Residue Number System Operands to Decimal Conversion for 3-Moduli Sets

Kazeem Alagbe Gbolagade[1,2], Member, IEEE and Sorin Dan Cotofana[1], Senior Member IEEE,
1. Computer Engineering Laboratory, Delft University of Technology,
The Netherlands. E-mail: {gbolagade,sorin}@ce.et.tudelft.nl
2. University for Development Studies, Navrongo, Ghana.

***Abstract*—This paper investigates the conversion of 3-moduli Residue Number System (RNS) operands to decimal. First we assume a general $\{m_i\}_{i=1,3}$ moduli set with the dynamic range $M = \prod_{i=1}^{3} m_i$ and introduce a modified Chinese Remainder Theorem (CRT) that requires mod-m_3 instead of mod-M calculations. Subsequently, we further simplify the conversion process by focussing on $\{2n+2, 2n+1, 2n\}$ moduli set, which has a common factor of 2. We introduce in a formal way a CRT based approach for this case, which requires the conversion of $\{2n+2, 2n+1, 2n\}$ set into moduli set with relatively prime moduli, i.e., $\left\{\frac{m_1}{2}, m_2, m_3\right\}$, when n is even, $n \geq 2$ and $\left\{m_1, m_2, \frac{m_3}{2}\right\}$, when n is odd, $n \geq 3$. We demonstrate that such a conversion can be easily done and doesn't require the computation of any multiplicative inverses. Finally, we further simplify the 3-moduli CRT for the specific case of $\{2n+2, 2n+1, 2n\}$ moduli set. For this case the propose CRT requires 4 additions, 4 multiplications and all the operations are mod-m_3 in case n is even and mod-$\frac{m_3}{2}$ if n is odd. This outperforms state of the art converters in terms of required operations and due to the fact that the numbers involved in the calculations are smaller it results in less complex adders and multipliers.**

***Index Terms*—Residue Number System, Moduli Set with a Common factor, RNS-Decimal Converter, Chinese Remainder Theorem.**

I. Introduction

Carry propagation constitutes the main reason why computing hardware based on Weighted Number System (WNS) cannot be speed up beyond certain bounds. Consequently, the reduction/elimination of carry chain is the major challenge in improving the computer arithmetic units performance. Several approaches to speed up the carry propagation, e.g., carry lookahead, prefix calculations, anticipated calculation, and alternative number representation systems, e.g., (redundant) signed digit systems, Residue Number Systems (RNS) have been proposed. RNS has interesting inherent characteristics such as parallelism, modularity, fault tolerance and carry free operations and for this reason it has been widely used in Digital Signal Processing (DSP) applications such as digital filtering, convolutions, correlation, fast Fourier transforms, discrete Fourier transforms and image processing [1]-[3]. RNS based calculation requires data conversions, which must be as fast as possible not to nullify the RNS advantages. Several converters have been proposed in the past [3], [4], [6]-[8] based on either the Chinese Remainder Theorem (CRT) or Mixed Radix Conversion (MRC).

In this paper we investigate the RNS to binary conversion for RNS with $\{m_1, m_2, m_3\}$ moduli set, with $m_1 > m_2 > m_3$. Such moduli sets have been extensively studied and the most utilized are $\{2^n+1, 2^n, 2^n-1\}$, [2], [4], [6], and $\{2n+2, 2n+1, 2n\}$, which constitutes an extension of the first one.

First we assume a general $\{m_i\}_{i=1,3}$ moduli set with the dynamic range $M = \prod_{i=1}^{n} m_i$ and introduce a modified Chinese Remainder Theorem (CRT) that requires mod-m_3 instead of mod-M calculations. Subsequently, we focuss on $\{2n+2, 2n+1, 2n\}$ moduli set, which has a common factor of 2. Given that for such a moduli set CRT cannot be directly applied we introduce in a formal way a CRT based approach for this case, which requires the conversion of $\{2n+2, 2n+1, 2n\}$ set into moduli set with relatively prime moduli, i.e., $\left\{\frac{m_1}{2}, m_2, m_3\right\}$, when n is even, $n \geq 2$ and $\left\{m_1, m_2, \frac{m_3}{2}\right\}$, when n is odd, $n \geq 3$. In general such a moduli set transformation is a complex computation process but for the case of $\{2n+2, 2n+1, 2n\}$ moduli set we demonstrate that it can be easily done and doesn't require the computation of any multiplicative inverses. Finally, we further simplify the 3-moduli CRT for the specific case of $\{2n+2, 2n+1, 2n\}$ moduli set. For this case the propose CRT requires 4 additions, 4 multiplications and all the operations are mod-m_3 in case n is even and mod-$\frac{m_3}{2}$ if n is odd. This outperforms state of the art converters in terms of required operations and due to the fact that the numbers involved in the calculations are smaller it results in less complex adders and multipliers.

