

Contents

Preface	xv
1 Introduction	1
1.1 Multiple Precision Arithmetic	1
1.1.1 What Is Multiple Precision Arithmetic?	1
1.1.2 The Need for Multiple Precision Arithmetic	2
1.1.3 Benefits of Multiple Precision Arithmetic	3
1.2 Purpose of This Text	4
1.3 Discussion and Notation	5
1.3.1 Notation	5
1.3.2 Precision Notation	5
1.3.3 Algorithm Inputs and Outputs	6
1.3.4 Mathematical Expressions	6
1.3.5 Work Effort	7
1.4 Exercises	7
1.5 Introduction to LibTomMath	9
1.5.1 What Is LibTomMath?	9
1.5.2 Goals of LibTomMath	9
1.6 Choice of LibTomMath	10
1.6.1 Code Base	10
1.6.2 API Simplicity	11
1.6.3 Optimizations	11
1.6.4 Portability and Stability	12
1.6.5 Choice	12

2	Getting Started	13
2.1	Library Basics	13
2.2	What Is a Multiple Precision Integer?	14
2.2.1	The mp_int Structure	15
2.3	Argument Passing	17
2.4	Return Values	18
2.5	Initialization and Clearing	19
2.5.1	Initializing an mp_int	19
2.5.2	Clearing an mp_int	22
2.6	Maintenance Algorithms	24
2.6.1	Augmenting an mp_int's Precision	24
2.6.2	Initializing Variable Precision mp_ints	27
2.6.3	Multiple Integer Initializations and Clearings	29
2.6.4	Clamping Excess Digits	31
3	Basic Operations	35
3.1	Introduction	35
3.2	Assigning Values to mp_int Structures	35
3.2.1	Copying an mp_int	35
3.2.2	Creating a Clone	39
3.3	Zeroing an Integer	41
3.4	Sign Manipulation	42
3.4.1	Absolute Value	42
3.4.2	Integer Negation	43
3.5	Small Constants	44
3.5.1	Setting Small Constants	44
3.5.2	Setting Large Constants	46
3.6	Comparisons	47
3.6.1	Unsigned Comparisons	47
3.6.2	Signed Comparisons	50
4	Basic Arithmetic	53
4.1	Introduction	53
4.2	Addition and Subtraction	54
4.2.1	Low Level Addition	54
4.2.2	Low Level Subtraction	59
4.2.3	High Level Addition	63
4.2.4	High Level Subtraction	66

4.3	Bit and Digit Shifting	69
4.3.1	Multiplication by Two	69
4.3.2	Division by Two	72
4.4	Polynomial Basis Operations	75
4.4.1	Multiplication by x	75
4.4.2	Division by x	78
4.5	Powers of Two	81
4.5.1	Multiplication by Power of Two	82
4.5.2	Division by Power of Two	85
4.5.3	Remainder of Division by Power of Two	88
5	Multiplication and Squaring	91
5.1	The Multipliers	91
5.2	Multiplication	92
5.2.1	The Baseline Multiplication	92
5.2.2	Faster Multiplication by the “Comba” Method	97
5.2.3	Even Faster Multiplication	104
5.2.4	Polynomial Basis Multiplication	107
5.2.5	Karatsuba Multiplication	109
5.2.6	Toom-Cook 3-Way Multiplication	116
5.2.7	Signed Multiplication	126
5.3	Squaring	128
5.3.1	The Baseline Squaring Algorithm	129
5.3.2	Faster Squaring by the “Comba” Method	133
5.3.3	Even Faster Squaring	137
5.3.4	Polynomial Basis Squaring	138
5.3.5	Karatsuba Squaring	138
5.3.6	Toom-Cook Squaring	143
5.3.7	High Level Squaring	144
6	Modular Reduction	147
6.1	Basics of Modular Reduction	147
6.2	The Barrett Reduction	148
6.2.1	Fixed Point Arithmetic	148
6.2.2	Choosing a Radix Point	150
6.2.3	Trimming the Quotient	151
6.2.4	Trimming the Residue	152
6.2.5	The Barrett Algorithm	153

6.2.6	The Barrett Setup Algorithm	156
6.3	The Montgomery Reduction	158
6.3.1	Digit Based Montgomery Reduction	160
6.3.2	Baseline Montgomery Reduction	162
6.3.3	Faster “Comba” Montgomery Reduction	167
6.3.4	Montgomery Setup	173
6.4	The Diminished Radix Algorithm	175
6.4.1	Choice of Moduli	177
6.4.2	Choice of k	178
6.4.3	Restricted Diminished Radix Reduction	178
6.4.4	Unrestricted Diminished Radix Reduction	184
6.5	Algorithm Comparison	189
7	Exponentiation	191
7.1	Exponentiation Basics	191
7.1.1	Single Digit Exponentiation	193
7.2	k -ary Exponentiation	195
7.2.1	Optimal Values of k	196
7.2.2	Sliding Window Exponentiation	197
7.3	Modular Exponentiation	198
7.3.1	Barrett Modular Exponentiation	203
7.4	Quick Power of Two	214
8	Higher Level Algorithms	217
8.1	Integer Division with Remainder	217
8.1.1	Quotient Estimation	219
8.1.2	Normalized Integers	220
8.1.3	Radix- β Division with Remainder	221
8.2	Single Digit Helpers	231
8.2.1	Single Digit Addition and Subtraction	232
8.2.2	Single Digit Multiplication	235
8.2.3	Single Digit Division	237
8.2.4	Single Digit Root Extraction	241
8.3	Random Number Generation	245
8.4	Formatted Representations	247
8.4.1	Reading Radix- n Input	247
8.4.2	Generating Radix- n Output	252

9	Number Theoretic Algorithms	255
9.1	Greatest Common Divisor	255
9.1.1	Complete Greatest Common Divisor	258
9.2	Least Common Multiple	263
9.3	Jacobi Symbol Computation	265
9.3.1	Jacobi Symbol	266
9.4	Modular Inverse	271
9.4.1	General Case	273
9.5	Primality Tests	279
9.5.1	Trial Division	279
9.5.2	The Fermat Test	282
9.5.3	The Miller-Rabin Test	284
	Bibliography	289
	Index	291