# NEW MODULO DECOMPOSED RESIDUE-TO-BINARY ALGORITHM FOR GENERAL MODULI SETS

*Shaoqiang Bi*, Wei Wang**, and Asim Al-Khalili**

*Department of Electrical & Computer Engineering
Concordia University
** Department of Electrical & Computer Engineering
The University of Western Ontario
Email: bsqiang@ece.concordia.ca, wwang@eng.uwo.ca, asim@ece.concordia.ca

## ABSTRACT

In this paper, we propose a new modulo arithmetic theorem to decompose the base of the modulo operations. This new theorem has been used to further reduce the modulo size of the modified CRT for general moduli sets. Furthermore, we have applied the modulo decomposition technique and the modulo improved CRT to derive a R/B algorithm for a newly found three-moduli set $M=\{2^n-1, 2^n, 2^{n-1}-1\}$. In comparison to the modified CRT, the improved CRT can cut by half the modulo size and reduce the length of the modulo operator in terms of 36%.

## 1. INTRODUCTION

Multimedia has become part of everyone's life. In addition to conventional user interfaces and I/O operations, the multimedia applications demand cost-effective, high-speed and low-power hardware implementations of real-time digital signal processing (DSP) algorithms. The carry-free nature of Residue Number Systems (RNS) has made it perfectly suited for high-speed DSP computation with high precision [1], [2].

As the most complicated part of a RNS system, the residue-to-binary converter has its speed and hardware complexity significantly depending on the chosen moduli set. For general moduli sets, the residue-to-binary (R/B) converters are based on the Chinese Remainder Theorem (CRT) or mixed-radix conversion. New algorithms called modified Chinese Remainder Theorems have been recently proposed to reduce the size of the modulo operation [3], [5].

The modulo carry-propagate addition is the critical part of the design of an area-time efficient residue-to-binary converter. The modulo operation consumes a large portion of the hardware and causes a large delay. Most of the known solutions for the modulo carry-propagate addition rely on end-around-carry adders. However, in end-around-carry adders, the carry-out is fed back into the carry-in, which may lead to an unwanted race condition [4].

In this paper, we propose a new theorem to further enhance the modulo operation leading to much smaller and faster modulo operation

## 2. BACKGROUND

For any two numbers $X$ and $P_i$, $x_i = X \bmod P_i$ is defined as $X = x_i + bP_i$ for some integer $b$ such that $0 \le x_i < P_i$. For convenience, we denote $X \bmod P_i$ by $\left|X\right|_{P_i}$.

To perform the R/B conversion, i.e., to convert the residue number $(x_1, x_2, ..., x_n)$ into the binary number $X$, the Chinese Remainder Theorem is widely used. The CRT requires a modulo-$M$ (large-valued) operation and it is not efficient for the implementation. Thus we need to use a new formulation of the CRT that reduces modulo operations from modulo $M = P_1P_2...P_m$ to modulo $P_2...P_n$ [3].

**Modified CRT:** Given the moduli set $\{P_1, P_2, ..., P_m\}$, the residue number $(x_1, x_2, ..., x_m)$ is converted into the binary number $X$ by

$$X = x_1 + P_1\left|\sum_{i=1}^{m} w_i x_i'\right|_{P_2...P_m} \qquad (1)$$

where $m > 1$, $w_1 = \dfrac{N_1\left|N_1^{-1}\right|_{P_1} - 1}{P_1}$, $w_i = \dfrac{N_i}{P_1}$, for $i = 2,3,...,m$,

$x_1' = x_1$, and $x_i' = \left|N_i^{-1}\right|_{P_i} x_i$, for $i = 2,3,...,m$.

In the next section, we will propose a new theorem that further reduces the base of the modulo operation in modified CRT. We need the following properties:

Lemma 1 $\left|KP_1\right|_{P_1P_2} = P_1\left|K\right|_{P_2}$ for all integers $K, P_1$ and $P_2$

Lemma 2 $\left|A+B\right|_P = \left|\left|A\right|_P + \left|B\right|_P\right|_P$ for all integers $A, B$ and $P$

Lemma 3 $\left|\left|K\right|_{P_1}\right|_{P_1P_2} = \left|K\right|_{P_1}$ for all integers $K, P_1$ and $P_2$

## 3. MODULO DECOMPOSITION ALGORITHM

We now propose a new theorem to decompose the base of the modulo arithmetic.

