

Contents

1	Number Systems	1
1.1	Introduction	1
1.1.1	Additional Notation	2
1.1.2	Positional Notation	3
1.2	Positional Notation Using One Base	3
1.2.1	Most Efficient Radix	4
1.2.2	Base Conversion	5
1.2.3	Bases Power of Two	8
1.2.4	Modular Arithmetic	11
1.2.5	Fractional Numbers: Fixed Point Representation	13
1.3	Multiple Radix Representations	15
1.3.1	Double Radix	15
1.3.2	Mixed Radix	15
1.4	Negative Integer Numbers	18
1.4.1	SM Representation	19
1.4.2	Complement Representations	20
1.4.3	Biased Representation	33
1.4.4	Advantages and Disadvantages of the Different Representations	36
1.5	Binary Numbers Multiplication	36
1.5.1	SM Representation	36
1.5.2	Complement Representations	37
1.6	Division and Square Root of Binary Integer Numbers	40
1.6.1	Division	40
1.6.2	Square Root	42
1.7	Decimal Numbers	43
1.7.1	BCD Sum	44
1.7.2	Negative Decimal Numbers	47
1.7.3	Packed BCD Codification (CHC)	49
1.8	Signed Digits	53
1.8.1	Negative Digits	53
1.8.2	Conversion Between Representations	55
1.8.3	Binary Signed Digits (BSD)	56

1.9	Redundant Number Systems	65
1.9.1	Carry Propagation	66
1.9.2	Binary Case	69
1.10	Conclusion	70
	References	70
2	Basic Arithmetic Circuits	71
2.1	Introduction.	71
2.1.1	Serial and Parallel Information	71
2.1.2	Circuit Multiplicity and Pipelining.	72
2.2	Binary Adders	74
2.2.1	Parallel Adders	74
2.2.2	Pipelined Adders	77
2.2.3	Serial Adders	77
2.3	Binary Subtractors	78
2.4	Multipliers	80
2.4.1	Combinational Multipliers	80
2.4.2	Sequential Multipliers	83
2.4.3	Multiplying by a Constant	87
2.5	Exponentiation.	89
2.5.1	Binary Methods.	91
2.5.2	Additive Chains.	95
2.6	Division and Square Root	98
2.6.1	Combinational Divisors	98
2.6.2	Sequential Divisors	99
2.6.3	Dividing by a Constant.	101
2.6.4	Modular Reduction	102
2.6.5	Calculating the Quotient by Undoing the Multiplication	105
2.6.6	Calculating the Quotient by Multiplying by the Inverse of the Divisor.	106
2.6.7	Modular Reduction (Again)	110
2.6.8	Square Root	111
2.7	BCD Adder/Subtractor	112
2.8	Comparators	113
2.9	Shifters	116
2.9.1	Shifters Built with Shift Registers	118
2.9.2	Combinational Shifters	118
2.10	Conclusion	120
	References	120
3	Residue Number Systems	121
3.1	Introduction.	121
3.2	Residue Algebra	122

3.3	Integer Representation Using Residues	130
3.4	Arithmetic Operations Using Residues	132
3.5	Mixed Radix System Associated to Each RNS	133
3.6	Moduli Selection	135
3.7	Conversions.	136
3.7.1	From Positional Notation to RNS	136
3.7.2	From RNS to Positional Notation	139
3.8	Modular Circuits	140
3.8.1	Addition and Subtraction	141
3.8.2	Multiplication and Division.	145
3.8.3	Montgomery Multiplier	150
3.8.4	Exponentiation	151
3.8.5	Two Implementation Examples: 3 and 7.	152
3.9	Conclusion	157
	References	157
4	Basic Algebraic Circuits.	159
4.1	LFSR	159
4.1.1	Type 1 LFSR	160
4.1.2	M Sequences.	164
4.1.3	Polynomials Associated to LFSRs	166
4.1.4	Type 2 LFSR	170
4.1.5	LFSRmod 2^m	174
4.2	LFSRmodp	177
4.2.1	Type 1 LFSRmodp	177
4.2.2	Type 2 LFSRmodp	181
4.2.3	LFSRmodp m	184
4.3	Circuits for Operating with Polynomials.	185
4.3.1	Circuits for Polynomial Addition and Subtraction	186
4.3.2	Circuits for Polynomial Multiplication	187
4.3.3	Circuits for Polynomial Division	192
4.4	Cellular Automata	200
4.4.1	One-Dimensional Linear Cellular Automata	200
4.4.2	One-Dimensional Non-linear Cellular Automata	209
4.5	Bidimensional Cellular Automata.	210
4.5.1	mod 2^n and modp Cellular Automata	214
4.6	Conclusion	215
	References	215
5	Galois Fields GF(2^m)	217
5.1	Addition Over GF(2^m)	217
5.2	Multiplication Over GF(2^m) with Power Representation	218
5.3	Multiplication Over GF(2^m) Using Standard Base	222
5.3.1	Modular Reduction	222
5.3.2	Parallel Multiplication	224

5.3.3	Serial-Parallel Multiplication	228
5.3.4	Serial Multiplication	236
5.4	Multiplication Over $GF(2^m)$ Using the Normal Base	238
5.5	Multiplication Over $GF(2^m)$ Using the Dual Base	246
5.6	Square and Square Root Over $GF(2^m)$	249
5.6.1	Square	250
5.6.2	Square Root	253
5.7	Exponentiation Over $GF(2^m)$	254
5.8	Inversion and Division Over $GF(2^m)$	256
5.9	Operations Over $GF((2^n)^m)$	260
5.10	Conclusion	270
	References	270
6	Galois Fields $GF(p^n)$	271
6.1	$GF(p)$	271
6.1.1	Modular Reduction	272
6.1.2	Inversion and Division	276
6.2	Addition and Subtraction Over $GF(p^n)$	278
6.3	Product Over $GF(p^n)$ Using Power Representation	278
6.4	Product Over $GF(p^n)$ Using the Standard Base	278
6.4.1	Parallel Multiplication	279
6.4.2	Serial-Parallel Multiplication	281
6.4.3	Serial Multiplication	286
6.5	Multiplication Over $GF(p^m)$ Using the Normal Base	287
6.6	Multiplication Over $GF(p^m)$ Using the Dual Base	292
6.7	A^2 and A^p Over $GF(p^m)$	296
6.7.1	Square	296
6.7.2	A^p	297
6.7.3	Exponentiation Over $GF(p^m)$	297
6.8	Inversion and Division Over $GF(p^m)$	300
6.9	Operations Over $GF((p^n)^m)$	302
6.10	Conclusion	302
	References	302
7	Two Galois Fields Cryptographic Applications	303
7.1	Introduction	303
7.2	Discrete Logarithm Based Cryptosystems	304
7.2.1	Fundamentals	304
7.2.2	A Real Example: $GF(2^{233})$	309
7.3	Elliptic Curve Cryptosystems	309
7.3.1	Fundamentals	309
7.3.2	A Real Example: $GF(2^{192} - 2^{64} - 1)$	314
7.4	Conclusion	315
	References	315

Appendix A: Finite or Galois Fields 317

Appendix B: Polynomial Algebra 325

Appendix C: Elliptic Curves 375

Index 389