

# Contents

<b>Preface</b>	<b>vii</b>
<b>1 PRIMES!</b>	<b>1</b>
1.1 Problems and progress . . . . .	1
1.1.1 Fundamental theorem and fundamental problem . . . . .	1
1.1.2 Technological and algorithmic progress . . . . .	2
1.1.3 The infinitude of primes . . . . .	6
1.1.4 Asymptotic relations and order nomenclature . . . . .	8
1.1.5 How primes are distributed . . . . .	10
1.2 Celebrated conjectures and curiosities . . . . .	14
1.2.1 Twin primes . . . . .	14
1.2.2 Prime $k$ -tuples and hypothesis H . . . . .	17
1.2.3 The Goldbach conjecture . . . . .	18
1.2.4 The convexity question . . . . .	20
1.2.5 Prime-producing formulae . . . . .	21
1.3 Primes of special form . . . . .	22
1.3.1 Mersenne primes . . . . .	22
1.3.2 Fermat numbers . . . . .	27
1.3.3 Certain presumably rare primes . . . . .	31
1.4 Analytic number theory . . . . .	33
1.4.1 The Riemann zeta function . . . . .	33
1.4.2 Computational successes . . . . .	38
1.4.3 Dirichlet $L$ -functions . . . . .	39
1.4.4 Exponential sums . . . . .	43
1.4.5 Smooth numbers . . . . .	48
1.5 Exercises . . . . .	49
1.6 Research problems . . . . .	75
<b>2 NUMBER-THEORETICAL TOOLS</b>	<b>83</b>
2.1 Modular arithmetic . . . . .	83
2.1.1 Greatest common divisor and inverse . . . . .	83
2.1.2 Powers . . . . .	85
2.1.3 Chinese remainder theorem . . . . .	87
2.2 Polynomial arithmetic . . . . .	89
2.2.1 Greatest common divisor for polynomials . . . . .	89
2.2.2 Finite fields . . . . .	91
2.3 Squares and roots . . . . .	96

2.3.1	Quadratic residues . . . . .	96
2.3.2	Square roots . . . . .	99
2.3.3	Finding polynomial roots . . . . .	103
2.3.4	Representation by quadratic forms . . . . .	106
2.4	Exercises . . . . .	108
2.5	Research problems . . . . .	113
<b>3</b>	<b>RECOGNIZING PRIMES AND COMPOSITES</b>	<b>117</b>
3.1	Trial division . . . . .	117
3.1.1	Divisibility tests . . . . .	117
3.1.2	Trial division . . . . .	118
3.1.3	Practical considerations . . . . .	119
3.1.4	Theoretical considerations . . . . .	120
3.2	Sieving . . . . .	121
3.2.1	Sieving to recognize primes . . . . .	121
3.2.2	Eratosthenes pseudocode . . . . .	122
3.2.3	Sieving to construct a factor table . . . . .	122
3.2.4	Sieving to construct complete factorizations . . . . .	123
3.2.5	Sieving to recognize smooth numbers . . . . .	123
3.2.6	Sieving a polynomial . . . . .	124
3.2.7	Theoretical considerations . . . . .	126
3.3	Recognizing smooth numbers . . . . .	128
3.4	Pseudoprimes . . . . .	131
3.4.1	Fermat pseudoprimes . . . . .	131
3.4.2	Carmichael numbers . . . . .	133
3.5	Probable primes and witnesses . . . . .	135
3.5.1	The least witness for $n$ . . . . .	140
3.6	Lucas pseudoprimes . . . . .	142
3.6.1	Fibonacci and Lucas pseudoprimes . . . . .	142
3.6.2	Grantham's Frobenius test . . . . .	145
3.6.3	Implementing the Lucas and quadratic Frobenius tests . . . . .	146
3.6.4	Theoretical considerations and stronger tests . . . . .	149
3.6.5	The general Frobenius test . . . . .	151
3.7	Counting primes . . . . .	152
3.7.1	Combinatorial method . . . . .	152
3.7.2	Analytic method . . . . .	158
3.8	Exercises . . . . .	162
3.9	Research problems . . . . .	168
<b>4</b>	<b>PRIMALITY PROVING</b>	<b>173</b>
4.1	The $n - 1$ test . . . . .	173
4.1.1	The Lucas theorem and Pepin test . . . . .	173
4.1.2	Partial factorization . . . . .	174
4.1.3	Succinct certificates . . . . .	179
4.2	The $n + 1$ test . . . . .	181
4.2.1	The Lucas–Lehmer test . . . . .	181

