

Contents

	<i>Preface</i>	<i>page</i> ix
	<i>Acknowledgements</i>	xi
	<i>Notation</i>	xiii
1	Integer arithmetic	1
1.1	Representation and notations	1
1.2	Addition and subtraction	2
1.3	Multiplication	3
1.3.1	Naive multiplication	4
1.3.2	Karatsuba's algorithm	5
1.3.3	Toom–Cook multiplication	6
1.3.4	Use of the fast Fourier transform (FFT)	8
1.3.5	Unbalanced multiplication	8
1.3.6	Squaring	11
1.3.7	Multiplication by a constant	13
1.4	Division	14
1.4.1	Naive division	14
1.4.2	Divisor preconditioning	16
1.4.3	Divide and conquer division	18
1.4.4	Newton's method	21
1.4.5	Exact division	21
1.4.6	Only quotient or remainder wanted	22
1.4.7	Division by a single word	23
1.4.8	Hensel's division	24
1.5	Roots	25
1.5.1	Square root	25
1.5.2	k th root	27
1.5.3	Exact root	28

vi	<i>Contents</i>	
1.6	Greatest common divisor	29
1.6.1	Naive GCD	29
1.6.2	Extended GCD	32
1.6.3	Half binary GCD, divide and conquer GCD	33
1.7	Base conversion	37
1.7.1	Quadratic algorithms	37
1.7.2	Subquadratic algorithms	38
1.8	Exercises	39
1.9	Notes and references	44
2	Modular arithmetic and the FFT	47
2.1	Representation	47
2.1.1	Classical representation	47
2.1.2	Montgomery's form	48
2.1.3	Residue number systems	48
2.1.4	MSB vs LSB algorithms	49
2.1.5	Link with polynomials	49
2.2	Modular addition and subtraction	50
2.3	The Fourier transform	50
2.3.1	Theoretical setting	50
2.3.2	The fast Fourier transform	51
2.3.3	The Schönhage–Strassen algorithm	55
2.4	Modular multiplication	58
2.4.1	Barrett's algorithm	58
2.4.2	Montgomery's multiplication	60
2.4.3	McLaughlin's algorithm	63
2.4.4	Special moduli	65
2.5	Modular division and inversion	65
2.5.1	Several inversions at once	67
2.6	Modular exponentiation	68
2.6.1	Binary exponentiation	70
2.6.2	Exponentiation with a larger base	70
2.6.3	Sliding window and redundant representation	72
2.7	Chinese remainder theorem	73
2.8	Exercises	75
2.9	Notes and references	77
3	Floating-point arithmetic	79
3.1	Representation	79
3.1.1	Radix choice	80
3.1.2	Exponent range	81

	<i>Contents</i>	vii
	3.1.3 Special values	82
	3.1.4 Subnormal numbers	82
	3.1.5 Encoding	83
	3.1.6 Precision: local, global, operation, operand	84
	3.1.7 Link to integers	86
	3.1.8 Ziv's algorithm and error analysis	86
	3.1.9 Rounding	87
	3.1.10 Strategies	90
3.2	Addition, subtraction, comparison	91
	3.2.1 Floating-point addition	92
	3.2.2 Floating-point subtraction	93
3.3	Multiplication	95
	3.3.1 Integer multiplication via complex FFT	98
	3.3.2 The middle product	99
3.4	Reciprocal and division	101
	3.4.1 Reciprocal	102
	3.4.2 Division	106
3.5	Square root	111
	3.5.1 Reciprocal square root	112
3.6	Conversion	114
	3.6.1 Floating-point output	115
	3.6.2 Floating-point input	117
3.7	Exercises	118
3.8	Notes and references	120
4	Elementary and special function evaluation	125
	4.1 Introduction	125
	4.2 Newton's method	126
	4.2.1 Newton's method for inverse roots	127
	4.2.2 Newton's method for reciprocals	128
	4.2.3 Newton's method for (reciprocal) square roots	129
	4.2.4 Newton's method for formal power series	129
	4.2.5 Newton's method for functional inverses	130
	4.2.6 Higher-order Newton-like methods	131
	4.3 Argument reduction	132
	4.3.1 Repeated use of a doubling formula	134
	4.3.2 Loss of precision	134
	4.3.3 Guard digits	135
	4.3.4 Doubling versus tripling	136
	4.4 Power series	136

4.4.1	Direct power series evaluation	140
4.4.2	Power series with argument reduction	140
4.4.3	Rectangular series splitting	141
4.5	Asymptotic expansions	144
4.6	Continued fractions	150
4.7	Recurrence relations	152
4.7.1	Evaluation of Bessel functions	153
4.7.2	Evaluation of Bernoulli and tangent numbers	154
4.8	Arithmetic-geometric mean	158
4.8.1	Elliptic integrals	158
4.8.2	First AGM algorithm for the logarithm	159
4.8.3	Theta functions	160
4.8.4	Second AGM algorithm for the logarithm	162
4.8.5	The complex AGM	163
4.9	Binary splitting	163
4.9.1	A binary splitting algorithm for sin, cos	166
4.9.2	The bit-burst algorithm	167
4.10	Contour integration	169
4.11	Exercises	171
4.12	Notes and references	179
5	Implementations and pointers	185
5.1	Software tools	185
5.1.1	CLN	185
5.1.2	GNU MP (GMP)	185
5.1.3	MPFQ	186
5.1.4	GNU MPFR	187
5.1.5	Other multiple-precision packages	187
5.1.6	Computational algebra packages	188
5.2	Mailing lists	189
5.2.1	The GMP lists	189
5.2.2	The MPFR list	190
5.3	On-line documents	190
	<i>References</i>	191
	<i>Index</i>	207