
Contents

Preface	xix
1 Introduction	1
1.1 Diophantine Equations	2
1.2 Modular Arithmetic	4
1.3 Primes and the Distribution of Primes	5
1.4 Cryptography	7
2 Divisibility	9
2.1 Divisibility	9
2.2 Euclid's Theorem	11
2.3 Euclid's Original Proof	13
2.4 The Sieve of Eratosthenes	15
2.5 The Division Algorithm	17
2.5.1 A Cryptographic Application	19
2.6 The Greatest Common Divisor	20
2.7 The Euclidean Algorithm	23
2.7.1 The Extended Euclidean Algorithm	25
2.8 Other Bases	31
2.9 Fermat and Mersenne Numbers	34
2.10 Chapter Highlights	38
2.11 Problems	38
2.11.1 Exercises	38
2.11.2 Projects	45
2.11.3 Computer Explorations	47
2.11.4 Answers to "Check Your Understanding"	48
	ix

3	Linear Diophantine Equations	51
3.1	$ax + by = c$	51
3.2	The Postage Stamp Problem	57
3.3	Chapter Highlights	60
3.4	Problems	60
3.4.1	Exercises	60
3.4.2	Answers to “Check Your Understanding”	62
4	Unique Factorization	63
4.1	The Starting Point	63
4.2	The Fundamental Theorem of Arithmetic	64
4.3	Euclid and the Fundamental Theorem of Arithmetic . .	69
4.4	Chapter Highlights	70
4.5	Problems	71
4.5.1	Exercises	71
4.5.2	Projects	73
4.5.3	Answers to “Check Your Understanding”	73
5	Applications of Unique Factorization	75
5.1	A Puzzle	75
5.2	Irrationality Proofs	77
5.2.1	Four More Proofs That $\sqrt{2}$ Is Irrational	79
5.3	The Rational Root Theorem	81
5.4	Pythagorean Triples	84
5.5	Differences of Squares	90
5.6	Prime Factorization of Factorials	92
5.7	The Riemann Zeta Function	94
5.7.1	$\sum 1/p$ Diverges	100
5.8	Chapter Highlights	105
5.9	Problems	106
5.8.1	Exercises	106
5.9.2	Projects	108
5.9.3	Computer Explorations	112

5.9.4	Answers to “Check Your Understanding”	112
6	Congruences	113
6.1	Definitions and Examples	113
6.2	Modular Exponentiation	122
6.3	Divisibility Tests	124
6.4	Linear Congruences	129
6.5	The Chinese Remainder Theorem	136
6.6	Fractions mod m	141
6.7	Queens on a Chessboard	143
6.8	Chapter Highlights	145
6.9	Problems	145
6.9.1	Exercises	145
6.9.2	Projects	152
6.9.3	Computer Explorations	153
6.9.4	Answers to “Check Your Understanding”	154
7	Classical Cryptosystems	155
7.1	Introduction	155
7.2	Shift and Affine Ciphers	156
7.3	Vigenère Ciphers	161
7.4	Transposition Ciphers	167
7.5	Stream Ciphers	170
7.5.1	One-Time Pad	171
7.5.2	Linear Feedback Shift Registers (LFSR)	172
7.6	Block Ciphers	175
7.7	Secret Sharing	179
7.8	Generating Random Numbers	181
7.9	Chapter Highlights	183
7.10	Problems	183
7.10.1	Exercises	183
7.10.2	Answers to “Check Your Understanding”	186

8	Fermat, Euler, and Wilson	189
8.1	Fermat's Theorem	189
8.2	Euler's Theorem	194
8.3	Wilson's Theorem	200
8.4	Chapter Highlights	202
8.5	Problems	203
8.5.1	Exercises	203
8.5.2	Projects	206
8.5.3	Computer Explorations	207
8.5.4	Answers to "Check Your Understanding"	207
9	RSA	209
9.1	RSA Encryption	210
9.2	Digital Signatures	217
9.3	Chapter Highlights	219
9.4	Problems	219
9.4.1	Exercises	219
9.4.2	Projects	224
9.4.3	Computer Explorations	225
9.4.4	Answers to "Check Your Understanding"	226
10	Polynomial Congruences	227
10.1	Polynomials Mod Primes	227
10.2	Solutions Modulo Prime Powers	230
10.3	Composite Moduli	234
10.4	Chapter Highlights	235
10.5	Problems	235
10.5.1	Exercises	235
10.5.2	Projects	236
10.5.3	Computer Explorations	237
10.5.4	Answers to "Check Your Understanding"	238

11 Order and Primitive Roots	239
11.1 Orders of Elements	239
11.1.1 Fermat Numbers	241
11.1.2 Mersenne Numbers	243
11.2 Primitive Roots	244
11.3 Decimals	250
11.3.1 Midy's Theorem	253
11.4 Card Shuffling	255
11.5 The Discrete Log Problem	257
11.5.1 Baby Step–Giant Step Method	258
11.5.2 The Index Calculus	260
11.6 Existence of Primitive Roots	263
11.7 Chapter Highlights	266
11.8 Problems	266
11.7.1 Exercises	266
11.8.2 Projects	269
11.8.3 Computer Explorations	271
11.8.4 Answers to “Check Your Understanding”	271
12 More Cryptographic Applications	273
12.1 Diffie–Hellman Key Exchange	273
12.2 Coin Flipping over the Telephone	275
12.3 Mental Poker	277
12.4 The ElGamal Public Key Cryptosystem	282
12.5 Chapter Highlights	285
12.6 Problems	285
12.6.1 Exercises	285
12.6.2 Projects	287
12.6.3 Computer Explorations	287
12.6.4 Answers to “Check Your Understanding”	288

