Contents

Preface ix

Introduction 1

Chapter 1. Integers 5
1. The Integers and the Well Ordering Property 5
2. Divisors and the Division Algorithm 6
3. Greatest Common Divisor and the Euclidean Algorithm 10
4. Prime Numbers and Unique Factorization 20
Exercises 29

Chapter 2. Modular Arithmetic 39
1. Basic Arithmetic 39
2. Inverses and Fermat's Little Theorem 44
3. Linear Congruences and the Chinese Remainder Theorem 51
Exercises 58

Chapter 3. Quadratic Reciprocity and Primitive Roots 65
1. Quadratic Reciprocity 65
2. Computing mth Roots Modulo n 76
3. Existence of Primitive Roots 81
Exercises 86

Chapter 4. Secrets 91
1. Basic Ciphers 92
2. Symmetric Ciphers 95
3. Diffie–Hellman Key Exchange 97
4. Public Key Cryptography (RSA) 98

5. Hash Functions and Check Digits 101
6. Secret Sharing 104
Exercises 105

Chapter 5. Arithmetic Functions 109
1. Euler Totient Function 109
2. Möbius Function 113
3. Functions on Divisors 121
4. Partitions 130
Exercises 134

Chapter 6. Algebraic Numbers 143
1. Algebraic or Transcendental 143
2. Quadratic Number Fields and Norms 145
3. Integers, Divisibility, Primes, and Irreducibles 148
4. Application: Sums of Two Squares 152
Exercises 154

Chapter 7. Rational and Irrational Numbers 157
1. Diophantine Approximation 157
2. Height of a Rational Number 159
3. Heights and Approximations 162
4. Continued Fractions 166
5. Approximating Irrational Numbers with Convergents 171
Exercises 181

Chapter 8. Diophantine Equations 187
1. Introduction and Examples 187
2. Working Modulo Primes 189
3. Pythagorean Triples 198
4. Fermat's Last Theorem 200
5. Pell's Equation and Fundamental Units 202
6. Waring Problem 208
Exercises 213

Chapter 9. Elliptic Curves 221
1. Introduction 221
2. Addition of Points 224
3. Points of Finite Order 229
4. Integer Points and the Nagel–Lutz Theorem 230
5. Mordell–Weil Group and Points of Infinite Order 236
6. Application: Congruent Numbers 237

Exercises 240

Chapter 10. Dynamical Systems 247
1. Discrete Dynamical Systems 247
2. Dynatomic Polynomials 254
3. Resultant and Reduction Modulo Primes 258
4. Periods Modulo Primes 262
5. Algorithms for Rational Periodic and Preperiodic Points 266
Exercises 269

Chapter 11. Polynomials 275
1. Introduction to Polynomials 275
2. Factorization and the Euclidean Algorithm 278
3. Modular Arithmetic for Polynomials 282
4. Diophantine Equations for Polynomials 288
Exercises 294

Bibliography 299

List of Algorithms 303

List of Notation 305

Index 307