# *Contents*

**Preface** **xv**

**0 Introduction** **1**

0.1 Diophantine Equations . . . . . 2
0.2 Modular Arithmetic . . . . . 4
0.3 Primes and the Distribution of Primes . . . . . 5
0.4 Cryptography . . . . . 7

**1 Divisibility** **9**

1.1 Divisibility . . . . . 9
1.2 Euclid's Theorem . . . . . 11
1.3 Euclid's Original Proof . . . . . 13
1.4 The Sieve of Eratosthenes . . . . . 15
1.5 The Division Algorithm . . . . . 17
1.5.1 A Cryptographic Application . . . . . 19
1.6 The Greatest Common Divisor . . . . . 20
1.7 The Euclidean Algorithm . . . . . 22
1.7.1 The Extended Euclidean Algorithm . . . . . 25
1.8 Other Bases . . . . . 30
1.9 Linear Diophantine Equations . . . . . 32
1.10 The Postage Stamp Problem . . . . . 38
1.11 Fermat and Mersenne Numbers . . . . . 41
1.12 Chapter Highlights . . . . . 46
1.13 Problems . . . . . 46
1.13.1 Exercises . . . . . 46
1.13.2 Projects . . . . . 53
1.13.3 Computer Explorations . . . . . 55

1.13.4 Answers to "Check Your Understanding" . . 57

**2 Unique Factorization 59**

2.1 Preliminary Results . . . . . 59
2.2 The Fundamental Theorem of Arithmetic . . . . . 61
2.3 Euclid and the Fundamental Theorem of Arithmetic 66
2.4 Chapter Highlights . . . . . 67
2.5 Problems . . . . . 67
2.5.1 Exercises . . . . . 67
2.5.2 Projects . . . . . 68
2.5.3 Answers to "Check Your Understanding" . . 70

**3 Applications of Unique Factorization 71**

3.1 A Puzzle . . . . . 71
3.2 Irrationality Proofs . . . . . 73
3.2.1 Four More Proofs That $\sqrt{2}$ Is Irrational . . 75
3.3 The Rational Root Theorem . . . . . 77
3.4 Pythagorean Triples . . . . . 80
3.5 Differences of Squares . . . . . 86
3.6 Prime Factorization of Factorials . . . . . 88
3.7 The Riemann Zeta Function . . . . . 90
3.8 Chapter Highlights . . . . . 96
3.9 Problems . . . . . 96
3.9.1 Exercises . . . . . 96
3.9.2 Projects . . . . . 100
3.9.3 Computer Explorations . . . . . 104
3.9.4 Answers to "Check Your Understanding" . . 105

**4 Congruences 107**

4.1 Definitions and Examples . . . . . 107
4.2 Modular Exponentiation . . . . . 115
4.3 Divisibility Tests . . . . . 116
4.4 Linear Congruences . . . . . 120
4.5 The Chinese Remainder Theorem . . . . . 127

4.6 Fractions mod $m$ . . . . . 132
4.7 Fermat's Theorem . . . . . 134
4.8 Euler's Theorem . . . . . 139
4.9 Wilson's Theorem . . . . . 147
4.10 Queens on a Chessboard . . . . . 149
4.11 Chapter Highlights . . . . . 151
4.12 Problems . . . . . 151
4.12.1 Exercises . . . . . 151
4.12.2 Projects . . . . . 159
4.12.3 Computer Explorations . . . . . 163
4.12.4 Answers to "Check Your Understanding" . . 164

**5 Cryptographic Applications 167**
5.1 Introduction . . . . . 167
5.2 Shift and Affine Ciphers . . . . . 170
5.3 Secret Sharing . . . . . 175
5.4 RSA . . . . . 177
5.5 Chapter Highlights . . . . . 184
5.6 Problems . . . . . 184
5.6.1 Exercises . . . . . 184
5.6.2 Projects . . . . . 188
5.6.3 Computer Explorations . . . . . 191
5.6.4 Answers to "Check Your Understanding" . . 192

