Contents

1 Introduction 1
References 6

2 Modulo Addition and Subtraction 9
2.1 Adders for General Moduli 9
2.2 Modulo (2^n-1) Adders 12
2.3 Modulo (2^n+1) Adders 16
References 24

3 Binary to Residue Conversion 27
3.1 Binary to RNS Converters Using ROMs 27
3.2 Binary to RNS Conversion Using Periodic Property of Residues of Powers of Two 28
3.3 Forward Conversion Using Modular Exponentiation 30
3.4 Forward Conversion for Multiple Moduli Using Shared Hardware 32
3.5 Low and Chang Forward Conversion Technique for Arbitrary Moduli 34
3.6 Forward Converters for Moduli of the Type $(2^n \pm k)$ 35
3.7 Scaled Residue Computation 36
References 37

4 Modulo Multiplication and Modulo Squaring 39
4.1 Modulo Multipliers for General Moduli 39
4.2 Multipliers mod (2^n-1) 44
4.3 Multipliers mod (2^n+1) 51
4.4 Modulo Squarers 69
References 77

5 RNS to Binary Conversion 81
5.1 CRT-Based RNS to Binary Conversion 81
5.2 Mixed Radix Conversion-Based RNS to Binary Conversion . . . 90

5.3 RNS to Binary Conversion Based on New CRT-I, New CRT-II, Mixed-Radix CRT and New CRT-III 95
5.4 RNS to Binary Converters for Other Three Moduli Sets 97
5.5 RNS to Binary Converters for Four and More Moduli Sets 99
5.6 RNS to Binary Conversion Using Core Function 111
5.7 RNS to Binary Conversion Using Diagonal Function 114
5.8 Performance of Reverse Converters 117
References 128

6 Scaling, Base Extension, Sign Detection and Comparison in RNS 133
6.1 Scaling and Base Extension Techniques in RNS 133
6.2 Magnitude Comparison 153
6.3 Sign Detection 157
References 160

7 Error Detection, Correction and Fault Tolerance in RNS-Based Designs 163
7.1 Error Detection and Correction Using Redundant Moduli 163
7.2 Fault Tolerance Techniques Using TMR 173
References 174

8 Specialized Residue Number Systems 177
8.1 Quadratic Residue Number Systems 177
8.2 RNS Using Moduli of the Form r^n 179
8.3 Polynomial Residue Number Systems 184
8.4 Modulus Replication RNS 186
8.5 Logarithmic Residue Number Systems 189
References 191

9 Applications of RNS in Signal Processing 195
9.1 FIR Filters 195
9.2 RNS-Based Processors 220
9.3 RNS Applications in DFT, FFT, DCT, DWT 226
9.4 RNS Application in Communication Systems 242
References 256

10 RNS in Cryptography 263
10.1 Modulo Multiplication Using Barrett's Technique 265
10.2 Montgomery Modular Multiplication 267
10.3 RNS Montgomery Multiplication and Exponentiation 287
10.4 Montgomery Inverse 295
10.5 Elliptic Curve Cryptography Using RNS 298
10.6 Pairing Processors Using RNS 306
References 343

Index 349

http://www.springer.com/978-3-319-41383-9

Residue Number Systems
Theory and Applications
Ananda Mohan, P.V.
2016, X, 351 p. 131 illus., 17 illus. in color., Hardcover
ISBN: 978-3-319-41383-9
A product of Birkhäuser Basel