The rest of the article is organised as follows: In Section II we introduce the necessary background. Section III presents our proposal starting from the formal representation of the CRT for moduli set sharing a common factor. In Section IV we evaluate the performance of our scheme while the paper is concluded in Section V.

II. Background

RNS is defined in terms of a set of relatively prime moduli set $\{m_i\}_{i=1,n}$ such that gcd $(m_i, m_j) = 1$ for $i \neq j$, where gcd means the greatest common divisor of m_i and m_j, while $M = \prod_{i=1}^{n} m_i$, is the dynamic range. The residues of a decimal number X can be obtained as $x_i = |X|_{m_i}$ thus it can be represented in RNS as $X = (x_1, x_2, x_3 ..., x_n)$, $0 \leq x_i < m_i$. This representation is unique for any integer $X \in [0, M-1]$. We note here that in this paper we use $|X|_{m_i}$ to denote the X mod m_i operation and the

978-1-4244-2167-1/08/$25.00 ©2008 IEEE

operator Θ to represent the operation of addition, subtraction, or multiplication. Given any two integer numbers K and L RNS represented by $K = (k_1, k_2, k_3, ..., k_n)$ and $L = (l_1, l_2, l_3, ..., l_n)$, respectively, $W = K\Theta L$, can be calculated as $W = (w_1, w_2, w_3, ..., w_n)$, where $w_i = |k_i \Theta l_i|_{m_i}$, for $i = 1, n$. This means that the complexity of the calculation of the Θ operation is determined by the number of bits required to represent the residues and not by the one required to represent the input operands.

For a moduli set$\{m_i\}_{i=1,n}$ with the dynamic range $M = \prod_{i=1}^{n} m_i$, the residue number $(x_1, x_2, x_3, ..., x_n)$ can be converted into the decimal number X, according to the Chinese Reminder Theorem, as follows [1]:

$$X = \left| \sum_{i=1}^{n} M_i \left| M_i^{-1} x_i \right|_{m_i} \right|_M , \tag{1}$$

where $M = \prod_{i=1}^{n} m_i$, $M_i = \frac{M}{m_i}$, and $M_i^{-1}$is the multiplicative inverse of M_i with respect to m_i.

We note here that the moduli set $\{m_i\}_{i=1,n}$ must be pairwise relatively prime for Equation (1) to be directly used. For the $\{2n + 2, 2n + 1, 2n\}$ moduli set $2n + 2$ and $2n$ share a common factor. This implies that to utilize Equation (1) in the conversion this moduli set must be first mapped to a set of relatively prime moduli. If a moduli set is not pairwise relatively prime, then not every residue set $(x_1, x_2, x_3, ..., x_n)$ corresponds to a number and this results into inconsistency. As given in [1], a set of residues is consistent if and only if $|x_i|_k = |x_j|_k$ where $k = gcd(m_i, m_j)$ for all i and j. If this holds true the decimal equivalent of $(x_1, x_2, x_3, ..., x_n)$ for moduli set which are not pairwise relatively prime can be computed as follows [1]:

$$|X|_{M_L} = \left| \sum_{i=1}^{n} \alpha_i x_i \right|_{M_L} , \tag{2}$$

where M_L is the Lowest Common Multiple (LCM) of $\{m_i\}_{i=1,n}$, the set of moduli sharing a common factor, X is the decimal equivalent of $\{x_i\}_{i=1,n}$, α_i is an integer such that $|\alpha_i|_{\frac{M_L}{\mu_i}} = 0$ and $|\alpha_i|_{\mu_i} = 1$, and $\{\mu_i\}_{i=1,n}$ is a set of integers such that $M_L = \prod_{i=1}^{n} \mu_i$ and μ_i divides m_i. It should be noted that α_i may not exist for some i.

III. Proposed Algorithm

The main idea behind our approach is to simplify Equation (1) by eliminating the large modulo M and by removing the cost of computing M_i^{-1}. In this section we demonstrate that the first is possible for any 3-moduli RNS, while the second one can be achieved only for 3-moduli sets which are not pairwise relatively prime.