**6 Polynomial Congruences 193**
6.1 Polynomials Mod Primes . . . . . 193
6.2 Solutions Modulo Prime Powers. . . . . 196
6.3 Composite Moduli . . . . . 202
6.4 Chapter Highlights . . . . . 203
6.5 Problems . . . . . 203
6.5.1 Exercises . . . . . 203
6.5.2 Projects . . . . . 204
6.5.3 Computer Explorations . . . . . 205

6.5.4 Answers to "Check Your Understanding" . . 206

**7 Order and Primitive Roots 207**

7.1 Orders of Elements . . . . . 207
7.1.1 Fermat Numbers . . . . . 209
7.1.2 Mersenne Numbers . . . . . 211
7.2 Primitive Roots . . . . . 211
7.3 Decimals . . . . . 217
7.3.1 Midy's Theorem . . . . . 220
7.4 Card Shuffling . . . . . 222
7.5 The Discrete Log Problem . . . . . 224
7.5.1 Baby Step-Giant Step Method . . . . . 226
7.5.2 The Index Calculus . . . . . 228
7.6 Existence of Primitive Roots . . . . . 231
7.7 Chapter Highlights . . . . . 233
7.8 Problems . . . . . 234
7.8.1 Exercises . . . . . 234
7.8.2 Projects . . . . . 238
7.8.3 Computer Explorations . . . . . 239
7.8.4 Answers to "Check Your Understanding" . . 240

**8 More Cryptographic Applications 241**

8.1 Diffie-Hellman Key Exchange . . . . . 241
8.2 Coin Flipping over the Telephone . . . . . 243
8.3 Mental Poker . . . . . 246
8.4 The ElGamal Public Key Cryptosystem . . . . . 250
8.5 Digital Signatures . . . . . 253
8.6 Chapter Highlights . . . . . 255
8.7 Problems . . . . . 255
8.7.1 Exercises . . . . . 255
8.7.2 Projects . . . . . 259
8.7.3 Computer Explorations . . . . . 260
8.7.4 Answers to "Check Your Understanding" . . 260

**9 Quadratic Reciprocity** **263**

9.1 Squares and Square Roots Mod Primes . . . . . 263
9.2 Computing Square Roots Mod $p$ . . . . . 270
9.3 Quadratic Equations . . . . . 272
9.4 The Jacobi Symbol . . . . . 274
9.5 Proof of Quadratic Reciprocity . . . . . 278
9.6 Chapter Highlights . . . . . 285
9.7 Problems . . . . . 286
9.7.1 Exercises . . . . . 286
9.7.2 Projects . . . . . 291
9.7.3 Answers to "Check Your Understanding" . . 293

**10 Primality and Factorization** **295**

10.1 Trial Division and Fermat Factorization . . . . . 295
10.2 Primality Testing . . . . . 299
10.2.1 Pseudoprimes . . . . . 299
10.2.2 The Pocklington-Lehmer Primality Test . . 304
10.2.3 The AKS Primality Test . . . . . 307
10.2.4 Fermat Numbers . . . . . 309
10.2.5 Mersenne Numbers . . . . . 311
10.3 Factorization . . . . . 312
10.3.1 $x^2 \equiv y^2$ . . . . . 312
10.3.2 Factoring Pseudoprimes and Factoring Using RSA Exponents . . . . . 315
10.3.3 Pollard's $p-1$ Method . . . . . 316
10.3.4 The Quadratic Sieve . . . . . 318
10.4 Coin Flipping over the Telephone . . . . . 326
10.5 Chapter Highlights . . . . . 328
10.6 Problems . . . . . 329
10.6.1 Exercises . . . . . 329
10.6.2 Projects . . . . . 332
10.6.3 Computer Explorations . . . . . 333
10.6.4 Answers to "Check Your Understanding" . . 334