4.2.2	An improved $n + 1$ test, and a combined $n^2 - 1$ test . . .	184
4.2.3	Divisors in residue classes . . . . .	186
4.3	The finite field primality test . . . . .	190
4.4	Gauss and Jacobi sums . . . . .	194
4.4.1	Gauss sums test . . . . .	194
4.4.2	Jacobi sums test . . . . .	199
4.5	The primality test of Agrawal, Kayal, and Saxena (AKS test) .	200
4.5.1	Primality testing with roots of unity . . . . .	201
4.5.2	The complexity of Algorithm 4.5.1 . . . . .	205
4.5.3	Primality testing with Gaussian periods . . . . .	207
4.5.4	A quartic time primality test . . . . .	213
4.6	Exercises . . . . .	217
4.7	Research problems . . . . .	222
<b>5</b>	<b>EXPONENTIAL FACTORING ALGORITHMS</b>	<b>225</b>
5.1	Squares . . . . .	225
5.1.1	Fermat method . . . . .	225
5.1.2	Lehman method . . . . .	227
5.1.3	Factor sieves . . . . .	228
5.2	Monte Carlo methods . . . . .	229
5.2.1	Pollard rho method for factoring . . . . .	229
5.2.2	Pollard rho method for discrete logarithms . . . . .	232
5.2.3	Pollard lambda method for discrete logarithms . . . . .	233
5.3	Baby-steps, giant-steps . . . . .	235
5.4	Pollard $p - 1$ method . . . . .	236
5.5	Polynomial evaluation method . . . . .	238
5.6	Binary quadratic forms . . . . .	239
5.6.1	Quadratic form fundamentals . . . . .	239
5.6.2	Factoring with quadratic form representations . . . . .	242
5.6.3	Composition and the class group . . . . .	245
5.6.4	Ambiguous forms and factorization . . . . .	248
5.7	Exercises . . . . .	251
5.8	Research problems . . . . .	255
<b>6</b>	<b>SUBEXPONENTIAL FACTORING ALGORITHMS</b>	<b>261</b>
6.1	The quadratic sieve factorization method . . . . .	261
6.1.1	Basic QS . . . . .	261
6.1.2	Basic QS: A summary . . . . .	266
6.1.3	Fast matrix methods . . . . .	268
6.1.4	Large prime variations . . . . .	270
6.1.5	Multiple polynomials . . . . .	273
6.1.6	Self initialization . . . . .	274
6.1.7	Zhang's special quadratic sieve . . . . .	276
6.2	Number field sieve . . . . .	278
6.2.1	Basic NFS: Strategy . . . . .	279
6.2.2	Basic NFS: Exponent vectors . . . . .	280

