International Journal of Innovative
Computing, Information and Control
Volume **6**, Number **4**, April **2010**

 ISSN 1349-4198
pp. 1865–1871

GENERALIZED ARYABHATA REMAINDER THEOREM

Chin-Chen Chang[1], Jieh-Shan Yeh[2] and Jen-Ho Yang[3]

[1]Department of Information Engineering and Computer Science
Feng Chia University
Taichung 40724, Taiwan
ccc@cs.ccu.edu.tw

[2]Department of Computer Science and Information Management
Providence University
200 ChungChi Rd., Taichung 43301, Taiwan
jsyeh@pu.edu.tw

[3]Department of Computer Science and Information Engineering
National Chung Cheng University
Chiayi 621, Taiwan
jenho@cs.ccu.edu.tw

Received October 2008; revised March 2009

Abstract. *The Chinese Remainder Theorem (CRT) and the Generalized Chinese Remainder Theorem (GCRT) are widely employed in signal processing, information coding, and cryptography. However, CRT and GCRT must compute the modular operation with a large number in the final step, which is a time-consuming operation. Instead, the Aryabhata Remainder Theorem (ART) reduces the computation time without computing such large modular operation. However, to the best of our knowledge, no previously published works discuss any variation of ART. Therefore, this study proposes the Generalized Aryabhata Remainder Theorem (GART) which is the first work that discusses the generalized version of ART. Unlike the time complexities of the GCRT, which is $O(n^2 \cdot t^2)$, GART is just $O(n \cdot t^2)$, where n is the number of moduli and t is the number of bits in each modulus. Therefore, the proposed GART is more efficient than GCRT.*
Keywords: Aryabhata remainder theorem, Chinese remainder theorem, Residue number system

1. **Introduction.** In recent years, Residue Number System (RNS) is a popular research in computing large number arithmetic because of its properties of parallel, carry-free and high-speed arithmetic [9]. In RNS, a number is moduloed by the selected moduli, and the number is represented by a vector of several residues. Therefore, the computations in RNS are performed on each residue independently. That is, a large number is separated into several small residues for parallel computing on a multi-processor computer. To apply RNS for large number arithmetic, the conversion between RNS and the binary number system is an important issue. Thus, the literature discloses many conversion algorithms with specific moduli in RNS [1,4,5,7,12].

The common method for the conversion with general moduli in RNS uses the Chinese Remainder Theorem (CRT). An integer is easily reconstructed from its residues which are moduloed by the moduli in RNS. Moreover, CRT can be applied to many applications, such as signal processing, information coding, cryptography, etc. Besides, many generalized version of CRT also have been proposed [2,3,6,11]. The Generalized CRT (GCRT) [1] is a variation of the conventional CRT. In some applications, such as image coding [10,13], GCRT is more practical and flexible than CRT because GCRT additionally provides an