

Contents

Part I

1	Basic Computer Arithmetic	3
1.1	Addition	4
1.1.1	Serial	5
1.1.2	Carry-Ripple	8
1.1.3	Parallel-Prefix	9
1.1.4	Carry-Select	17
1.1.5	High Precision	20
1.1.6	Signed Numbers and Subtraction	21
1.2	Multiplication	29
1.2.1	Sequential	31
1.2.2	High Radix	36
1.2.3	Parallel and Sequential-Parallel	41
1.2.4	High Precision	43
1.2.5	Signed Numbers	45
1.2.6	Squaring	45
1.3	Division	47
	References	67

Part II

2	Mathematical Fundamentals I: Number Theory	71
2.1	Congruences	71
2.2	Modular-Arithmetic Operations	73
2.2.1	Addition, Subtraction, and Multiplication	73
2.2.2	Division	74
2.3	Generators and Primitive Roots	75
2.4	Quadratic Residues and Square Roots	78
2.5	The Chinese Remainder Theorem	82
2.6	Residue Number Systems	85
	References	87

3	Modular-Arithmetic Cryptosystems	89
3.1	Message Encryption	90
3.1.1	RSA Algorithm	90
3.1.2	Rabin Algorithm	93
3.1.3	El-Gamal Algorithm	94
3.1.4	Massey-Omura Algorithm	95
3.1.5	Goldwasser-Micali Algorithm	97
3.2	Key Agreement	99
3.3	Digital Signatures	100
3.3.1	El-Gamal Algorithm	100
3.3.2	NIST Algorithm	102
	References	103
4	Modular Reduction	105
4.1	Barrett Reduction	106
4.1.1	Basic Algorithm	108
4.1.2	Extension of Basic Algorithm	112
4.1.3	Implementation	114
4.2	Montgomery Reduction	118
4.2.1	Algorithm	119
4.2.2	Implementation	122
4.3	Lookup-Table Reduction	129
4.4	Special-Moduli Reduction	132
	References	140
5	Modular Addition and Multiplication	143
5.1	Addition	143
5.1.1	Generic Structures	144
5.1.2	Special-Moduli	147
5.1.3	Subtraction	151
5.2	Multiplication	154
5.2.1	Multiplication with Direct Reduction	156
5.2.2	Multiplication with Barrett Reduction	163
5.2.3	Multiplication with Montgomery Reduction	165
5.2.4	Multiplication with Special Moduli	172
	References	180
6	Modular Exponentiation, Inversion, and Division	183
6.1	Exponentiation	183
6.2	Inversion and Division	193
	References	201
 Part III		
7	Mathematical Fundamentals II: Abstract Algebra	205
7.1	Groups and Fields	205
7.1.1	Groups	205
7.1.2	Fields	209

7.2	Ordinary Polynomial Arithmetic	211
7.3	Polynomial Arithmetic Over Finite Fields	216
7.4	Construction of $GF(p^m)$	219
	References	224
8	Elliptic-Curve Basics	225
8.1	Basic Curves	225
8.1.1	Point Addition: Geometric Interpretation	226
8.1.2	Point Addition and Multiplication: Algebraic Interpretation	228
8.2	Elliptic Curves Over Finite Fields	230
8.2.1	$y^2 = x^3 + ax + b$ Over $GF(p)$	231
8.2.2	$y^2 + xy = x^3 + ax + b$ Over $GF(2^m)$	233
8.3	Point-Multiplication Implementation	236
8.4	Projective Coordinates	238
	References	241
9	Elliptic-Curve Cryptosystems	243
9.1	Message Encryption	244
9.1.1	El-Gamal System	245
9.1.2	Massey-Omura System	245
9.1.3	Menezes-Vanstone System	246
9.2	Key Agreement	247
9.2.1	Diffie-Hellman System	247
9.2.2	Matsumoto-Takashima-Imai System	248
9.2.3	Menezes-Qu-Vanstone System	248
9.3	Digital Signatures	249
9.4	Message Embedding	251
	References	251
10	Polynomial-Basis Arithmetic	253
10.1	Addition and Subtraction	253
10.2	Multiplication and Squaring	255
10.2.1	Direct Multiplication	256
10.2.2	Montgomery Multiplication and Squaring	267
10.3	Reduction	272
10.4	Exponentiation, Inversion, and Division	277
	References	287
11	Normal-Basis Arithmetic	289
11.1	Addition, Subtraction, and Squaring	290
11.2	Multiplication	292
11.3	Exponentiation, Inversion, and Division	303
	References	312

A Mathematical Proofs 315

 A.1 Part II of Main Text 315

 A.2 Part III of Main Text 325

 References 331

Index 333