**Theorem 1** Given integers $K$, $P_1, P_2, \cdots, P_n$, where n>1, we have

$$|K|_{P_1 P_2 \cdots P_n} = \sum_{m=1}^{n-1} \left( \left\lfloor \frac{K}{\prod_{i=1}^{m} P_i} \right\rfloor_{P_{m+1}} \prod_{i=1}^{m} P_i \right) + |K|_{P_1} \qquad (2)$$

**Proof:** (Proved by mathematical induction)

(1) Base step:

Since n >1, let n = 2. We have

$$|K|_{P_1P_2} = \left| P_1 \left\lfloor \frac{K}{P_1} \right\rfloor + |K|_{P_1} \right|_{P_1P_2} = \left\| P_1 \left\lfloor \frac{K}{P_1} \right\rfloor_{P_1P_2} + \left| |K|_{P_1} \right|_{P_1P_2} \right|_{P_1P_2}$$

$$= \left| P_1 \left\lfloor \frac{K}{P_1} \right\rfloor_{P_2} + |K|_{P_1} \right|_{P_1P_2}$$

Since $P_1 \left\lfloor \frac{K}{P_1} \right\rfloor_{P_2} \le P_1(P_2 - 1)$ and $|K|_{P_1} < P_1$, we have $\left( P_1 \left\lfloor \frac{K}{P_1} \right\rfloor_{P_2} + |K|_{P_1} \right) < P_1P_2$. Thus $|K|_{P_1P_2} = P_1 \left\lfloor \frac{K}{P_1} \right\rfloor_{P_2} + |K|_{P_1}$.

When n = 3, we have

$$|K|_{P_1P_2P_3} = P_1P_2 \left\lfloor \frac{K}{P_1P_2} \right\rfloor_{P_3} + |K|_{P_1P_2}$$

$$= P_1P_2 \left\lfloor \frac{K}{P_1P_2} \right\rfloor_{P_3} + P_1 \left\lfloor \frac{K}{P_1} \right\rfloor_{P_2} + |K|_{P_1}$$

$$= \sum_{m=1}^{2} \left( \left\lfloor \frac{K}{\prod_{i=1}^{m} P_i} \right\rfloor_{P_{m+1}} \prod_{i=1}^{m} P_i \right) + |K|_{P_1}$$

Thus, Theorem 1 holds for n =2 and n =3.

(2) Induction step:

Assumption: Theorem 1 is true when n = $W$, where $W$ is a positive integer and $W > 1$. That is,

$$|K|_{P_1P_2 \cdots P_W} = \sum_{m=1}^{W-1} \left( \left\lfloor \frac{K}{\prod_{i=1}^{m} P_i} \right\rfloor_{P_{m+1}} \prod_{i=1}^{m} P_i \right) + |K|_{P_1}$$

We need to show that Theorem 1 holds for n = $W$+1.

That is, $|K|_{P_1P_2 \cdots P_W P_{W+1}} = \sum_{m=1}^{W} \left( \left\lfloor \frac{K}{\prod_{i=1}^{m} P_i} \right\rfloor_{P_{m+1}} \prod_{i=1}^{m} P_i \right) + |K|_{P_1}$

Proof for induction step:

$$|K|_{P_1P_2 \cdots P_W P_{W+1}} = P_1P_2 \cdots P_W \left\lfloor \frac{K}{P_1P_2 \cdots P_W} \right\rfloor_{P_{W+1}} + |K|_{P_1P_2 \cdots P_W}$$

$$= \left\lfloor \frac{K}{\prod_{i=1}^{W} P_i} \right\rfloor_{P_{W+1}} \prod_{i=1}^{W} P_i + \sum_{m=1}^{W-1} \left( \left\lfloor \frac{K}{\prod_{i=1}^{m} P_i} \right\rfloor_{P_{m+1}} \prod_{i=1}^{m} P_i \right) + |K|_{P_1}$$

$$= \sum_{m=1}^{W} \left( \left\lfloor \frac{K}{\prod_{i=1}^{m} P_i} \right\rfloor_{P_{m+1}} \prod_{i=1}^{m} P_i \right) + |K|_{P_1}$$

Thus, we have shown that Theorem 1 holds for n = $W$ + 1 under the assumption that Theorem 1 holds for n = $W$.

