Translations of

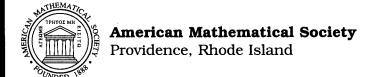
MATHEMATICAL MONOGRAPHS

Volume 232

Number-Theoretic Algorithms in Cryptography

O. N. Vasilenko

Translated by Alex Martsinkovsky



Contents

Preface	to the English Edition	ix
Preface	•	xi
Notation	n	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		
	Factorization of Integers	73
4.1.	Introduction, Elliptic curves and their properties	73

vi CONTENTS

A.4. Primality testing using elliptic curves 4.5. Summary Chapter 5. Algorithms for Computing Discrete Logarithm 5.1. Introduction. Deterministic methods 5.2. Pollard's \(\rho\) method for the discrete logarithm problem 5.3. The discrete logarithm problem in prime fields 5.4. Discrete logarithm in Galois fields 5.5. Discrete logarithm and the number field sieve 99 5.6. Fermat quotient and discrete logarithm with composite modulus 102 5.7. Summary Chapter 6. Factorization of Polynomials over Finite Fields 6.1. Introduction. A probabilistic algorithm for solving algebraic equations in finite fields 6.2. Solving quadratic equations 6.3. The Berlekamp algorithm 121 6.4. The Cantor-Zassenhaus method 6.5. Some other improvements of the Berlekamp algorithm 127 6.6. A probabilistic algorithm for irreducibility testing of polynomials over finite fields 6.7. Summary Chapter 7. Reduced Lattice Bases and Their Applications 7.1. Introduction. Lattices and bases 7.2. LLL-reduced bases and their properties 7.3. An algorithm for constructing an LLL-reduced lattice basis 7.4. The Schnorr-Euchner algorithm and an integral LLL algorithm 7.5. Some applications of the LLL algorithm 7.6. The Ferguson-Forcade algorithm 7.7. Summary Chapter 8. Factorization of Polynomials over the Field of Rational Numbers with Polynomial Complexity 8.1. Introduction 8.2. The LLL factorization algorithm: Factorization modulo a prime 8.3. The LLL factorization algorithm: Pactorization modulo a prime 8.4. The LLL factorization algorithm: Lifting the factorization 8.5. The LLL factorization algorithm: A complete description 8.6. A usable factorization algorithm: A complete description 8.7. Factorization of polynomials using approximations 8.8. Summary Chapter 9. Discrete Fourier Transform and Its Applications 9.1. Introduction. Discrete Fourier transform and its properties 9.2. Computing the discrete Fourier transform of polynomials 176 9.3. Discrete Fourier Transform and multiplication of polynomials	4.2. 4.3.	Lenstra's algorithm for factorization of integers using elliptic curves Computing the order of the group of points of an elliptic curve over a	75 70
4.5. Summary Chapter 5. Algorithms for Computing Discrete Logarithm 5.1. Introduction. Deterministic methods 5.2. Pollard's p-method for the discrete logarithm problem 5.3. The discrete logarithm problem in prime fields 5.4. Discrete logarithm in Galois fields 5.5. Discrete logarithm and the number field sieve 5.6. Fermat quotient and discrete logarithm with composite modulus 5.7. Summary Chapter 6. Factorization of Polynomials over Finite Fields 6.1. Introduction. A probabilistic algorithm for solving algebraic equations in finite fields 6.2. Solving quadratic equations 6.3. The Berlekamp algorithm 6.4. The Cantor-Zassenhaus method 6.5. Some other improvements of the Berlekamp algorithm 6.6. A probabilistic algorithm for irreducibility testing of polynomials over finite fields 6.7. Summary 131 Chapter 7. Reduced Lattice Bases and Their Applications 7.1. Introduction. Lattices and bases 7.2. LLL-reduced bases and their properties 7.3. An algorithm for constructing an LLL-reduced lattice basis 7.4. The Schnorr-Euchner algorithm and an integral LLL algorithm 7.5. Some applications of the LLL algorithm 7.6. The Ferguson-Forcade algorithm and an integral LLL algorithm 7.7. Summary Chapter 8. Factorization of Polynomials over the Field of Rational Numbers with Polynomial Complexity 8.1. Introduction 8.2. The LLL factorization algorithm: Factorization modulo a prime 8.3. The LLL factorization algorithm: Lifting the factorization 8.4. The LLL factorization algorithm: Lifting the factorization 8.5. The LLL factorization algorithm: Lifting the factorization 8.6. A usable factorization algorithm: Lifting the factorization 8.7. Factorization of polynomials using approximations 109 8.8. Summary 100 101 102 103 104 105 105 106 107 108 109 109 109 109 109 109 109	4.4	finite field	78
