

Contents

Series Foreword	xi
Preface	xiii
1 Introduction	1
1.1 Number Theory and Complexity	3
1.2 Number Theory and Computation: A Brief History	4
1.3 Condensed History of the Theory of Computation	11
1.4 Notes on Chapter 1	13
2 Fundamentals of Number Theory	19
2.1 Notation, Definitions, and Some Computational Problems	19
2.2 More Definitions	22
2.3 Multiplicative Functions and Möbius Inversion	23
2.4 Notation: Big-O, Little-o, Big-Omega, Big-Theta	25
2.5 Abel's Identity and Euler's Summation Formula	25
2.6 Asymptotic Integration	27
2.7 Estimating Sums over Primes	28
2.8 Basic Concepts of Abstract Algebra	29
2.9 Exercises	34
2.10 Notes on Chapter 2	37
3 A Survey of Complexity Theory	41
3.1 Notation	41
3.2 The Notion of "Step"	41
3.3 Language Classes	44
3.4 Reductions and \mathcal{NP} -Completeness	47
3.5 Randomized Complexity Classes	50
3.6 A Formal Computational Model	52
3.7 Other Resources	55
3.8 Parallel Complexity Classes	57
3.9 Exercises	59
3.10 Notes on Chapter 3	63
4 The Greatest Common Divisor	67
4.1 The Euclidean Algorithm	67
4.2 The Euclidean Algorithm: Worst-Case Analysis	68
4.3 The Extended Euclidean Algorithm	70
4.4 The Euclidean Algorithm and Continuants	73

4.5	Continued Fractions	75
4.6	The Least-Remainder Euclidean Algorithm	79
4.7	The Binary gcd Algorithm	82
4.8	Constructing a gcd-Free Basis	84
4.9	Exercises	90
4.10	Notes on Chapter 4	96
5	Computing in $\mathbb{Z}/(n)$	101
5.1	Basics	101
5.2	Addition, Subtraction, Multiplication	101
5.3	Multiplicative Inverse	102
5.4	The Power Algorithm	102
5.5	The Chinese Remainder Theorem	104
5.6	The Multiplicative Structure of $(\mathbb{Z}/(n))^*$	108
5.7	Quadratic Residues	109
5.8	The Legendre Symbol	110
5.9	The Jacobi Symbol	111
5.10	Exercises	114
5.11	Notes on Chapter 5	120
6	Finite Fields	125
6.1	Basics	125
6.2	The Euclidean Algorithm	127
6.3	Continued Fractions	130
6.4	Computing in $k[X]/(f)$	132
6.5	Galois Theory	133
6.6	The Structure of $k[X]/(f)$	136
6.7	Characters	141
6.8	Exercises	143
6.9	Notes on Chapter 6	148
7	Solving Equations over Finite Fields	155
7.1	Square Roots: Group-Theoretic Methods	155
7.2	Square Roots: Field-Theoretic Methods	157
7.3	Computing d -th Roots	160
7.4	Polynomial Factoring Algorithms	163
7.5	Other Results on Polynomial Factoring	168
7.6	Synthesis of Finite Fields	171

7.7	Hensel's Lemma	173
7.8	Complexity-Theoretic Results	177
7.9	Exercises	188
7.10	Notes on Chapter 7	194
8	Prime Numbers: Facts and Heuristics	203
8.1	Some History	204
8.2	The Density of Primes	206
8.3	Sharp Estimates and the Riemann Hypothesis	211
8.4	Primes in Arithmetic Progressions and the ERH	215
8.5	Applications of the ERH	217
8.6	Other Conjectures about Primes	224
8.7	Extensions to Algebraic Numbers	227
8.8	Some Useful Explicit Estimates	233
8.9	Exercises	236
8.10	Notes on Chapter 8	245
9	Prime Numbers: Basic Algorithms	265
9.1	Primality Proofs and Fermat's Theorem	266
9.2	Primality Tests for Numbers of Special Forms	272
9.3	Pseudoprimes and Carmichael Numbers	275
9.4	Probabilistic Primality Tests	278
9.5	ERH-Based Methods	283
9.6	Primality Testing Using Algebraic Number Theory	285
9.7	Generation of "Random" Primes	293
9.8	Prime Number Sieves	295
9.9	Computing $\pi(x)$ and p_n	299
9.10	Exercises	303
9.11	Notes on Chapter 9	308
A	Solutions to Exercises	319
	Bibliography	389
	Index to Notation	487
	Index	489