In conclusion, from the base step and induction step, Theorem 1 holds for any positive integers that are greater than 1.

■

With Theorem 1, it is seen that a modulo operation based on the product of n positive integers $P_1, P_2, \cdots, P_n$ can be decomposed to n individual modulo operations where each operation is based on one of the positive integers $P_1, P_2, \cdots, P_n$. Using Theorem 1, a modulo operation with large base can be partitioned into several small wordlength channels in parallel. Thus, Theorem 1 can result in a parallel and high-speed operation.

We give the following example to illustrate how Theorem 1 works.

**Example 1:** For a modulo operation $|1099|_{120}$ and four small integers $2 \times 3 \times 4 \times 5 = 120$, we have

$$|1099|_{120} = 19$$

using Theorem 1, we have

$$|1099|_{2\times3\times4\times5} = 2\times3\times4\times \left\lfloor \frac{1099}{2\times3\times4} \right\rfloor_5 + 2\times3\times \left\lfloor \frac{1099}{2\times3} \right\rfloor_4$$

$$+ 2\times \left\lfloor \frac{1099}{2} \right\rfloor_3 + |1099|_2$$

$$= 0 + 18 + 0 + 1 = 19$$

With Theorem 1, we use 4 parallel small size modulo operations to take the place of one big size modulo operation. The length of modulo operation is reduced from 7 bits to 3 bits. Theorem 1 provides us with a very high concurrent operation, thus resulting in very high speed and low-power VLSI implementation.

## 4. MODULO DECOMPOSITION R/B ALGORITHM FOR GENERAL MODULI SETS

In this section, we apply the proposed modulo reduction technique to simplify the modulo operation with large base in the modified CRT for general moduli sets.

**Theorem 2** Given the moduli set $\{P_1, P_2, \cdots, P_n\}$, the residue number $(x_1, x_2, \cdots, x_n)$ is converted into the binary number $X$ by

$$X = x_1 + \sum_{m=1}^{n-2}\left(\left\| \frac{\sum_{i=1}^{n} w_i x_i'}{\prod_{i=2}^{m+1} P_i} \right\|_{P_{m+2}} \prod_{i=1}^{m+1} P_i\right) + P_1\left|\sum_{i=1}^{n} w_i x_i'\right|_{P_2} \qquad (3)$$

where n>1,

$$w_1 = \frac{N_1\left|N_1^{-1}\right|_{P_1} - 1}{P_1},$$

$$w_i = \frac{N_i}{P_1}, \text{ for i } = 2,3,\ldots,n$$

$$x_1' = x_1,$$

$$x_i' = \left|N_i^{-1} x_i\right|_{P_i}, \text{ for i = 2,3,…,n}$$

(Proof is omitted due to lack of space)

Theorem 2 can reduce the complexity of the modulo operation in CRT and the modified CRT to a great scale by partitioning the modulo operation with a large base to several individual modulo operations of small bases in parallel. The parallelism provides high concurrent operation and reduces the delay. And by choosing the bases of several individual modulo operations with similar magnitude, we can increase the modularity and reduce the area further. We use the following example to compare the Modified CRT and Theorem 2.

**Example 2:** Given the moduli set {9, 8, 7, 5}, the residue number (7, 4, 3, 2) is converted to the binary number format $X$.

Using the modified CRT, we get $w_1 = 311$, $w_2 = 35$, $w_3 = 40$, $w_4 = 56$, $\left|N_1^{-1}\right|_9 = 10$, $\left|N_2^{-1}\right|_8 = 3$, $\left|N_3^{-1}\right|_7 = 5$, and $\left|N_4^{-1}\right|_5 = 4$. The modulo base is $8\times7\times5 = 280$.

$$X = x_1 + 9\times\left|311\times x_1 + 35\times3\times x_2 + 40\times5\times x_3 + 56\times4\times x_4\right|_{280}$$
$$= 7 + 9\times\left|3645\right|_{280} = 7 + 9\times5 = 52$$

Using Theorem 2, we get $w_1 = 311$, $w_2 = 35$, $w_3 = 40$, $w_4 = 56$, $\left|N_1^{-1}\right|_9 = 10$, $\left|N_2^{-1}\right|_8 = 3$, $\left|N_3^{-1}\right|_7 = 5$, and $\left|N_4^{-1}\right|_5 = 4$.