Chapter 5. Algorithms for Computing Discrete Logarithm 5.1. Introduction. Deterministic methods 5.2. Pollard's \$\rho\$-method for the discrete logarithm problem 5.3. The discrete logarithm problem in prime fields 5.4. Discrete logarithm in Galois fields 5.5. Discrete logarithm and the number field sieve 99 5.6. Fermat quotient and discrete logarithm with composite modulus 5.7. Summary 113 Chapter 6. Pactorization of Polynomials over Finite Fields 6.1. Introduction. A probabilistic algorithm for solving algebraic equations in finite fields 6.2. Solving quadratic equations 6.3. The Berlekamp algorithm 6.4. The Cantor-Zassenhaus method 6.5. Some other improvements of the Berlekamp algorithm 6.6. A probabilistic algorithm for irreducibility testing of polynomials over finite fields 6.7. Summary 131 Chapter 7. Reduced Lattice Bases and Their Applications 7.1. Introduction. Lattices and bases 7.2. LLL-reduced bases and their properties 7.3. An algorithm for constructing an LLL-reduced lattice basis 7.4. The Schnorr-Euchner algorithm and an integral LLL algorithm 7.5. Some applications of the LLL algorithm 7.6. The Ferguson-Forcade algorithm 7.7. Summary 136 Chapter 8. Factorization of Polynomials over the Field of Rational Numbers with Polynomial Complexity 8.1. Introduction 8.2. The LLL factorization algorithm: Factorization modulo a prime 8.3. The LLL factorization algorithm: Using lattices 8.4. The LLL factorization algorithm: Lifting the factorization 8.5. The LLL factorization algorithm: Lifting the factorization 8.6. A usable factorization algorithm: Lifting the factorization 8.7. Factorization of polynomials using approximations 109 8.8. Summary 174 Chapter 9. Discrete Fourier Transform and its properties 9.1. Introduction. Discrete Fourier transform and its properties 9.2. Computing the discrete Fourier transform			
5.1. Introduction. Deterministic methods 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 136 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 141 7.6. The Ferguson-Forcade algorithm 142 7.7. Summary 156 Chapter 8. Factorization of Polynomials over the Field of Rational Numbers with Polynomial Complexity 159 8.1. Introduction 8.2. The LLL factorization algorithm: Factorization modulo a prime 160 8.3. The LLL factorization algorithm: Factorization modulo a prime 161 8.4. The LLL factorization algorithm: Lifting the factorization 162 8.5. The LLL factorization algorithm: Lifting the factorization 163 8.6. A usable factorization algorithm: Lifting the factorization 164 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 176 Chapter 9. Discrete Fourier Transform and Its Applications 175 9.1. Introduction. Discrete Fourier transform	4.0.	Summary	01
5.2. Pollard's ρ-method for the discrete logarithm problem 5.3. The discrete logarithm problem in prime fields 5.4. Discrete logarithm in Galois fields 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 6.1. Introduction. A probabilistic algorithm for solving algebraic equations in finite fields 6.2. Solving quadratic equations 6.3. The Berlekamp algorithm 6.4. The Cantor-Zassenhaus method 6.5. Some other improvements of the Berlekamp algorithm 6.6. A probabilistic algorithm for irreducibility testing of polynomials over finite fields 6.7. Summary 131 Chapter 7. Reduced Lattice Bases and Their Applications 135 7.1. Introduction. Lattices and bases 136 7.2. LLL-reduced bases and their properties 136 7.3. An algorithm for constructing an LLL-reduced lattice basis 7.4. The Schnorr-Euchner algorithm and an integral LLL algorithm 140 7.5. Some applications of the LLL algorithm 141 7.6. The Ferguson-Forcade algorithm and an integral LLL algorithm 142 7.7. Summary 156 Chapter 8. Factorization of Polynomials over the Field of Rational Numbers with Polynomial Complexity 159 8.1. Introduction 8.2. The LLL factorization algorithm: Factorization modulo a prime 160 8.3. The LLL factorization algorithm: Factorization modulo a prime 161 8.4. The LLL factorization algorithm: Lifting the factorization 162 8.5. The LLL factorization algorithm: Lifting the factorization 163 8.6. A usable factorization algorithm: Lifting the factorization 164 8.7. Factorization of polynomials using approximations 165 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	Chapter	5. Algorithms for Computing Discrete Logarithm	91
