Benjamin Fine
Gerhard Rosenberger

Number Theory

An Introduction via the Distribution of Primes

Birkhäuser
Boston • Basel • Berlin

Contents

Preface ... xi

1 **Introduction and Historical Remarks** ... 1

2 **Basic Number Theory** ... 7
- 2.1 The Ring of Integers ... 7
- 2.2 Divisibility, Primes, and Composites ... 11
- 2.3 The Fundamental Theorem of Arithmetic ... 16
- 2.4 Congruences and Modular Arithmetic ... 21
  - 2.4.1 Basic Theory of Congruences ... 22
  - 2.4.2 The Ring of Integers Modulo *n* ... 23
  - 2.4.3 Units and the Euler Phi Function ... 26
  - 2.4.4 Fermat's Little Theorem and the Order of an Element ... 31
  - 2.4.5 On Cyclic Groups ... 34
- 2.5 The Solution of Polynomial Congruences Modulo *m* ... 37
  - 2.5.1 Linear Congruences and the Chinese Remainder Theorem ... 37
  - 2.5.2 Higher-Degree Congruences ... 42
- 2.6 Quadratic Reciprocity ... 45

3 **The Infinitude of Primes** ... 55
- 3.1 The Infinitude of Primes ... 55
  - 3.1.1 Some Direct Proofs and Variations ... 55
  - 3.1.2 Some Analytic Proofs and Variations ... 58
  - 3.1.3 The Fermat and Mersenne Numbers ... 61
  - 3.1.4 The Fibonacci Numbers and the Golden Section ... 65
  - 3.1.5 Some Simple Cases of Dirichlet's Theorem ... 78
  - 3.1.6 A Topological Proof and a Proof Using Codes ... 83
- 3.2 Sums of Squares ... 86
  - 3.2.1 Pythagorean Triples ... 87
  - 3.2.2 Fermat's Two-Square Theorem ... 89
  - 3.2.3 The Modular Group ... 94

3.2.4 Lagrange's Four-Square Theorem 100
3.2.5 The Infinitude of Primes Through Continued Fractions 102
3.3 Dirichlet's Theorem 104
3.4 Twin Prime Conjecture and Related Ideas 121
3.5 Primes Between x and $2x$ 122
3.6 Arithmetic Functions and the Möbius Inversion Formula 123

4 The Density of Primes 133
4.1 The Prime Number Theorem: Estimates and History 133
4.2 Chebychev's Estimate and Some Consequences 136
4.3 Equivalent Formulations of the Prime Number Theorem 149
4.4 The Riemann Zeta Function and the Riemann Hypothesis 157
4.4.1 The Real Zeta Function of Euler 158
4.4.2 Analytic Functions and Analytic Continuation 163
4.4.3 The Riemann Zeta Function 166
4.5 The Prime Number Theorem 173
4.6 The Elementary Proof 180
4.7 Some Extensions and Comments 185

5 Primality Testing: An Overview 197
5.1 Primality Testing and Factorization 197
5.2 Sieving Methods 198
5.2.1 Brun's Sieve and Brun's Theorem 204
5.3 Primality Testing and Prime Records 212
5.3.1 Pseudoprimes and Probabilistic Testing 218
5.3.2 The Lucas–Lehmer Test and Prime Records 225
5.3.3 Some Additional Primality Tests 231
5.4 Cryptography and Primes 234
5.4.1 Some Number-Theoretic Cryptosystems 237
5.4.2 Public Key Cryptography and the RSA Algorithm 240
5.5 The AKS Algorithm 243

6 Primes and Algebraic Number Theory 253
6.1 Algebraic Number Theory 253
6.2 Unique Factorization Domains 255
6.2.1 Euclidean Domains and the Gaussian Integers 261
6.2.2 Principal Ideal Domains 268
6.2.3 Prime and Maximal Ideals 272
6.3 Algebraic Number Fields 275
6.3.1 Algebraic Extensions of $\mathbb{Q}$ 282
6.3.2 Algebraic and Transcendental Numbers 284
6.3.3 Symmetric Polynomials 287
6.3.4 Discriminant and Norm 290
6.4 Algebraic Integers 294
6.4.1 The Ring of Algebraic Integers 296

6.4.2 Integral Bases 297
6.4.3 Quadratic Fields and Quadratic Integers 300
6.4.4 The Transcendence of e and π 303
6.4.5 The Geometry of Numbers: Minkowski Theory 306
6.4.6 Dirichlet's Unit Theorem 308
6.5 The Theory of Ideals 311
6.5.1 Unique Factorization of Ideals 313
6.5.2 An Application of Unique Factorization 319
6.5.3 The Ideal Class Group 321
6.5.4 Norms of Ideals 323
6.5.5 Class Number 326

Bibliography and Cited References 333

Index 337