Preface

The design of algorithms and hardware implementation for signal processing systems has received considerable attention over the last few decades. The primary area of application was in digital computation and digital signal processing. These systems earlier used microprocessors, and, more recently, field programmable gate arrays (FPGA), graphical processing units (GPU), and application-specific integrated circuits (ASIC) have been used. The technology is evolving continuously to meet the demands of low power and/or low area and/or computation time.

Several number systems have been explored in the past such as the conventional binary number system, logarithmic number system, and residue number system (RNS), and their relative merits have been well appreciated. The residue number system was applied for digital computation in the early 1960s, and hardware was built using the technology available at that time. During the 1970s, active research in this area commenced with application in digital signal processing. The emphasis was on exploiting the power of RNS in applications where several multiplications and additions needed to be carried out efficiently using small word length processors. The research carried out was documented in an IEEE press publication in 1975. During the 1980s, there was a resurgence in this area with an emphasis on hardware that did not need ROMs. Extensive research has been carried out since 1980s and several techniques for overcoming certain bottlenecks in sign detection, scaling, comparison, and forward and reverse conversion.

A compilation of the state of the art was attempted in 2002 in a textbook, and this was followed by another book in 2007. Since 2002, several new investigations have been carried out to increase the dynamic range using more moduli, special moduli which are close to powers of two, and designs that use only combinational logic. Several new algorithms/theorems for reverse conversion, comparison, scaling, and error correction/detection have also been investigated. The number of moduli has been increased, yet the same time focusing on retaining the speed/area advantages.

It is interesting to note that in addition to application in computer arithmetic, application in digital communication systems has gained a lot of attention. Several applications in wireless communication, frequency synthesis, and realization of

transforms such as discrete cosine transform have been explored. The most interesting development has been the application of RNS in cryptography. Some of the cryptography algorithms used in authentication which need big word lengths ranging from 1024 bits to 4096 bits using RSA (Rivest Shamir Adleman) algorithm and with word lengths ranging from 160 bits to 256 bits used in elliptic curve cryptography have been realized using the residue number systems. Several applications have been in the implementation of Montgomery algorithm and implementation of pairing protocols which need thousands of modulo multiplication, addition, and reduction operations. Recent research has shown that RNS can be one of the preferred solutions for these applications, and thus it is necessary to include this topic in the study of RNS-based designs.

This book brings together various topics in the design and implementation of RNS-based systems. It should be useful for the cryptographic research community, researchers, and students in the areas of computer arithmetic and digital signal processing. It can be used for self-study, and numerical examples have been provided to assist understanding. It can also be prescribed for a one-semester course in a graduate program.

The author wishes to thank Electronics Corporation of India Limited, Bangalore, where a major part of this work was carried out, and the Centre for Development of Advanced Computing, Bangalore, where some part was carried out, for providing an outstanding R&D environment. He would like to express his gratitude to Dr. Nelaturu Sarat Chandra Babu, Executive Director, CDAC Bangalore, for his encouragement. The author also acknowledges Ramakrishna, Shiva Rama Kumar, Sridevi, Srinivas, Mahathi, and his grandchildren Baby Manognyaa and Master Abhinav for the warmth and cheer they have spread. The author wishes to thank Danielle Walker, Associate Editor, Birkhäuser Science for arranging the reviews, her patience in waiting for the final manuscript and assistance for launching the book to production. Special thanks are also to Agnes Felema. A and the Production and graphics team at SPi-Global for their most efficiently typesetting, editing and readying the book for production.

Bangalore, India P.V. Ananda Mohan
April 2015

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