$$\sum_{i=1}^{n} w_i x_i' = 311\times7 + 35\times3\times4 + 40\times5\times3 + 56\times4\times2 = 3645$$

$$X = x_1 + P_1P_2P_3\left\| \frac{\sum_{i=1}^{n} w_i x_i'}{P_2P_3} \right\|_{P_4} + P_1\left[ 2^n \left\| \frac{\sum_{i=1}^{n} w_i x_i'}{2^n} \right\|_{P_3} + \left|\sum_{i=1}^{n} w_i x_i'\right|_{2^n} \right]$$

$$= 7 + 9\times8\times7\times\left\| \frac{3645}{8\times7} \right\|_5 + 9\times8\times\left\| \frac{3645}{8} \right\|_7 + \left|3645\right|_8 = 52$$

The above R/B conversion requires one modulo-280 operation if using the modified CRT. By using Theorem 2, the same R/B conversion requires only three small size operations: modulo-5, modulo-7 and modulo-8. That is to say, compared to the modified CRT, the proposed method decreases the modulo size from 9-bit to 4-bit.

## 5. NEW R/B ALGORITHM FOR M

We now apply the modulo reduction technique and the modulo reduced CRT to derive R/B algorithms for one newly found three-moduli set in form of $\{2^n-1, 2^n, 2^{n-1}-1\}$. We present the three-moduli case of Theorem 2 as Corallary 1.

**Collorary 1**: Given the moduli set $\{P_1, P_2, P_3\}$, where $P_2 = 2^k$, the residue number $(x_1, x_2, x_3)$ is converted into the binary number $X$ by

$$X = x_1 + P_1\left[ 2^k \left\| \frac{\sum_{i=1}^{3} w_i x_i'}{2^k} \right\|_{P_3} + \left|\sum_{i=1}^{3} w_i x_i'\right|_{2^k} \right] \qquad (4)$$

where n>1,

$$w_1 = \frac{N_1\left|N_1^{-1}\right|_{P_1} - 1}{P_1},$$

$$w_i = \frac{N_i}{P_1}, \text{ for i } = 2,3,\ldots,n$$

$$x_1' = x_1,$$

$$w_1 = \frac{N_1\left|N_1^{-1}\right|_{P_1} - 1}{P_1}, \text{ for i = 2,3,…,n}$$

(Proof is omitted due to lack of space)

The following R/B algorithm for a newly found three-moduli sets in form of $\{P_1, 2^n, P_3\}$ is derived based on Collorary 1. The modulo operation of the R/B algorithms is simplified to modulo one number.

**Proposition 1:** For $M=\{2^n-1, 2^n, 2^{n-1}-1\}$, we have

$$X = x_1 + (2^n - 1)Y$$

where n>1, and

$$Y = 2^n\left\| \frac{K}{2^n} \right\|_{2^{n-1}-1} + \left|K\right|_{2^n}$$

$$K = \left(2^{2n-1} - 2^{n+1} + 1\right)x_1 + \left(2^{2n-2} - 1\right)x_2 + 2^{2n-2}x_3$$

(Proof is omitted due to lack of space)

When $P_1 = 2^n$, $|K|_{P_1} = |K|_{2^n}$ is just a truncation operation. $|K|_{2^n}$ is the $n$-bit LSBs of $K$, whereas the floor operation $\left\lfloor \frac{K}{P_1} \right\rfloor = \left\lfloor \frac{K}{2^n} \right\rfloor$ is the remaining part after the truncation. Then these two operations will not require any hardware resources in the VLSI implementation.

**Example 3:** For a R/B converter with 8-bit dynamic range based on the moduli set $M=\{2^n-1, 2^n, 2^{n-1}-1\}$, the specific moduli set {15,16,7} is chosen when n=4, since $7\times16\times15=1680>2^8=256$. Randomly choose a number from 0 to 255, for example, $X$=38. Its RNS representation $X=(x_1, x_2, x_3)$ is (8,6,3).

