International Journal of Innovative Computing, Information and Control
Volume **5**, Number **7**, July **2009**

 ISSN 1349-4198
pp. **2053–2060**

A PARALLEL CONVERSION ALGORITHM BASED UPON ARYABHATA REMAINDER THEOREM FOR RESIDUE NUMBER SYSTEM

Chin-Chen Chang[1] and Jen-Ho Yang[2]

[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 Engineering
National Chung Cheng University
Chiayi, 621, Taiwan
jenho@cs.ccu.edu.tw

Received January 2008; revised May 2008

Abstract. *To solve the conversion problem in Residue Number System (RNS) with a general moduli set, a common solution is to use Chinese Remainder Theorem (CRT). In CRT, it has to compute a modular arithmetic with a large number to adjust the final result, which is a time-consuming operation. On the contrary, Aryabhata Remainder Theorem (ART) distributes this time-consuming operation into several modular arithmetic with smaller numbers in each iteration. Thus, ART is more suitable than CRT for the parallel processing. In this paper, we propose a parallel conversion algorithm based upon ART for RNS. Unlike the time complexities of the previous researches are O(n), ours is just O($\log_2 n$), where n is the number of the moduli in RNS. Therefore, our algorithm is more efficient than the previous ones.*
Keywords: Chinese remainder theorem, Aryabhata remainder theorem, Residue number system

1. **Introduction.** Recently, numerous number of systems have been proposed to make computers more powerful. One of these systems, which has advantages in computing large numbers, is Residue Number System (RNS). Residue Number System is a particular interest in computing large numbers due to its properties of parallelism, carry-free, and high-speed arithmetic [6]. In RNS, we first choose a set of relatively prime moduli to be the base of this system. Then, the numbers in RNS are represented by the residue of each modulus, and the computations can be performed on each residue independently. Thus, RNS can be applied to many applications, such as digital signature scheme [12] and signal processing [13].

To apply RNS in large number arithmetic, the conversion between RNS and the decimal number system is an important issue. Recently, many researches [2, 3, 9] have been proposed to simplify and accelerate the conversion by choosing a specific set of moduli.

Most of these researches choose each modulus being near the power of 2 to reduce the conversion time, such as $\{2n\text{-}1,\ 2n,\ 2n\text{+}1\}$ and $\{2^n\text{-}1,\ 2^n,\ 2^n\text{+}1\}$ [2, 3]. However, for the general moduli set, the conversion can only be done by the Chinese Remainder Theorem (CRT) or Mixed Radix Conversion (MRC). To convert RNS to the decimal number system, MRC is strictly performed in the sequential processes. On the other hand, CRT can be implemented by parallel processors to make it faster than MRC. Thus, most of the previous researches [1, 7, 11] are based upon CRT when the general moduli