We first introduce a modified CRT for general moduli set of length three which doesn't require mod-M computations.

Theorem 1: For a moduli set $\{m_i\}_{i=1,3}$ the decimal equivalent X of the residue set $\{x_1, x_2, x_3\}$ can be computed as:

$$X = (x_1 + x_2) + m_1 m_2 \left| k_1 x_1 + k_2 x_2 + \left| M_3^{-1} \right|_{m_3} x_3 \right|_{m_3} ,$$

where M_3^{-1} is the multiplicative inverse of M_3, $k_1 = \frac{(M_1 |M_1^{-1}|_{m_1} - 1)}{m_1 m_2}$ and $k_2 = \frac{(M_2 |M_2^{-1}|_{m_2} - 1)}{m_1 m_2}$.

Proof: We use lemmas presented earlier in [7]:

Lemma 1: $|am_1|_{m_1 m_2} = m_1 |a|_{m_2}$

Lemma 2: $M_1 \left| M_1^{-1} \right|_{m_1} = 1 + k_1 m_1 m_2$

Lemma 3: $M_2 \left| M_2^{-1} \right|_{m_2} = 1 + k_2 m_1 m_2$

Expanding Equation (1) for $n = 3$ we obtain:

$$X = |M_1 \left| M_1^{-1} \right|_{m_1} x_1 + M_2 \left| M_2^{-1} \right|_{m_2} x_2 + M_3 \left| M_3^{-1} \right|_{m_3} x_3|_{m_1 m_2 m_3} \tag{3}$$

Using Lemma 2 and 3 in the above equation, we have:

$$X = |(1 + k_1 m_1 m_2) x_1 + (1 + k_2 m_1 m_2) x_2 + M_3 \left| M_3^{-1} \right|_{m_3} x_3|_{m_1 m_2 m_3} \tag{4}$$

Further simplification gives:

$$X = (x_1 + x_2) + |k_1 m_1 m_2 x_1 + k_2 m_1 m_2 x_2 + M_3 \left| M_3^{-1} \right|_{m_3} x_3|_{m_1 m_2 m_3} \tag{5}$$

Applying Lemma 1, we get:

$$X = (x_1 + x_2) + m_1 m_2 |k_1 x_1 + k_2 x_2 + M_3^* \left| M_3^{-1} \right|_{m_3} x_3|_{m_3} \tag{6}$$

Here, $M_3^* = \frac{M_3}{m_1 m_2} = 1$, the equation then reduces to:

$$X = (x_1 + x_2) + m_1 m_2 |k_1 x_1 + k_2 x_2 + \left| M_3^{-1} \right|_{m_3} x_3|_{m_3} \tag{7}$$

■

It can be observed that Equation (7) makes use of mod-m_3 (the smallest modulus) instead of mod-M operations thus the magnitude of involved values is smaller than in the traditional CRT, and that k_1 and k_2 can be precomputed.

The next simplification step is the elimination of the M_i^{-1}. To achieve that we restrict to $\{2n + 2, 2n + 1, 2n\}$ moduli sets and first introduce a formal representation of Equation (2).

Theorem 2: For a moduli set $\{m_i\}_{i=1,n}$ sharing a common factor, which must first be mapped into a set of pairwise relatively prime moduli, $\{\mu_i\}_{i=1,n}$, the decimal equivalent X of the residue set $\{x_1, x_2, x_3, ..., x_n\}$ can be computed as:

$$|X|_{M_L} = \left| \sum_{i=1}^{n} \beta_i \left| \beta_i^{-1} \right|_{\mu_i} x_i \right|_{M_L} , \tag{8}$$

where $M_L = LCM \{m_i\}_{i=1}^{n} = \prod_{i=1}^{n} \mu_i$, $\beta_i = \frac{M_L}{\mu_i}$, $\left| \beta_i^{-1} \right|_{\mu_i}$ is the multiplicative inverse of β_i with respect to μ_i.

Proof: To demonstrate the correctness of Equation (8), we shall relate it to Equation (2). All the conditions in Equation (2) have been taken care of in our mapping formula except for the condition that α_i is an integer such that $|\alpha_i|_{\frac{M_L}{\mu_i}} = 0$ and $|\alpha_i|_{\mu_i} = 1$.

