>	
<b>Quadratic Reciprocity</b>	<b>50</b>
§1 Quadratic Residues	50
§2 Law of Quadratic Reciprocity	53
§3 A Proof of the Law of Quadratic Reciprocity	58

<b>CHAPTER 6</b>	
<b>Quadratic Gauss Sums</b>	<b>66</b>
§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
<b>CHAPTER 7</b>	
<b>Finite Fields</b>	<b>79</b>
§1 Basic Properties of Finite Fields	79
§2 The Existence of Finite Fields	83
§3 An Application to Quadratic Residues	85
<b>CHAPTER 8</b>	
<b>Gauss and Jacobi Sums</b>	<b>88</b>
§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
<b>CHAPTER 9</b>	
<b>Cubic and Biquadratic Reciprocity</b>	<b>108</b>
§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
<b>CHAPTER 10</b>	
<b>Equations over Finite Fields</b>	<b>138</b>
§1 Affine Space, Projective Space, and Polynomials	138
§2 Chevalley's Theorem	143
§3 Gauss and Jacobi Sums over Finite Fields	145

<b>CHAPTER 11</b>	
<b>The Zeta Function</b>	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
<b>CHAPTER 12</b>	
<b>Algebraic Number Theory</b>	172
§1 Algebraic Preliminaries	172
§2 Unique Factorization in Algebraic Number Fields	174
§3 Ramification and Degree	181
<b>CHAPTER 13</b>	
<b>Quadratic and Cyclotomic Fields</b>	188
§1 Quadratic Number Fields	188
§2 Cyclotomic Fields	193
§3 Quadratic Reciprocity Revisited	199
<b>CHAPTER 14</b>	
<b>The Stickelberger Relation and the Eisenstein Reciprocity Law</b>	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
<b>CHAPTER 15</b>	
<b>Bernoulli Numbers</b>	228
§1 Bernoulli Numbers; Definitions and Applications	228
§2 Congruences Involving Bernoulli Numbers	234
§3 Herbrand's Theorem	241
<b>CHAPTER 16</b>	
<b>Dirichlet <math>L</math>-functions</b>	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

<b>CHAPTER 17</b>	
<b>Diophantine Equations</b>	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
<b>CHAPTER 18</b>	
<b>Elliptic Curves</b>	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
<b>CHAPTER 19</b>	
<b>The Mordell–Weil Theorem</b>	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
<b>CHAPTER 20</b>	
<b>New Progress in Arithmetic Geometry</b>	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
<b>Selected Hints for the Exercises</b>	367
<b>Bibliography</b>	375
<b>Index</b>	385