5.3. The discrete logarithm problem in prime fields 5.4. Discrete logarithm in Galois fields 5.5. Discrete logarithm and the number field sieve 5.6. Fermat quotient and discrete logarithm with composite modulus 102 5.7. Summary 113 Chapter 6. Factorization of Polynomials over Finite Fields 6.1. Introduction. A probabilistic algorithm for solving algebraic equations in finite fields 6.2. Solving quadratic equations 118 6.3. The Berlekamp algorithm 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 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 141 7.6. The Ferguson-Forcade algorithm and an integral LLL algorithm 140 7.5. Summary 150 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: Factorization modulo a prime 180 8.4. The LLL factorization algorithm: Factorization modulo a prime 181 8.5. The LLL factorization algorithm: Using lattices 182 8.6. A usable factorization algorithm: Lifting the factorization 185 8.7. Factorization of polynomials using approximations 186 8.8. Summary 174 Chapter 9. Discrete Fourier Transform and its properties 175 9.1. Introduction. Discrete Fourier transform and its properties 175 9.2. Computing the discrete Fourier transform 176	5.1.	Introduction. Deterministic methods	
5.4. Discrete logarithm in Galois fields 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 136 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 147 7.6. The Ferguson-Forcade algorithm and an integral LLL algorithm 140 7.5. 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: Factorization modulo a prime 161 8.4. The LLL factorization algorithm: Lifting the factorization 162 8.5. The LLL factorization algorithm: A complete description 167 8.6. A usable factorization algorithm: A complete description 167 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 and its properties 175	5.2.	,	
5.5. Discrete logarithm and the number field sieve 5.6. Fermat quotient and discrete logarithm with composite modulus 5.7. Summary 113 Chapter 6. Factorization of Polynomials over Finite Fields 6.1. Introduction. A probabilistic algorithm for solving algebraic equations in finite fields 6.2. Solving quadratic equations 6.3. The Berlekamp algorithm 6.4. The Cantor-Zassenhaus method 6.5. Some other improvements of the Berlekamp algorithm 6.6. A probabilistic algorithm for irreducibility testing of polynomials over finite fields 6.7. Summary 131 Chapter 7. Reduced Lattice Bases and Their Applications 125 126 127 128 129 130 Chapter 7. Reduced Lattice Bases and Their Applications 135 136 137 13. Introduction. Lattices and bases 136 137 13. Introduction. Lattices and bases 138 139 140 150 150 150 150 150 150 150 150 150 15			
5.6. Fermat quotient and discrete logarithm with composite modulus 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 147 7.7. Summary 156 Chapter 8. Factorization of Polynomials over the Field of Rational Numbers with Polynomial Complexity 159 8.1. Introduction 8.2. The LLL factorization algorithm: Factorization modulo a prime 8.3. The LLL factorization algorithm: Lifting the factorization 161 8.4. The LLL factorization algorithm: Lifting the factorization 162 8.5. The LLL factorization algorithm: Lifting the factorization 163 8.6. A usable factorization algorithm: A complete description 164 8.7. Factorization of polynomials using approximations 165 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 and its properties			
Chapter 6. Factorization of Polynomials over Finite Fields 6.1. Introduction. A probabilistic algorithm for solving algebraic equations in finite fields 6.2. Solving quadratic equations 6.3. The Berlekamp algorithm 6.4. The Cantor-Zassenhaus method 6.5. Some other improvements of the Berlekamp algorithm 6.6. A probabilistic algorithm for irreducibility testing of polynomials over finite fields 6.7. Summary 6.8. A probabilistic algorithm for irreducibility testing of polynomials over finite fields 6.9. Summary 6.10. The Reduced Lattice Bases and Their Applications 6.11. Introduction. Lattices and bases 6.12. LLL-reduced bases and their properties 6.13. An algorithm for constructing an LLL-reduced lattice basis 6.13. The Schnorr-Euchner algorithm and an integral LLL algorithm 6.14. The Schnorr-Euchner algorithm and an integral LLL algorithm 6.15. Some applications of the LLL algorithm 6.16. The Ferguson-Forcade algorithm 6.17. Summary 7.18. Introduction 7.19. Summary 7.10. Introduction of Polynomials over the Field of Rational Numbers with Polynomial Complexity 7.19. The LLL factorization algorithm: Factorization modulo a prime 7.19. The LLL factorization algorithm: Lifting the factorization 7.19. The LLL factorization algorithm: Lifting the factorization 7.19. The LLL factorization algorithm: Lifting the factorization 7. Summary 7. Chapter 7. Pactorization of polynomials using approximations 7. Introduction. Discrete Fourier transform and its properties		S .	