Let us assume that $\alpha_i = \beta_i * k$. This implies that $|\beta_i * k|_{\mu_i} = 1$, meaning that: $k = \left| \beta_i^{-1} \right|_{\mu_i}$. We can then write $\alpha_i = \beta_i * \left| \beta_i^{-1} \right|_{\mu_i}$ and this is what we have in Equation (8).

We then show that $|\alpha_i|_{\frac{M_L}{\mu_i}} = 0$. $|\alpha_i|_{\frac{M_L}{\mu_i}} = \left|\beta_i * \left|\beta_i^{-1}\right|_{\mu_i}\right|_{\frac{M_L}{\mu_i}}$, which implies that $|\alpha_i|_{\frac{M_L}{\mu_i}} = \left|\frac{M_L}{\mu_i} * \left|\beta_i^{-1}\right|_{\mu_i}\right|_{\frac{M_L}{\mu_i}}$ since $\beta_i = \frac{M_L}{\mu_i}$, $|\alpha_i|_{\frac{M_L}{\mu_i}} = 0$. Hence, Equation (8) is a formal representation of Equation (2). ■

To utilize Equation (8) in the conversion we need a method to compute relatively prime $\{\mu_i\}_{i=1,n}$ for a moduli set $\{m_i\}_{i=1,n}$ sharing a common factor. According to [3] and [4] the moduli set $\{2n+2, 2n+1, 2n\}$ with a common factor can be mapped to a set of pairwise relatively prime moduli, μ_i given by:

1) $\{n+1, 2n+1, 2n\}$, which implies that the new moduli set is $\left\{\frac{m_1}{2}, m_2, m_3\right\}$, when n is even, $n \geq 2$,
2) $\{2n+2, 2n+1, n\}$, which implies that the new moduli set is $\left\{m_1, m_2, \frac{m_3}{2}\right\}$, when n is odd, $n \geq 3$.

The conditions $(n \geq 2)$ and $(n \geq 3)$ are very important as due to them $\mu_i > 1$ meaning that $\left|\beta_i^{-1}\right|_{\mu_i}$ in Equation (8) and as consequence α_i in Equation (2) always exists.

Based on this we wrote a C++ program for the moduli set $\{2n+2, 2n+1, 2n\}$ to obtain the LCM of the moduli for different values of n and taking the condition $M_L = \prod_{i=1}^{n} \mu_i$ and $|m_i|_{\mu_i} = 0$ into consideration. From the pattern of results obtained we could see that mapping from m_i to μ_i can be done by classifying the values of n into even and odd, which is in good agreement with what has been suggested in [3] and [4]. Moreover, based on the collected experimental data, some of which are displayed in Table III, IV, V and VI, we observed that there is a well established relationship between the various multiplicative inverses and the moduli. Deductions are made based on this observation and the relations are presented in Table I and II.

The experimental results presented in Table I, using the new set $\left\{\frac{m_1}{2}, m_2, m_3\right\}$, suggest that the following relations exist between the moduli and the multiplicative inverses:

$\left|\mu_1^{-1}\right|_{\mu_3} = \frac{m_1}{2}$, $\left|(\mu_1\mu_2)^{-1}\right|_{\mu_3} = \frac{m_1}{2}$,
$\left|(\mu_2\mu_3)^{-1}\right|_{\mu_1} = \frac{m_3}{4} + 1$, $\left|(\mu_1\mu_3)^{-1}\right|_{\mu_2} = m_2 - 2$,
$\left|\mu_1^{-1}\right|_{\mu_2} = 2$.

Similarly,Table II, using the new set $\left\{m_1, m_2, \frac{m_3}{2}\right\}$, suggest that the following holds true:

$\left|\mu_1^{-1}\right|_{\mu_3} = \frac{m_1}{4}$, $\left|(\mu_1\mu_2)^{-1}\right|_{\mu_3} = \frac{m_1}{4}$,
$\left|(\mu_2\mu_3)^{-1}\right|_{\mu_1} = m_1 - \frac{m_3}{2}$, $\left|(\mu_1\mu_3)^{-1}\right|_{\mu_2} = m_2 - 2$,
$\left|\mu_1^{-1}\right|_{\mu_2} = 2$.

As previously mentioned for moduli sets with a common factor not all remainder sets are valid numbers. The following proposition state the condition for a 3-residue set to represent a valid number.

