

Table of Contents

1. Elementary Number Theory	1
1.1 Introduction	1
1.1.1 What is Number Theory?	1
1.1.2 Applications of Number Theory	13
1.1.3 Algebraic Preliminaries	14
1.2 Theory of Divisibility	21
1.2.1 Basic Concepts and Properties of Divisibility	21
1.2.2 Fundamental Theorem of Arithmetic	27
1.2.3 Mersenne Primes and Fermat Numbers	33
1.2.4 Euclid's Algorithm	40
1.2.5 Continued Fractions	44
1.3 Diophantine Equations	52
1.3.1 Basic Concepts of Diophantine Equations	52
1.3.2 Linear Diophantine Equations	54
1.3.3 Pell's Equations	57
1.4 Arithmetic Functions	63
1.4.1 Multiplicative Functions	63
1.4.2 Functions $\tau(n)$, $\sigma(n)$ and $s(n)$	66
1.4.3 Perfect, Amicable and Sociable Numbers	71
1.4.4 Functions $\phi(n)$, $\lambda(n)$ and $\mu(n)$	79
1.5 Distribution of Prime Numbers	85
1.5.1 Prime Distribution Function $\pi(x)$	85
1.5.2 Approximations of $\pi(x)$ by $x/\ln x$	87
1.5.3 Approximations of $\pi(x)$ by $\text{Li}(x)$	94
1.5.4 The Riemann ζ -Function $\zeta(s)$	95
1.5.5 The n th Prime	104
1.5.6 Distribution of Twin Primes	106
1.5.7 The Arithmetic Progression of Primes	110
1.6 Theory of Congruences	111
1.6.1 Basic Concepts and Properties of Congruences	111
1.6.2 Modular Arithmetic	118
1.6.3 Linear Congruences	123
1.6.4 The Chinese Remainder Theorem	130
1.6.5 High-Order Congruences	133

1.6.6	Legendre and Jacobi Symbols	139
1.6.7	Orders and Primitive Roots	150
1.6.8	Indices and k th Power Residues	155
1.7	Arithmetic of Elliptic Curves	160
1.7.1	Basic Concepts of Elliptic Curves	160
1.7.2	Geometric Composition Laws of Elliptic Curves	163
1.7.3	Algebraic Computation Laws for Elliptic Curves	164
1.7.4	Group Laws on Elliptic Curves	168
1.7.5	Number of Points on Elliptic Curves	169
1.8	Bibliographic Notes and Further Reading	171
2.	Computational/Algorithmic Number Theory	173
2.1	Introduction	173
2.1.1	What is Computational/Algorithmic Number Theory?	174
2.1.2	Effective Computability	177
2.1.3	Computational Complexity	181
2.1.4	Complexity of Number-Theoretic Algorithms	188
2.1.5	Fast Modular Exponentiations	194
2.1.6	Fast Group Operations on Elliptic Curves	198
2.2	Algorithms for Primality Testing	202
2.2.1	Deterministic and Rigorous Primality Tests	202
2.2.2	Fermat's Pseudoprimality Test	206
2.2.3	Strong Pseudoprimality Test	208
2.2.4	Lucas Pseudoprimality Test	215
2.2.5	Elliptic Curve Test	222
2.2.6	Historical Notes on Primality Testing	225
2.3	Algorithms for Integer Factorization	228
2.3.1	Complexity of Integer Factorization	228
2.3.2	Trial Division and Fermat Method	232
2.3.3	Legendre's Congruence	234
2.3.4	Continued FRACtion Method (CFRAC)	237
2.3.5	Quadratic and Number Field Sieves (QS/NFS)	240
2.3.6	Pollard's " ρ " and " $p-1$ " Methods	244
2.3.7	Lenstra's Elliptic Curve Method (ECM)	251
2.4	Algorithms for Discrete Logarithms	254
2.4.1	Shanks' Baby-Step Giant-Step Algorithm	255
2.4.2	Silver-Pohlig-Hellman Algorithm	258
2.4.3	Index Calculus for Discrete Logarithms	262
2.4.4	Algorithms for Elliptic Curve Discrete Logarithms	266
2.4.5	Algorithm for Root Finding Problem	270
2.5	Quantum Number-Theoretic Algorithms	273
2.5.1	Quantum Information and Computation	273
2.5.2	Quantum Computability and Complexity	278
2.5.3	Quantum Algorithm for Integer Factorization	279
2.5.4	Quantum Algorithms for Discrete Logarithms	285

2.6	Miscellaneous Algorithms in Number Theory	287
2.6.1	Algorithms for Computing $\pi(x)$	287
2.6.2	Algorithms for Generating Amicable Pairs	292
2.6.3	Algorithms for Verifying Goldbach's Conjecture	295
2.6.4	Algorithm for Finding Odd Perfect Numbers	299
2.7	Bibliographic Notes and Further Reading	300
3.	Applied Number Theory in Computing/Cryptography . . .	303
3.1	Why Applied Number Theory?	303
3.2	Computer Systems Design	305
3.2.1	Representing Numbers in Residue Number Systems	305
3.2.2	Fast Computations in Residue Number Systems	308
3.2.3	Residue Computers	312
3.2.4	Complementary Arithmetic	315
3.2.5	Hash Functions	317
3.2.6	Error Detection and Correction Methods	321
3.2.7	Random Number Generation	326
3.3	Cryptography and Information Security	332
3.3.1	Introduction	332
3.3.2	Secret-Key Cryptography	333
3.3.3	Data/Advanced Encryption Standard (DES/AES)	344
3.3.4	Public-Key Cryptography	348
3.3.5	Discrete Logarithm Based Cryptosystems	354
3.3.6	RSA Public-Key Cryptosystem	358
3.3.7	Quadratic Residuosity Cryptosystems	373
3.3.8	Elliptic Curve Public-Key Cryptosystems	379
3.3.9	Digital Signatures	385
3.3.10	Digital Signature Standard (DSS)	392
3.3.11	Database Security	395
3.3.12	Secret Sharing	399
3.3.13	Internet/Web Security and Electronic Commerce	403
3.3.14	Steganography	409
3.3.15	Quantum Cryptography	410
3.4	Bibliographic Notes and Further Reading	411
	Bibliography	415
	Index	429



<http://www.springer.com/978-3-540-43072-8>

Number Theory for Computing

Yan, S.Y.

2002, XXII, 435 p., Hardcover

ISBN: 978-3-540-43072-8