Chapter 6. Factorization of Polynomials over Finite Fields 6.1. Introduction. A probabilistic algorithm for solving algebraic equations in finite fields 6.2. Solving quadratic equations 6.3. The Berlekamp algorithm 6.4. The Cantor-Zassenhaus method 6.5. Some other improvements of the Berlekamp algorithm 6.6. A probabilistic algorithm for irreducibility testing of polynomials over finite fields 6.7. Summary 6.8. Summary 6.9. LLL-reduced Lattice Bases and Their Applications 7.1. Introduction. Lattices and bases 7.2. LLL-reduced bases and their properties 7.3. An algorithm for constructing an LLL-reduced lattice basis 7.4. The Schnorr-Euchner algorithm and an integral LLL algorithm 7.5. Some applications of the LLL algorithm 7.6. The Ferguson-Forcade algorithm 7.7. Summary 7.8. Summary 7.9. Summary 7.9. Summary 7.10. Introduction 7.11. Introduction of Polynomials over the Field of Rational Numbers with Polynomial Complexity 8.1. Introduction 8.2. The LLL factorization algorithm: Factorization modulo a prime 8.3. The LLL factorization algorithm: Lifting the factorization 8.4. The LLL factorization algorithm: Lifting the factorization 8.5. The LLL factorization algorithm: A complete description 8.6. A usable factorization algorithm: A complete description 8.7. Factorization of polynomials using approximations 8.8. Summary 8.9. Lintroduction. Discrete Fourier transform and its properties 9.1. Introduction. Discrete Fourier transform and its properties 9.1. Introduction. Discrete Fourier transform and its properties 9.2. Computing the discrete Fourier transform			
6.1. Introduction. A probabilistic algorithm for solving algebraic equations in finite fields 6.2. Solving quadratic equations 6.3. The Berlekamp algorithm 6.4. The Cantor-Zassenhaus method 6.5. Some other improvements of the Berlekamp algorithm 6.6. A probabilistic algorithm for irreducibility testing of polynomials over finite fields 6.7. Summary 6.8. A probabilistic algorithm for irreducibility testing of polynomials over finite fields 6.9. Summary 6.0. The Reduced Lattice Bases and Their Applications 6.0. A probabilistic algorithm for constructing and LLL-reduced lattice basis 6.0. Introduction. Lattices and bases 6.0. An algorithm for constructing an LLL-reduced lattice basis 6.0. An algorithm for constructing and LLL-reduced lattice basis 6.0. The Schnorr-Euchner algorithm and an integral LLL algorithm 6.0. The Ferguson-Forcade algorithm 6.0. The Ferguson-Forcade algorithm 6.0. The Ferguson-Forcade algorithm 6.0. The Ferguson-Forcade algorithm 7.0. Summary 7.1 Introduction 8.2 The LLL factorization algorithm: Using lattices 8.3 The LLL factorization algorithm: Using lattices 8.4 The LLL factorization algorithm: Lifting the factorization 8.5 The LLL factorization algorithm: A complete description 8.6 A usable factorization algorithm: A complete description 8.7 Factorization of polynomials using approximations 8.8 Summary 8.9 Discrete Fourier Transform and Its Applications 9.1 Introduction. Discrete Fourier transform and its properties 9.1 Introduction. Discrete Fourier transform and its properties 9.2 Computing the discrete Fourier transform	5.7.	Summary	113
6.1. Introduction. A probabilistic algorithm for solving algebraic equations in finite fields 6.2. Solving quadratic equations 6.3. The Berlekamp algorithm 6.4. The Cantor-Zassenhaus method 6.5. Some other improvements of the Berlekamp algorithm 6.6. A probabilistic algorithm for irreducibility testing of polynomials over finite fields 6.7. Summary 6.8. A probabilistic algorithm for irreducibility testing of polynomials over finite fields 6.9. Summary 6.0. The Reduced Lattice Bases and Their Applications 6.0. Introduction. Lattices and bases 6.0. LLL-reduced bases and their properties 7.0. LLL-reduced bases and their properties 7.0. An algorithm for constructing an LLL-reduced lattice basis 7.0. The Schnorr-Euchner algorithm and an integral LLL algorithm 7.0. Some applications of the LLL algorithm 7.0. The Ferguson-Forcade algorithm 7.1. Introduction 7.2. Summary 