Based on the modified CRT, we have

$$Y = \left|\left(2^{2n-1} - 2^{n+1} + 1\right)x_1 + \left(2^{2n-2} - 1\right)x_2 + 2^{2n-2}x_3\right|_{2^n(2^{n-1}-1)}$$
$$= \left|(2^{2\times4-1} - 2^{4+1} + 1)\times 8 + (2^{2\times4-2} - 1)\times 6 + 2^{2\times4-2}\times 3\right|_{2^4(2^{4-1}-1)}$$
$$= |1346|_{112} = 2$$
$$X = x_1 + (2^n - 1)\times Y = 8 + 15\times 2 = 38$$

Based on Proposition 1, we have

$$K = \left(2^{2n-1} - 2^{n+1} + 1\right)x_1 + \left(2^{2n-2} - 1\right)x_2 + 2^{2n-2}x_3$$
$$= (2^{2\times4-1} - 2^{4+1} + 1)\times 8 + (2^{2\times4-2} - 1)\times 6 + 2^{2\times4-2}\times 3 = 1346$$
$$Y = 2^n \left\| \frac{K}{2^n} \right\|_{2^{n-1}-1} + |K|_{2^n}$$
$$= 2^4 \times \left\| \frac{1346}{2^4} \right\|_7 + |1346|_{16}$$
$$= 2^4 \times |84|_7 + |1346|_{16}$$

The binary representation of 1346 is $(10101000010)_2$, thus $1346\times 2^{-4} = (1010100.0010)_2$. And $(1010100)_2$ is equal to 84, while $(0010)_2$ is the binary representation of $|1346|_{16}$. Then, we have

$$Y = 2^4 \times |(1010100)_2|_7 + (0010)_2$$
$$= 2^4 \times (000)_2 + (0010)_2$$
$$= (00000010)_2 = 2$$
$$X = x_1 + (2^n - 1)\times Y = 8 + 15\times 2 = 38$$

When using the modified CRT, the above residue-to-binary conversion needs a modulo 112 operation. By using Proposition 1 which is derived from Theorem 2, the modulo size is reduced from 112 to 7. That is to say, the length of modulo operation is reduced from 7-bit to 3-bit. Also, the modulo operator is decreased from 1346 to 84, reduced by 4-bit. The 4-bit LSBs of $Y$ are just the same 4-bit LSBs of 1346. Also notice that the operations of multiplication by $2^4$ and addition to $(0010)_2$ correspond to a simple concatenation operation. The comparison between the modified CRT and the improved CRT is summarized in Table I. The reduction in size of both the modulo base and the modulo operator will result in a saving of the hardware resource for a VLSI implementation. It is noticeable that the concatenation and calculation do not consume any hardware resources. Thus, Theorem 2 is useful for the VLSI implementation of R/B converters to reduce the size of the modulo operation.

TABLE I
COMPARISON BETWEEN
MODIFIED CRT AND IMPROVED CRT

| | Modified CRT | Improved CRT | Improvement |
|---|---|---|---|
| Modulo Size | 7-bit | 3-bit | 57% |
| Modulo Operator | 11-bit | 7-bit | 36% |

## 6. CONCLUSION

In this paper, we have proposed a new modulo arithmetic theorem to decompose the base of the modulo operations. This new theorem has been used to further reduce the modulo size of the modified CRT [3], [5] for general moduli sets. Furthermore, we have applied the modulo decomposition technique and the modulo improved CRT to derive a R/B algorithm for one newly found three-moduli set $M=\{2^n-1, 2^n, 2^{n-1}-1\}$. Comparing with the modified CRT, the improved CRT can cut down more than half of the modulo size and reduce the length of the modulo operator in terms of 36%.

## 7. REFERENCES


[1] H. L. Garner, " The residue number system," *IRE Trans. Electronic Computers*. vol. 8, pp. 140-147, June 1959.

[2] M. A. Soderstrand, *Residue Number System Arithmetic: Modern Applications in Digital Signal Processing.* New York: IEEE Press, 1986.

[3] Wei Wang, M. N. S. Swamy, M. O. Ahmad and Yuke Wang, "A study of residue-to-binary converters for three-moduli sets," *IEEE Trans. Circuits and Systems-I*, vol. 50, No. 2, Feb. 2003.

[4] C.Efstathiou, D.Nikolos, and J.Kalamatianos, "Area-time efficient modulo $2^n$-1 adder design," *IEEE Trans. Circuits and Systems*, 41(7): 463-467, July 1994.

[5] Yuke Wang, "Residue-to-binary converters based on new Chinese remainder theorems," *IEEE Trans. Circuits and Systems-II*, pp. 197-206, Mar. 2000.