**11 Geometry of Numbers** **337**

11.1 Volumes and Minkowski's Theorem . . . . . 337

11.2 Sums of Two Squares . . . . . 342

11.2.1 Algorithm for Writing $p \equiv 1 \pmod 4$ as a Sum of Two Squares . . . . . 345

11.3 Sums of Four Squares . . . . . 347

11.4 Pell's Equation . . . . . 349

11.4.1 Bhāskara's Chakravala Method . . . . . 353

11.5 Chapter Highlights . . . . . 355

11.6 Problems . . . . . 356

11.6.1 Exercises . . . . . 356

11.6.2 Projects . . . . . 359

11.6.3 Answers to "Check Your Understanding" . . 365

**12 Arithmetic Functions** **367**

12.1 Perfect Numbers . . . . . 367

12.2 Multiplicative Functions . . . . . 371

12.3 Chapter Highlights . . . . . 378

12.4 Problems . . . . . 378

12.4.1 Exercises . . . . . 378

12.4.2 Projects . . . . . 381

12.4.3 Computer Explorations . . . . . 381

12.4.4 Answers to "Check Your Understanding" . . 382

**13 Continued Fractions** **383**

13.1 Rational Approximations; Pell's Equation . . . . . 384

13.1.1 Evaluating Continued Fractions . . . . . 387

13.1.2 Pell's Equation . . . . . 389

13.2 Basic Theory . . . . . 392

13.3 Rational Numbers . . . . . 400

13.4 Periodic Continued Fractions . . . . . 402

13.4.1 Purely Periodic Continued Fractions . . . . 404

13.4.2 Eventually Periodic Continued Fractions . . 409

13.5 Square Roots of Integers . . . . . 411
13.6 Some Irrational Numbers . . . . . 414
13.7 Chapter Highlights . . . . . 420
13.8 Problems . . . . . 421
13.8.1 Exercises . . . . . 421
13.8.2 Projects . . . . . 422
13.8.3 Computer Explorations . . . . . 425
13.8.4 Answers to "Check Your Understanding" . . 425

**14 Gaussian Integers** **427**
14.1 Complex Arithmetic . . . . . 427
14.2 Gaussian Irreducibles . . . . . 429
14.3 The Division Algorithm . . . . . 433
14.4 Unique Factorization . . . . . 436
14.5 Applications . . . . . 442
14.5.1 Sums of Two Squares . . . . . 442
14.5.2 Pythagorean Triples . . . . . 445
14.5.3 $y^2 = x^3 - 1$ . . . . . 447
14.6 Chapter Highlights . . . . . 448
14.7 Problems . . . . . 449
14.7.1 Exercises . . . . . 449
14.7.2 Projects . . . . . 450
14.7.3 Computer Explorations . . . . . 450
14.7.4 Answers to "Check Your Understanding" . . 450

**15 Algebraic Integers** **453**
15.1 Quadratic Fields and Algebraic Integers . . . . . 453
15.2 Units . . . . . 458
15.3 $\mathbb{Z}[\sqrt{-2}]$ . . . . . 462
15.4 $\mathbb{Z}[\sqrt{3}]$ . . . . . 466
15.4.1 The Lucas-Lehmer Test . . . . . 469
15.5 Non-unique Factorization . . . . . 472
15.6 Chapter Highlights . . . . . 474

15.7 Problems . . . . . 475
15.7.1 Exercises . . . . . 475
15.7.2 Projects . . . . . 476
15.7.3 Answers to "Check Your Understanding" . . 478

**16 Analytic Methods 479**
16.1 $\sum 1/p$ Diverges . . . . . 479
16.2 Bertrand's Postulate . . . . . 485
16.3 Chebyshev's Approximate Prime Number Theorem 493
16.4 Chapter Highlights . . . . . 499
16.5 Problems . . . . . 499
16.5.1 Exercises . . . . . 499
16.5.2 Projects . . . . . 500
16.5.3 Computer Explorations . . . . . 501

**17 Epilogue: Fermat's Last Theorem 503**
17.1 Introduction . . . . . 503
17.2 Elliptic Curves . . . . . 506
17.3 Modularity . . . . . 510

**A Supplementary Topics 513**
A.1 Geometric Series . . . . . 513
A.2 Mathematical Induction . . . . . 515
A.3 Pascal's Triangle and the Binomial Theorem . . . . 521
A.4 Fibonacci Numbers . . . . . 526
A.5 Problems . . . . . 530
A.5.1 Exercises . . . . . 530
A.5.2 Answers to "Check Your Understanding" . . 532

**B Answers and Hints for Odd-Numbered Exercises 535**

**Index 549**