7.3. Summary 7.4. The Ferguson-Forcade algorithm 7.5. Summary 7.6. The Ferguson-Forcade algorithm 7.7. Summary 7.8. Introduction 8.9. The LLL factorization algorithm: Factorization modulo a prime 8.1. Introduction 8.2. The LLL factorization algorithm: Using lattices 8.3. The LLL factorization algorithm: Lifting the factorization 8.5. The LLL factorization algorithm: Lifting the factorization 8.5. The LLL factorization algorithm: A complete description 8.6. A usable factorization algorithm: A complete description 8.7. Factorization of polynomials using approximations 8.8. Summary 8.9. Discrete Fourier Transform and Its Applications 9.1. Introduction. Discrete Fourier transform and its properties 9.2. Computing the discrete Fourier transform 9.3. Introduction Discrete Fourier transform 9.4. Computing the discrete Fourier transform	Chapter	6. Factorization of Polynomials over Finite Fields	115
6.2. Solving quadratic equations 6.3. The Berlekamp algorithm 6.4. The Cantor-Zassenhaus method 6.5. Some other improvements of the Berlekamp algorithm 6.6. A probabilistic algorithm for irreducibility testing of polynomials over finite fields 6.7. Summary 131 Chapter 7. Reduced Lattice Bases and Their Applications 7.1. Introduction. Lattices and bases 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 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 8.3. The LLL factorization algorithm: Lifting the factorization 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: A complete description 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 and its properties	6.1.	· · · · · · · · · · · · · · · · · · ·	
6.3. The Berlekamp algorithm 6.4. The Cantor-Zassenhaus method 6.5. Some other improvements of the Berlekamp algorithm 6.6. A probabilistic algorithm for irreducibility testing of polynomials over finite fields 6.7. Summary 6.8. Summary 6.9. Summary 6.9. Introduction. Lattice Bases and Their Applications 7.1. Introduction. Lattices and bases 7.2. LLL-reduced bases and their properties 7.3. An algorithm for constructing an LLL-reduced lattice basis 7.4. The Schnorr-Euchner algorithm and an integral LLL algorithm 7.5. Some applications of the LLL algorithm 7.6. The Ferguson-Forcade algorithm 7.7. Summary 7.8. Introduction Chapter 8. Factorization of Polynomials over the Field of Rational Numbers with Polynomial Complexity 8.1. Introduction 8.2. The LLL factorization algorithm: Factorization modulo a prime 8.3. The LLL factorization algorithm: Using lattices 8.4. The LLL factorization algorithm: Lifting the factorization 8.5. The LLL factorization algorithm: A complete description 8.6. A usable factorization algorithm: A complete description 8.7. Factorization of polynomials using approximations 8.8. Summary Chapter 9. Discrete Fourier Transform and Its Applications 9.1. Introduction. Discrete Fourier transform and its properties 175 9.2. Computing the discrete Fourier transform and its properties			
6.4. The Cantor-Zassenhaus method 6.5. Some other improvements of the Berlekamp algorithm 6.6. A probabilistic algorithm for irreducibility testing of polynomials over finite fields 6.7. Summary 6.8. Summary 6.9. Summary 6.9. Summary 6.9. Summary 6.9. Summary 6.9. Summary 7.1. Introduction. Lattices Bases and Their Applications 7.1. Introduction. Lattices and bases 7.2. LLL-reduced bases and their properties 7.3. An algorithm for constructing an LLL-reduced lattice basis 7.4. The Schnorr-Euchner algorithm and an integral LLL algorithm 7.5. Some applications of the LLL algorithm 7.6. The Ferguson-Forcade algorithm 7.7. Summary 7.8. Factorization of Polynomials over the Field of Rational Numbers with Polynomial Complexity 8.1. Introduction 8.2. The LLL factorization algorithm: Factorization modulo a prime 8.3. The LLL factorization algorithm: Using lattices 8.4. The LLL factorization algorithm: Lifting the factorization 8.5. The LLL factorization algorithm: A complete description 8.6. A usable factorization algorithm 8.7. Factorization of polynomials using approximations 8.8. Summary 7.9. Discrete Fourier Transform and Its Applications 9.1. Introduction. Discrete Fourier transform and its properties 9.2. Computing the discrete Fourier transform 176	6.2.		118