Proposition 1: For RNS with moduli set $\{m_1, m_2, m_3\}$ sharing a common factor, (x_1, x_2, x_3) represents a valid number if and only if $(x_1 + x_3)$ is even.

Proof: This proposition has been proved in [4]. ■

Making the appropriate substitution in Theorem 1 we can particularize it for 3-moduli RNS sharing a common factor as follows:

S/N	Multiplicative inverses	Equivalent values
1	$\left\|\mu_1^{-1}\right\|_{\mu_2}$	2
2	$\left\|\mu_2^{-1}\right\|_{\mu_3}$	1
3	$\left\|\mu_1^{-1}\right\|_{\mu_3}$	$\frac{m_1}{2}$
4	$\left\|(\mu_1\mu_2)^{-1}\right\|_{\mu_3}$	$\frac{m_1}{2}$
5	$\left\|(\mu_2\mu_3)^{-1}\right\|_{\mu_1}$	$\frac{m_3}{4} + 1$
6	$\left\|(\mu_1\mu_3)^{-1}\right\|_{\mu_2}$	$m_2 - 2$

Table I
MULTIPLICATIVE INVERSE VALUE FOR N EVEN ($(n \geq 2)$)

S/N	Multiplicative inverses	Equivalent values
1	$\left\|\mu_1^{-1}\right\|_{\mu_2}$	1
2	$\left\|\mu_2^{-1}\right\|_{\mu_3}$	1
3	$\left\|\mu_1^{-1}\right\|_{\mu_3}$	$\frac{m_1}{4}$
4	$\left\|(\mu_1\mu_2)^{-1}\right\|_{\mu_3}$	$\frac{m_1}{4}$
5	$\left\|(\mu_2\mu_3)^{-1}\right\|_{\mu_1}$	$m_1 - \frac{m_3}{2}$
6	$\left\|(\mu_1\mu_3)^{-1}\right\|_{\mu_2}$	$(m_2 - 2)$

Table II
MULTIPLICATIVE INVERSE VALUE FOR N ODD ($(n \geq 3)$)

Corollary 1: For the moduli set $\{2n+2, 2n+1, 2n\}$ the decimal equivalent X of the residue set $\{x_1, x_2, x_3\}$, $(x_1 + x_3)$ being even, can be computed as follows:

1) If n is **even**:

$$X = (x_1 + x_2) + \frac{m_1 m_2}{2}|k_1 x_1 + k_2 x_2 + \frac{m_1}{2} x_3|_{m_3},$$

where

$$k_1 = \frac{2((m_2 m_3)(\frac{m_3}{4} + 1) - 1)}{(m_1 m_2)},$$
$$k_2 = \frac{2(\frac{(m_1 m_3)}{2}(m_2 - 2) - 1)}{m_1 m_2}.$$

2) If n is **odd**:

$$X = (x_1 + x_2) + m_1 m_2 \left|k_1 x_1 + k_2 x_2 + \frac{m_1}{4} x_3\right|_{\frac{m_3}{2}},$$

where

$$k_1 = \frac{(\frac{m_2 m_3}{2}(m_1 - \frac{m_3}{2}) - 1)}{m_1 m_2},$$
$$k_2 = \frac{(\frac{m_1 m_3}{2}(m_2 - 2) - 1)}{m_1 m_2}.$$

Proof: Trivial with proper substitutions from Table I and II and due to Proposition 1. ■

IV. PERFORMANCE EVALUATION

Clearly, it can be seen that the numbers involved in the multiplication are very small when compared to the numbers involved in the direct CRT implementation. Additionally, the large modulo M calculations are replaced by modulo calculations with the smallest modulus in the moduli set under consideration.

n	Given Set	New Set	$\left\|(\mu_1\mu_2)^{-1}\right\|_{\mu_3}$
2	$\{6,5,4\}$	$\{3,5,4\}$	3
4	$\{10,9,8\}$	$\{5,9,8\}$	5
6	$\{14,13,12\}$	$\{7,13,12\}$	7
8	$\{18,17,16\}$	$\{9,17,16\}$	9
10	$\{22,21,20\}$	$\{11,21,20\}$	11
12	$\{26,25,24\}$	$\{13,25,24\}$	13

