

# Contents

<i>Preface</i>	vii
1. Introduction	1
1.1 Conventional number systems . . . . .	2
1.2 Redundant signed-digit number systems . . . . .	5
1.3 Residue number systems and arithmetic . . . . .	6
1.3.1 Choice of moduli . . . . .	9
1.3.2 Negative numbers . . . . .	10
1.3.3 Basic arithmetic . . . . .	11
1.3.4 Conversion . . . . .	13
1.3.5 Base extension . . . . .	14
1.3.6 Alternative encodings . . . . .	14
1.4 Using residue number systems . . . . .	15
1.5 Summary . . . . .	17
References . . . . .	18
2. Mathematical fundamentals	21
2.1 Properties of congruences . . . . .	22
2.2 Basic number representation . . . . .	24
2.3 Algebra of residues . . . . .	27
2.4 Chinese Remainder Theorem . . . . .	39
2.5 Complex residue-number systems . . . . .	40
2.6 Redundant residue number systems . . . . .	42
2.7 The Core Function . . . . .	44
2.8 Summary . . . . .	47
References . . . . .	47

3.	Forward conversion	49
3.1	Special moduli-sets . . . . .	50
3.1.1	$\{2^{n-1}, 2^n, 2^{n+1}\}$ moduli-sets . . . . .	52
3.1.2	Extended special moduli-sets . . . . .	56
3.2	Arbitrary moduli-sets: look-up tables . . . . .	58
3.2.1	Serial/sequential conversion . . . . .	59
3.2.2	Sequential/parallel conversion: arbitrary partitioning . . . . .	62
3.2.3	Sequential/parallel conversion: periodic partitioning . . . . .	65
3.3	Arbitrary moduli-sets: combinational logic . . . . .	68
3.3.1	Modular exponentiation . . . . .	68
3.3.2	Modular exponentiation with periodicity . . . . .	78
3.4	Summary . . . . .	80
	References . . . . .	80
4.	Addition	83
4.1	Conventional adders . . . . .	84
4.1.1	Ripple adder . . . . .	85
4.1.2	Carry-skip adder . . . . .	88
4.1.3	Carry-lookahead adders . . . . .	91
4.1.4	Conditional-sum adder . . . . .	97
4.1.5	Parallel-prefix adders . . . . .	101
4.1.6	Carry-select adder . . . . .	108
4.2	Residue addition: arbitrary modulus . . . . .	111
4.3	Addition modulo $2^n - 1$ . . . . .	119
4.3.1	Ripple adder . . . . .	122
4.3.2	Carry-lookahead adder . . . . .	123
4.3.3	Parallel-prefix adder . . . . .	127
4.4	Addition modulo $2^n + 1$ . . . . .	130
4.4.1	Diminished-one addition . . . . .	130
4.4.2	Direct addition . . . . .	131
4.5	Summary . . . . .	134
	References . . . . .	134
5.	Multiplication	137
5.1	Conventional multiplication . . . . .	138
5.1.1	Basic binary multiplication . . . . .	139
5.1.2	High-radix multiplication . . . . .	142

5.2	Conventional division . . . . .	151
5.2.1	Subtractive division . . . . .	151
5.2.2	Multiplicative division . . . . .	160
5.3	Modular multiplication: arbitrary modulus . . . . .	162
5.3.1	Table lookup . . . . .	162
5.3.2	Modular reduction of partial products . . . . .	165
5.3.3	Product partitioning . . . . .	169
5.3.4	Multiplication by reciprocal of modulus . . . . .	173
5.3.5	Subtractive division . . . . .	176
5.4	Modular multiplication: modulus $2^n - 1$ . . . . .	177
5.5	Modular multiplication: modulus $2^n + 1$ . . . . .	185
5.6	Summary . . . . .	191
	References . . . . .	191
6.	Comparison, overflow-detection, sign-determination, scaling, and division . . . . .	193
6.1	Comparison . . . . .	194
6.1.1	Sum-of-quotients technique . . . . .	195
6.1.2	Core Function and parity . . . . .	197
6.2	Scaling . . . . .	198
6.3	Division . . . . .	201
6.3.1	Subtractive division . . . . .	201
6.3.2	Multiplicative division . . . . .	207
6.4	Summary . . . . .	210
	References . . . . .	210
7.	Reverse conversion . . . . .	213
7.1	Chinese Remainder Theorem . . . . .	213
7.1.1	Pseudo-SRT implementation . . . . .	220
7.1.2	Base-extension implementation . . . . .	223
7.2	Mixed-radix number systems and conversion . . . . .	227
7.3	The Core Function . . . . .	234
7.4	Reverse converters for $\{2n - 1, 2n, 2n + 1\}$ moduli-sets . . . . .	237
7.5	High-radix conversion . . . . .	248
7.6	Summary . . . . .	251
	References . . . . .	251
8.	Applications . . . . .	255

8.1	Digital signal processing . . . . .	256
8.1.1	Digital filters . . . . .	257
8.1.2	Sum-of-products evaluation . . . . .	264
8.1.3	Discrete Fourier Transform . . . . .	272
8.1.4	RNS implementation of the DFT . . . . .	275
8.2	Fault-tolerance . . . . .	278
8.3	Communications . . . . .	286
8.4	Summary . . . . .	288
	References . . . . .	289
	<i>Index</i>	293