6.5. Some other improvements of the Berlekamp algorithm 6.6. A probabilistic algorithm for irreducibility testing of polynomials over finite fields 6.7. Summary 131 Chapter 7. Reduced Lattice Bases and Their Applications 7.1. Introduction. Lattices and bases 7.2. LLL-reduced bases and their properties 136 7.3. An algorithm for constructing an LLL-reduced lattice basis 7.4. The Schnorr-Euchner algorithm and an integral LLL algorithm 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 18.3. 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: A complete description 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	6.3.	. •	
6.6. A probabilistic algorithm for irreducibility testing of polynomials over finite fields 6.7. Summary 131 Chapter 7. Reduced Lattice Bases and Their Applications 7.1. Introduction. Lattices and bases 7.2. LLL-reduced bases and their properties 136 7.3. An algorithm for constructing an LLL-reduced lattice basis 7.4. The Schnorr-Euchner algorithm and an integral LLL algorithm 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: A complete description 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 and its properties			
finite fields 6.7. Summary 131 Chapter 7. Reduced Lattice Bases and Their Applications 7.1. Introduction. Lattices and bases 7.2. LLL-reduced bases and their properties 7.3. An algorithm for constructing an LLL-reduced lattice basis 7.4. The Schnorr-Euchner algorithm and an integral LLL algorithm 7.5. Some applications of the LLL algorithm 7.6. The Ferguson-Forcade algorithm 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: A complete description 165 8.5. The LLL factorization algorithm: A complete description 167 8.6. A usable factorization algorithm: A complete description 168 8.7. Factorization of polynomials using approximations 169 8.8. Summary 174 Chapter 9. Discrete Fourier Transform and Its Applications 9.1. Introduction. Discrete Fourier transform and its properties 175 9.2. Computing the discrete Fourier transform and its properties		1 0	127
Chapter 7. Reduced Lattice Bases and Their Applications 7.1. Introduction. Lattices and bases 7.2. LLL-reduced bases and their properties 7.3. An algorithm for constructing an LLL-reduced lattice basis 7.4. The Schnorr-Euchner algorithm and an integral LLL algorithm 7.5. Some applications of the LLL algorithm 7.6. The Ferguson-Forcade algorithm 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 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: Loughlet 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 9.1. Introduction. Discrete Fourier transform and its properties 175 9.2. Computing the discrete Fourier transform	6.6.	· · · · · · · · · · · · · · · · · · ·	190
Chapter 7. Reduced Lattice Bases and Their Applications 7.1. Introduction. Lattices and bases 7.2. LLL-reduced bases and their properties 7.3. An algorithm for constructing an LLL-reduced lattice basis 7.4. The Schnorr-Euchner algorithm and an integral LLL algorithm 7.5. Some applications of the LLL algorithm 7.6. The Ferguson-Forcade algorithm 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 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	6.7		
7.1. Introduction. Lattices and bases 7.2. LLL-reduced bases and their properties 7.3. An algorithm for constructing an LLL-reduced lattice basis 7.4. The Schnorr-Euchner algorithm and an integral LLL algorithm 7.5. Some applications of the LLL algorithm 7.6. The Ferguson-Forcade algorithm 7.7. Summary 7.7. Summary 7.8. Factorization of Polynomials over the Field of Rational Numbers 8.1. Introduction 8.2. The LLL factorization algorithm: Factorization modulo a prime 8.3. The LLL factorization algorithm: Using lattices 8.4. The LLL factorization algorithm: Lifting the factorization 8.5. The LLL factorization algorithm: A complete description 8.6. A usable factorization algorithm: A complete description 8.7. Factorization of polynomials using approximations 8.8. Summary 7.9. Discrete Fourier Transform and Its Applications 9.1. Introduction. Discrete Fourier transform and its properties 9.2. Computing the discrete Fourier transform 9.3. The discrete Fourier transform and its properties 9.4. Computing the discrete Fourier transform 9.5. The computing the discrete Fourier transform 9.6. Augusta Applications 9.7. Introduction. Discrete Fourier transform and its properties 9.8. Computing the discrete Fourier transform	0.7.	5 difficility	101
