0 1 1 2 3 5 8 13 21 34 55 89 144 233 377
610 987 1597 2584 4181 6765 10946 17711
28657 46368 75025 121393 196418 317811
514229 832040 1346269 2178309 3524578
5702887 9227465 14930352 24157817
39088169 63245986 102334155 165580141
267914296 433494437 SECOND EDITION

BEGINNING NUMBER THEORY

701408733 1134903170 1836311903 2971215073
4807526976 7778742049 12586269025 20365011074
32951280099 53316291173 86267571272
139583862445 225851433717 365435296162
591286729879 956722026041 1548008755920
2504730781961 4052739537881 NEVILLE ROBBINS

Contents

Preface ix
About This Book ix
Features x

Chapter 1 Preliminaries 1
1.1 Introduction 1
1.2 Conjectures, Theorems, and Proofs 4
1.3 Well-Ordering and Induction 8
Well-Ordering Principle 8
1.4 Sigma Notation and Product Notation 16
1.5 Binomial Coefficients 18
1.6 Greatest Integer Function 23
Review Exercises 26

Chapter 2 Divisibility 27
2.1 Introduction 27
2.2 Divisibility, Greatest Common Divisor, Euclid's Algorithm 28
Greatest Common Divisor via Euclid's Algorithm 31
2.3 Least Common Multiple 40
2.4 Representations of Integers 43
Decimal Representations of Integers 43
Binary Representations of Integers 46
Review Exercises 50

Chapter 3 Primes 53
3.1 Introduction 53
3.2 Primes, Prime Counting Function, Prime Number Theorem 54
Test of Primality by Trial Division 56

3.3 Sieve of Eratosthenes, Canonical Factorization, Fundamental Theorem of Arithmetic 61

Sieve of Eratosthenes 61

Determining the Canonical Factorization of a Natural Number 63

Review Exercises 70

Chapter 4 Congruences 71

4.1 Introduction 71

4.2 Congruences and Equivalence Relations 72

Equivalence Relations 73

4.3 Linear Congruences 79

4.4 Linear Diophantine Equations and the Chinese Remainder Theorem 89

4.5 Polynomial Congruences 94

4.6 Modular Arithmetic: Fermat's Theorem 99

4.7 Wilson's Theorem and Fermat Numbers 106

4.8 Pythagorean Equation 111

Review Exercises 116

Chapter 5 Arithmetic Functions 119

5.1 Introduction 119

5.2 Sigma Function, Tau Function, Dirichlet Product 119

5.3 Dirichlet Inverse, Moebius Function, Euler's Function, Euler's Theorem 134

An Application to Algebra 143

Review Exercises 146

Chapter 6 Primitive Roots and Indices 147

6.1 Introduction 147

6.2 Primitive Roots: Definition and Properties 148

6.3 Primitive Roots: Existence 155

6.4 Indices 164

Review Exercises 167

Chapter 7 Quadratic Congruences 169

7.1 Introduction 169

7.2 Quadratic Residues and the Legendre Symbol 170

7.3 Gauss' Lemma and the Law of Quadratic Reciprocity 175

7.4 Solution of Quadratic Congruences 186

Algorithm for Solving Quadratic Congruences 187

7.5 Quadratic Congruences with Composite Moduli 190

7.6 Jacobi Symbol 194

Review Exercises 198

Chapter 8 Sums of Squares 201

8.1 Introduction 201

8.2 Sums of Two Squares 201

8.3 Sums of Four Squares 210

Review Exercises 218

Chapter 9 Continued Fractions 221

9.1 Introduction 221

9.2 Finite Continued Fractions 221

9.3 Infinite Continued Fractions 233

9.4 Approximation by Continued Fractions 239

9.5 Periodic Continued Fractions: I 246

9.6 Periodic Continued Fractions: II 253

Review Exercises 261

Chapter 10 Nonlinear Diophantine Equations 263

10.1 Introduction 263

10.2 Fermat's Last Theorem 262

Pell's Equation: $x_2 - Dy_2 = 1$ 264

Mordell's Equation: $x_3 = y_2 + k$ 276

Review Exercises 278

Chapter 11 Computational Number Theory 279

11.1 Introduction 279

11.2 Pseudoprimes and Carmichael Numbers 283

11.3 Miller's Test and Strong Pseudoprimes 288

11.4 Factoring: Fermat's Method and the Continued Fraction Method 292

Trial Division 292

Fermat's Method 292

Continued Fraction Method 292

11.5 Quadratic Sieve Method 296

11.6 Pollard $p - 1$ Method 299

Review Exercises 301

Chapter 12 Cryptology 303

12.1 Introduction 303

12.2 Character Ciphers 305

12.3 Block Ciphers 308

One-Time Pads: Exponential Ciphers 309

Public-Key Cryptography 311

Signatures 312

Review Exercises 313

Appendix A Some Open Questions in Elementary Number Theory 315

Appendix B Tables 321

Appendix C Answers to Selected Exercises 323

Bibliography 333

Index 335