

# Contents

---

<b>Preface</b>	<b>xiii</b>
Some Features of This Book . . . . .	xiv
A Note to Students . . . . .	xv
A Note to Instructors . . . . .	xv
<b>Notation</b>	<b>xvii</b>
<b>1 Early Number Theory</b>	<b>1</b>
1.1 Ancient Mathematics . . . . .	1
1.2 Diophantus . . . . .	7
Geometry and Pythagorean Triples . . . . .	8
The Method of Diophantus . . . . .	11
Fermat's Last Theorem . . . . .	14
Connections: Congruent Numbers . . . . .	16
1.3 Euclid . . . . .	20
Greek Number Theory . . . . .	21
Division and Remainders . . . . .	22
Linear Combinations and Euclid's Lemma . . . . .	24
Euclidean Algorithm . . . . .	30
1.4 Nine Fundamental Properties . . . . .	36
1.5 Connections . . . . .	41
Trigonometry . . . . .	41
Integration . . . . .	42
<b>2 Induction</b>	<b>45</b>
2.1 Induction and Applications . . . . .	45
Unique Factorization . . . . .	53
Strong Induction . . . . .	57
Differential Equations . . . . .	60
2.2 Binomial Theorem . . . . .	63
Combinatorics . . . . .	69
2.3 Connections . . . . .	73
An Approach to Induction . . . . .	73
Fibonacci Sequence . . . . .	75
<b>3 Renaissance</b>	<b>81</b>
3.1 Classical Formulas . . . . .	82
3.2 Complex Numbers . . . . .	91

	Algebraic Operations . . . . .	92
	Absolute Value and Direction . . . . .	99
	The Geometry Behind Multiplication . . . . .	101
3.3	Roots and Powers . . . . .	106
3.4	Connections: Designing Good Problems . . . . .	116
	Norms . . . . .	116
	Pippins and Cheese . . . . .	118
	Gaussian Integers: Pythagorean Triples Revisited. . . . .	119
	Eisenstein Triples and Diophantus . . . . .	122
	Nice Boxes. . . . .	123
	Nice Functions for Calculus Problems. . . . .	124
	Lattice Point Triangles . . . . .	126
<b>4</b>	<b>Modular Arithmetic</b>	<b>131</b>
4.1	Congruence . . . . .	131
4.2	Public Key Codes . . . . .	149
4.3	Commutative Rings . . . . .	154
	Units and Fields . . . . .	160
	Subrings and Subfields . . . . .	166
4.4	Connections: Julius and Gregory . . . . .	169
4.5	Connections: Patterns in Decimal Expansions . . . . .	177
	Real Numbers . . . . .	177
	Decimal Expansions of Rationals . . . . .	179
	Periods and Blocks . . . . .	182
<b>5</b>	<b>Abstract Algebra</b>	<b>191</b>
5.1	Domains and Fraction Fields . . . . .	192
5.2	Polynomials . . . . .	196
	Polynomial Functions . . . . .	204
5.3	Homomorphisms . . . . .	206
	Extensions of Homomorphisms . . . . .	213
	Kernel, Image, and Ideals . . . . .	216
5.4	Connections: Boolean Things . . . . .	221
	Inclusion-Exclusion . . . . .	227
<b>6</b>	<b>Arithmetic of Polynomials</b>	<b>233</b>
6.1	Parallels to $\mathbb{Z}$ . . . . .	233
	Divisibility . . . . .	233
	Roots . . . . .	239
	Greatest Common Divisors . . . . .	243
	Unique Factorization . . . . .	248
	Principal Ideal Domains . . . . .	255
6.2	Irreducibility . . . . .	259
	Roots of Unity . . . . .	264
6.3	Connections: Lagrange Interpolation . . . . .	270
<b>7</b>	<b>Quotients, Fields, and Classical Problems</b>	<b>277</b>
7.1	Quotient Rings . . . . .	277
7.2	Field Theory . . . . .	287
	Characteristics . . . . .	287
	Extension Fields . . . . .	289

Algebraic Extensions . . . . .	293
Splitting Fields . . . . .	300
Classification of Finite Fields . . . . .	305
7.3 Connections: Ruler–Compass Constructions . . . . .	308
Constructing Regular $n$ -gons . . . . .	320
Gauss’s construction of the 17-gon . . . . .	322
<b>8 Cyclotomic Integers</b>	<b>329</b>
8.1 Arithmetic in Gaussian and Eisenstein Integers . . . . .	330
Euclidean Domains . . . . .	333
8.2 Primes Upstairs and Primes Downstairs . . . . .	337
Laws of Decomposition . . . . .	339
8.3 Fermat’s Last Theorem for Exponent 3 . . . . .	349
Preliminaries . . . . .	350
The First Case . . . . .	351
Gauss’s Proof of the Second Case . . . . .	354
8.4 Approaches to the General Case . . . . .	359
Cyclotomic integers . . . . .	360
Kummer, Ideal Numbers, and Dedekind . . . . .	365
8.5 Connections: Counting Sums of Squares . . . . .	371
A Proof of Fermat’s Theorem on Divisors . . . . .	373
<b>9 Epilog</b>	<b>379</b>
9.1 Abel and Galois . . . . .	379
9.2 Solvability by Radicals . . . . .	381
9.3 Symmetry . . . . .	384
9.4 Groups . . . . .	389
9.5 Wiles and Fermat’s Last Theorem . . . . .	396
Elliptic Integrals and Elliptic Functions . . . . .	397
Congruent Numbers Revisited . . . . .	400
Elliptic Curves . . . . .	404
<b>A Appendices</b>	<b>409</b>
A.1 Functions . . . . .	409
A.2 Equivalence Relations . . . . .	420
A.3 Vector Spaces . . . . .	424
Bases and Dimension . . . . .	427
Linear Transformations . . . . .	435
A.4 Inequalities . . . . .	441
A.5 Generalized Associativity . . . . .	442
A.6 A Cyclotomic Integer Calculator . . . . .	444
Eisenstein Integers . . . . .	445
Symmetric Polynomials . . . . .	446
Algebra with Periods . . . . .	446
<b>References</b>	<b>449</b>
<b>Index</b>	<b>451</b>
<b>About the Authors</b>	<b>459</b>