7.2. LLL-reduced bases and their properties 7.3. An algorithm for constructing an LLL-reduced lattice basis 7.4. The Schnorr-Euchner algorithm and an integral LLL algorithm 7.5. Some applications of the LLL algorithm 7.6. The Ferguson-Forcade algorithm 7.7. Summary 156 Chapter 8. Factorization of Polynomials over the Field of Rational Numbers with Polynomial Complexity 8.1. Introduction 8.2. The LLL factorization algorithm: Factorization modulo a prime 8.3. The LLL factorization algorithm: Using lattices 8.4. The LLL factorization algorithm: Lifting the factorization 8.5. The LLL factorization algorithm: A complete description 8.6. A usable factorization algorithm: A complete description 8.7. Factorization of polynomials using approximations 8.8. Summary 174 Chapter 9. Discrete Fourier Transform and Its Applications 9.1. Introduction. Discrete Fourier transform and its properties 9.2. Computing the discrete Fourier transform 175	Chapter		
7.3. An algorithm for constructing an LLL-reduced lattice basis 7.4. The Schnorr-Euchner algorithm and an integral LLL algorithm 7.5. Some applications of the LLL algorithm 7.6. The Ferguson-Forcade algorithm 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			
7.4. The Schnorr-Euchner algorithm and an integral LLL algorithm 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 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: A complete description 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			
7.5. Some applications of the LLL algorithm 7.6. The Ferguson-Forcade algorithm 7.7. Summary 156 Chapter 8. Factorization of Polynomials over the Field of Rational Numbers with Polynomial Complexity 8.1. Introduction 8.2. The LLL factorization algorithm: Factorization modulo a prime 8.3. The LLL factorization algorithm: Using lattices 8.4. The LLL factorization algorithm: Lifting the factorization 8.5. The LLL factorization algorithm: A complete description 8.6. A usable factorization algorithm: A complete description 8.7. Factorization of polynomials using approximations 8.8. Summary 174 Chapter 9. Discrete Fourier Transform and Its Applications 9.1. Introduction. Discrete Fourier transform and its properties 9.2. Computing the discrete Fourier transform		*	
7.6. The Ferguson-Forcade algorithm 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 9.1. Introduction. Discrete Fourier transform and its properties 9.2. Computing the discrete Fourier transform 176		* · · · · · · · · · · · · · · · · · · ·	
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			
Chapter 8. Factorization of Polynomials over the Field of Rational Numbers with Polynomial Complexity 8.1. Introduction 8.2. The LLL factorization algorithm: Factorization modulo a prime 8.3. The LLL factorization algorithm: Using lattices 8.4. The LLL factorization algorithm: Lifting the factorization 8.5. The LLL factorization algorithm: A complete description 8.6. A usable factorization algorithm 8.7. Factorization of polynomials using approximations 8.8. Summary 174 Chapter 9. Discrete Fourier Transform and Its Applications 9.1. Introduction. Discrete Fourier transform and its properties 9.2. Computing the discrete Fourier transform 175		8	
