

Contents

Preface to the English Edition	ix
Preface	xi
Notation	xiii
Chapter 1. Primality Testing and Construction of Large Primes	1
1.1. Introduction	1
1.2. Elementary methods of primality testing	1
1.3. Primality tests for numbers of a special form	3
1.4. $(N \pm 1)$ -methods for primality testing, and construction of large primes	8
1.5. The Konyagin-Pomerance algorithm	13
1.6. Miller's algorithm	15
1.7. Probabilistic primality tests	19
1.8. Modern methods for primality testing	23
1.9. Summary. A deterministic polynomial algorithm for primality testing	27
Chapter 2. Factorization of Integers with Exponential Complexity	35
2.1. Introduction. Fermat's method	35
2.2. Pollard's $(P - 1)$ -method	37
2.3. Pollard's ρ -method	39
2.4. The Sherman-Lehman method	40
2.5. Lenstra's algorithm	42
2.6. The Pollard-Strassen algorithm	47
2.7. Williams' $(P + 1)$ -method and its generalizations	48
2.8. Shanks' methods	48
2.9. Other methods. Summary	49
Chapter 3. Factorization of Integers with Subexponential Complexity	51
3.1. Introduction	51
3.2. Dixon's method. Additional strategies	52
3.3. The Brillhart-Morrison algorithm	55
3.4. Quadratic sieve	58
3.5. The methods of Schnorr-Lenstra and Lenstra-Pomerance	61
3.6. Number field sieves	62
3.7. Summary	71
Chapter 4. Application of Elliptic Curves to Primality Testing and Factorization of Integers	73
4.1. Introduction. Elliptic curves and their properties	73

4.2.	Lenstra's algorithm for factorization of integers using elliptic curves	75
4.3.	Computing the order of the group of points of an elliptic curve over a finite field	78
4.4.	Primality testing using elliptic curves	84
4.5.	Summary	87
Chapter 5.	Algorithms for Computing Discrete Logarithm	91
5.1.	Introduction. Deterministic methods	91
5.2.	Pollard's ρ -method for the discrete logarithm problem	93
5.3.	The discrete logarithm problem in prime fields	93
5.4.	Discrete logarithm in Galois fields	96
5.5.	Discrete logarithm and the number field sieve	99
5.6.	Fermat quotient and discrete logarithm with composite modulus	102
5.7.	Summary	113
Chapter 6.	Factorization of Polynomials over Finite Fields	115
6.1.	Introduction. A probabilistic algorithm for solving algebraic equations in finite fields	115
6.2.	Solving quadratic equations	118
6.3.	The Berlekamp algorithm	121
6.4.	The Cantor-Zassenhaus method	125
6.5.	Some other improvements of the Berlekamp algorithm	127
6.6.	A probabilistic algorithm for irreducibility testing of polynomials over finite fields	129
6.7.	Summary	131
Chapter 7.	Reduced Lattice Bases and Their Applications	135
7.1.	Introduction. Lattices and bases	135
7.2.	LLL-reduced bases and their properties	136
7.3.	An algorithm for constructing an LLL-reduced lattice basis	138
7.4.	The Schnorr-Euchner algorithm and an integral LLL algorithm	140
7.5.	Some applications of the LLL algorithm	143
7.6.	The Ferguson-Forcade algorithm	147
7.7.	Summary	156
Chapter 8.	Factorization of Polynomials over the Field of Rational Numbers with Polynomial Complexity	159
8.1.	Introduction	159
8.2.	The LLL factorization algorithm: Factorization modulo a prime	160
8.3.	The LLL factorization algorithm: Using lattices	161
8.4.	The LLL factorization algorithm: Lifting the factorization	165
8.5.	The LLL factorization algorithm: A complete description	167
8.6.	A usable factorization algorithm	168
8.7.	Factorization of polynomials using approximations	169
8.8.	Summary	174
Chapter 9.	Discrete Fourier Transform and Its Applications	175
9.1.	Introduction. Discrete Fourier transform and its properties	175
9.2.	Computing the discrete Fourier transform	176
9.3.	Discrete Fourier transform and multiplication of polynomials	177

9.4. Discrete Fourier transform and polynomial division	181
9.5. Applying the discrete Fourier transform to the Pollard-Strassen algorithm	183
9.6. Summary	185
Chapter 10. High-Precision Integer Arithmetic	187
10.1. Introduction. Addition and multiplication	187
10.2. Multiplication	188
10.3. Division	191
10.4. Some algorithms of modular arithmetic	198
Chapter 11. Solving Systems of Linear Equations over Finite Fields	203
11.1. Introduction	203
11.2. Solving linear systems in integers	204
11.3. Gaussian and structured Gaussian elimination	207
11.4. The Lanczos algorithm	208
11.5. The Wiedemann algorithm	211
11.6. Other methods. Summary	214
Appendix. Facts from Number Theory	215
Bibliography	223
References added in the English edition	233
Index	241