6.2.3	Basic NFS: Complexity . . . . .	285
6.2.4	Basic NFS: Obstructions . . . . .	288
6.2.5	Basic NFS: Square roots . . . . .	291
6.2.6	Basic NFS: Summary algorithm . . . . .	292
6.2.7	NFS: Further considerations . . . . .	294
6.3	Rigorous factoring . . . . .	301
6.4	Index-calculus method for discrete logarithms . . . . .	302
6.4.1	Discrete logarithms in prime finite fields . . . . .	303
6.4.2	Discrete logarithms via smooth polynomials and smooth algebraic integers . . . . .	305
6.5	Exercises . . . . .	306
6.6	Research problems . . . . .	315
<b>7</b>	<b>ELLIPTIC CURVE ARITHMETIC</b>	<b>319</b>
7.1	Elliptic curve fundamentals . . . . .	319
7.2	Elliptic arithmetic . . . . .	323
7.3	The theorems of Hasse, Deuring, and Lenstra . . . . .	333
7.4	Elliptic curve method . . . . .	335
7.4.1	Basic ECM algorithm . . . . .	336
7.4.2	Optimization of ECM . . . . .	339
7.5	Counting points on elliptic curves . . . . .	347
7.5.1	Shanks–Mestre method . . . . .	347
7.5.2	Schoof method . . . . .	351
7.5.3	Atkin–Morain method . . . . .	358
7.6	Elliptic curve primality proving (ECP) . . . . .	368
7.6.1	Goldwasser–Kilian primality test . . . . .	368
7.6.2	Atkin–Morain primality test . . . . .	371
7.6.3	Fast primality-proving via elliptic curves (fastECP) . . . . .	373
7.7	Exercises . . . . .	374
7.8	Research problems . . . . .	380
<b>8</b>	<b>THE UBIQUITY OF PRIME NUMBERS</b>	<b>387</b>
8.1	Cryptography . . . . .	387
8.1.1	Diffie–Hellman key exchange . . . . .	387
8.1.2	RSA cryptosystem . . . . .	389
8.1.3	Elliptic curve cryptosystems (ECCs) . . . . .	391
8.1.4	Coin-flip protocol . . . . .	396
8.2	Random-number generation . . . . .	397
8.2.1	Modular methods . . . . .	398
8.3	Quasi-Monte Carlo (qMC) methods . . . . .	404
8.3.1	Discrepancy theory . . . . .	404
8.3.2	Specific qMC sequences . . . . .	407
8.3.3	Primes on Wall Street? . . . . .	409
8.4	Diophantine analysis . . . . .	415
8.5	Quantum computation . . . . .	418
8.5.1	Intuition on quantum Turing machines (QTMs) . . . . .	419

8.5.2	The Shor quantum algorithm for factoring . . . . .	422
8.6	Curious, anecdotal, and interdisciplinary references to primes . . . . .	424
8.7	Exercises . . . . .	431
8.8	Research problems . . . . .	436
<b>9</b>	<b>FAST ALGORITHMS FOR LARGE-INTEGER ARITHMETIC</b>	<b>443</b>
9.1	Tour of “grammar-school” methods . . . . .	443
9.1.1	Multiplication . . . . .	443
9.1.2	Squaring . . . . .	444
9.1.3	Div and mod . . . . .	445
9.2	Enhancements to modular arithmetic . . . . .	447
9.2.1	Montgomery method . . . . .	447
9.2.2	Newton methods . . . . .	450
9.2.3	Moduli of special form . . . . .	454
9.3	Exponentiation . . . . .	457
9.3.1	Basic binary ladders . . . . .	458
9.3.2	Enhancements to ladders . . . . .	460
9.4	Enhancements for gcd and inverse . . . . .	463
9.4.1	Binary gcd algorithms . . . . .	463
9.4.2	Special inversion algorithms . . . . .	465
9.4.3	Recursive-gcd schemes for very large operands . . . . .	466
9.5	Large-integer multiplication . . . . .	473
9.5.1	Karatsuba and Toom–Cook methods . . . . .	473
9.5.2	Fourier transform algorithms . . . . .	476
9.5.3	Convolution theory . . . . .	488
9.5.4	Discrete weighted transform (DWT) methods . . . . .	493
9.5.5	Number-theoretical transform methods . . . . .	498
9.5.6	Schönhage method . . . . .	502
9.5.7	Nussbaumer method . . . . .	503
9.5.8	Complexity of multiplication algorithms . . . . .	506
9.5.9	Application to the Chinese remainder theorem . . . . .	508
9.6	Polynomial arithmetic . . . . .	509
9.6.1	Polynomial multiplication . . . . .	510
9.6.2	Fast polynomial inversion and remaindering . . . . .	511
9.6.3	Polynomial evaluation . . . . .	514
9.7	Exercises . . . . .	518
9.8	Research problems . . . . .	535
	<b>Appendix: BOOK PSEUDOCODE</b>	<b>541</b>
	<b>References</b>	<b>547</b>
	<b>Index</b>	<b>577</b>



<http://www.springer.com/978-0-387-25282-7>

Prime Numbers

A Computational Perspective

Crandall, R.; Pomerance, C.

2005, XV, 597 p., Hardcover

ISBN: 978-0-387-25282-7