with Polynomial Complexity 8.1. Introduction 8.2. The LLL factorization algorithm: Factorization modulo a prime 8.3. The LLL factorization algorithm: Using lattices 8.4. The LLL factorization algorithm: Lifting the factorization 8.5. The LLL factorization algorithm: A complete description 8.6. A usable factorization algorithm 8.7. Factorization of polynomials using approximations 8.8. Summary 174 Chapter 9. Discrete Fourier Transform and Its Applications 9.1. Introduction. Discrete Fourier transform and its properties 9.2. Computing the discrete Fourier transform 175	7.7.	Summary	156
with Polynomial Complexity 8.1. Introduction 8.2. The LLL factorization algorithm: Factorization modulo a prime 8.3. The LLL factorization algorithm: Using lattices 8.4. The LLL factorization algorithm: Lifting the factorization 8.5. The LLL factorization algorithm: A complete description 8.6. A usable factorization algorithm 8.7. Factorization of polynomials using approximations 8.8. Summary 174 Chapter 9. Discrete Fourier Transform and Its Applications 9.1. Introduction. Discrete Fourier transform and its properties 9.2. Computing the discrete Fourier transform 175	Chapter	8. Factorization of Polynomials over the Field of Rational Numbers	
8.2. The LLL factorization algorithm: Factorization modulo a prime 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 9.1. Introduction. Discrete Fourier transform and its properties 9.2. Computing the discrete Fourier transform 176		with Polynomial Complexity	159
8.3. The LLL factorization algorithm: Using lattices 8.4. The LLL factorization algorithm: Lifting the factorization 8.5. The LLL factorization algorithm: A complete description 8.6. A usable factorization algorithm 8.7. Factorization of polynomials using approximations 8.8. Summary 174 Chapter 9. Discrete Fourier Transform and Its Applications 9.1. Introduction. Discrete Fourier transform and its properties 9.2. Computing the discrete Fourier transform 175	8.1.	Introduction	159
8.4. The LLL factorization algorithm: Lifting the factorization 8.5. The LLL factorization algorithm: A complete description 8.6. A usable factorization algorithm 8.7. Factorization of polynomials using approximations 8.8. Summary 174 Chapter 9. Discrete Fourier Transform and Its Applications 9.1. Introduction. Discrete Fourier transform and its properties 9.2. Computing the discrete Fourier transform 175	8.2.	The LLL factorization algorithm: Factorization modulo a prime	160
8.5. The LLL factorization algorithm: A complete description 8.6. A usable factorization algorithm 8.7. Factorization of polynomials using approximations 8.8. Summary 174 Chapter 9. Discrete Fourier Transform and Its Applications 9.1. Introduction. Discrete Fourier transform and its properties 9.2. Computing the discrete Fourier transform 175	8.3.	The LLL factorization algorithm: Using lattices	161
8.6. A usable factorization algorithm 8.7. Factorization of polynomials using approximations 8.8. Summary Chapter 9. Discrete Fourier Transform and Its Applications 9.1. Introduction. Discrete Fourier transform and its properties 9.2. Computing the discrete Fourier transform 176	8.4.	The LLL factorization algorithm: Lifting the factorization	165
8.7. Factorization of polynomials using approximations 169 8.8. Summary 174 Chapter 9. Discrete Fourier Transform and Its Applications 9.1. Introduction. Discrete Fourier transform and its properties 9.2. Computing the discrete Fourier transform 176	8.5.	The LLL factorization algorithm: A complete description	167
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	8.6.	A usable factorization algorithm	168
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	8.7.	Factorization of polynomials using approximations	169
 9.1. Introduction. Discrete Fourier transform and its properties 9.2. Computing the discrete Fourier transform 175 176 	8.8.	Summary	174
 9.1. Introduction. Discrete Fourier transform and its properties 9.2. Computing the discrete Fourier transform 175 176 	Chapter	9. Discrete Fourier Transform and Its Applications	175
9.2. Computing the discrete Fourier transform 176	-		
1 0			

CONTENTS vii

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
Append	ix. Facts from Number Theory	215
Bibliogr	Bibliography	
Refer	ences added in the English edition	233
Index		241