13 Quadratic Reciprocity	289
13.1 Squares and Square Roots Mod Primes	289
13.2 Computing Square Roots Mod p	296
13.3 Quadratic Equations	298
13.4 The Jacobi Symbol	300
13.5 Proof of Quadratic Reciprocity	305
13.6 Chapter Highlights	312
13.7 Problems	312
13.7.1 Exercises	312
13.7.2 Projects	316
13.7.3 Answers to “Check Your Understanding”	318
14 Primality and Factorization	319
14.1 Trial Division and Fermat Factorization	319
14.2 Primality Testing	323
14.2.1 Pseudoprimes	323
14.2.2 The Pocklington–Lehmer Primality Test	328
14.2.3 The AKS Primality Test	331
14.2.4 Fermat Numbers	333
14.2.5 Mersenne Numbers	335
14.3 Factorization	335
14.3.1 $x^2 \equiv y^2$	336
14.3.2 Factoring Pseudoprimes and Factoring Using RSA Exponents	339
14.3.3 Pollard’s $p - 1$ Method	340
14.3.4 The Quadratic Sieve	342
14.4 Coin Flipping over the Telephone	350
14.5 Chapter Highlights	352
14.6 Problems	352
14.6.1 Exercises	352
14.6.2 Projects	355
14.6.3 Computer Explorations	355
14.6.4 Answers to “Check Your Understanding”	356

15 Geometry of Numbers	357
15.1 Volumes and Minkowski's Theorem	357
15.2 Sums of Two Squares	362
15.2.1 Algorithm for Writing $p \equiv 1 \pmod{4}$ as a Sum of Two Squares	366
15.3 Sums of Four Squares	368
15.4 Pell's Equation	370
15.4.1 Bhāskara's Chakravala Method	373
15.5 Chapter Highlights	376
15.6 Problems	376
15.6.1 Exercises	376
15.6.2 Projects	380
15.6.3 Answers to "Check Your Understanding"	384
16 Arithmetic Functions	385
16.1 Perfect Numbers	385
16.2 Multiplicative Functions	389
16.3 Chapter Highlights	395
16.4 Problems	395
16.3.1 Exercises	395
16.4.2 Projects	397
16.4.3 Computer Explorations	398
16.4.4 Answers to "Check Your Understanding"	399
17 Continued Fractions	401
17.1 Rational Approximations; Pell's Equation	402
17.1.1 Evaluating Continued Fractions	405
17.1.2 Pell's Equation	407
17.2 Basic Theory	410
17.3 Rational Numbers	418
17.4 Periodic Continued Fractions	420
17.4.1 Purely Periodic Continued Fractions	422
17.4.2 Eventually Periodic Continued Fractions	427

17.5 Square Roots of Integers	429
17.6 Some Irrational Numbers	432
17.7 Chapter Highlights	438
17.8 Problems	438
17.8.1 Exercises	438
17.8.2 Projects	439
17.8.3 Computer Explorations	441
17.8.4 Answers to “Check Your Understanding”	441
18 Gaussian Integers	443
18.1 Complex Arithmetic	443
18.2 Gaussian Irreducibles	445
18.3 The Division Algorithm	449
18.4 Unique Factorization	452
18.5 Applications	458
18.5.1 Sums of Two Squares	458
18.5.2 Pythagorean Triples	461
18.5.3 $y^2 = x^3 - 1$	462
18.6 Chapter Highlights	464
18.7 Problems	464
18.7.1 Exercises	464
18.7.2 Projects	465
18.7.3 Computer Explorations	465
18.7.4 Answers to “Check Your Understanding”	465
19 Algebraic Integers	467
19.1 Quadratic Fields and Algebraic Integers	467
19.2 Units	472
19.3 $\mathbb{Z}[\sqrt{-2}]$	476
19.4 $\mathbb{Z}[\sqrt{3}]$	479
19.4.1 The Lucas–Lehmer Test	482
19.5 Non-Unique Factorization	486
19.6 Chapter Highlights	488

19.7 Problems	488
19.7.1 Exercises	488
19.7.2 Projects	489
19.7.3 Answers to “Check Your Understanding”	491
20 The Distribution of Primes	493
20.1 Bertrand’s Postulate	493
20.2 Chebyshev’s Approximate Prime Number Theorem	502
20.3 Chapter Highlights	507
20.4 Problems	508
20.4.1 Exercises	508
20.4.2 Projects	509
20.4.3 Computer Explorations	510
21 Epilogue: Fermat’s Last Theorem	511
21.1 Introduction	511
21.2 Elliptic Curves	514
21.3 Modularity	517
A Supplementary Topics	521
A.1 What Is a Proof?	521
A.1.1 Proof by Contradiction	527
A.2 Geometric Series	530
A.3 Mathematical Induction	531
A.4 Pascal’s Triangle and the Binomial Theorem	537
A.5 Fibonacci Numbers	543
A.6 Matrices	546
A.7 Problems	550
A.7.1 Exercises	550
A.7.2 Answers to “Check Your Understanding”	552
B Answers and Hints for Odd-Numbered Exercises	555
Index	573