Table III
MAPPING FOR N EVEN AND MULTIPLICATIVE INVERSE

n	$\left\|\mu_1^{-1}\right\|_{\mu_3}$	$\left\|(\mu_2\mu_3)^{-1}\right\|_{\mu_1}$	$\left\|(\mu_1\mu_3)^{-1}\right\|_{\mu_2}$
2	3	2	3
4	5	3	7
6	7	4	11
8	9	5	15
10	11	6	19
12	13	7	23

Table IV
MULTIPLICATIVE INVERSE VALUES FOR N EVEN

Previous work on 3-moduli RNS in [3,4] has demonstrated improvement over traditional CRT in terms of operands magnitude as this determines the complexity and delay of the associated RNS hardware. Additionally, [4] outperformed [3] in terms of the operands magnitude thus we compare our proposal with this approach. As indicated in Table VII our proposal requires less arithmetic operations and even more important for the hardware, complexity of the operands magnitude is significantly reduced. More specifically, the modulo operation has been reduced from modulo $M = m_1m_3$ to modulo m_3 or $\frac{m_3}{2}$.

V. CONCLUSIONS

First we assumed a general $\{m_i\}_{i=1,3}$ moduli set with the dynamic range $M = \prod_{i=1}^{n} m_i$ and introduced a modified Chinese Remainder Theorem (CRT) that requires mod-m_3 instead of mod-M calculations. This scheme can be utilized in conjunction with well established moduli sets, e.g, $\{2^n+1, 2^n, 2^n-1\}$ and $\{2n+2, 2n+1, 2n\}$ and makes the CRT based conversion more effective as it reduces the magnitude of the values involved in the conversion thus the associated costs in area and delay. Subsequently, we further simplified the conversion process by focussing on $\{2n+2, 2n+1, 2n\}$ moduli set, which has a common factor of 2. Given that for such a moduli set CRT cannot be directly applied, we introduced in a formal way a CRT based approach for this case, which requires the conversion of $\{2n+2, 2n+1, 2n\}$ set into moduli set with relatively prime moduli, i.e., $\left\{\frac{m_1}{2}, m_2, m_3\right\}$, when n is even, $n \geq 2$ and $\left\{m_1, m_2, \frac{m_3}{2}\right\}$, when n is odd, $n \geq 3$. We demonstrated that the moduli set transformation can be easily done and doesn't require the computation of any multiplicative inverses. Finally, we further simplified the 3-moduli CRT for the specific case of $\{2n+2, 2n+1, 2n\}$ moduli set. For this case the propose CRT required 4 additions, 4 multiplications and all the operations are mod-m_3 in case n is even and mod-$\frac{m_3}{2}$ if n is odd. This outperforms state of the art converter in terms of required operations and due to the fact that the numbers involved in the calculations are smaller it results in less complex adders and multipliers. Our proposal is particularly suitable in DSP applications where the moduli sets are restricted and the dynamic range does not necessarily need to be too large.

n	Given Set	New Set	$\left\|(\mu_1\mu_2)^{-1}\right\|_{\mu_3}$
3	$\{8,7,6\}$	$\{8,7,3\}$	2
5	$\{12,11,10\}$	$\{12,11,5\}$	3
7	$\{16,15,14\}$	$\{16,15,7\}$	4
9	$\{20,19,18\}$	$\{20,19,9\}$	5
11	$\{24,23,22\}$	$\{24,23,11\}$	6
13	$\{28,27,26\}$	$\{28,27,13\}$	7

Table V
MAPPING FOR N ODD AND MULTIPLICATIVE INVERSE

n	$\left\|\mu_1^{-1}\right\|_{\mu_3}$	$\left\|(\mu_2\mu_3)^{-1}\right\|_{\mu_1}$	$\left\|(\mu_1\mu_3)^{-1}\right\|_{\mu_2}$
3	2	5	5
5	3	7	9
7	4	9	13
9	5	11	17
11	6	13	21
13	7	15	25

Table VI
MULTIPLICATIVE INVERSE VALUES FOR N ODD

Operations	[4]	Proposed Algorithm
Additions	5	4
Multiplications	4	4
Reduced M	m_3m_1	m_3 or $\frac{m_3}{2}$

Table VII
PERFORMANCE COMPARISON

REFERENCES

[1] Szabo, N. and Tanaka, R: 'Residue Arithmetic and its Application to Computer Technology' , MC-Graw-Hill, New York, 1967.
[2] M. A. Soderstrand, W. K. Jenkins, G. A. Jullien, and F. J. Taylor, Residue Number System Arithmetic: Modern Applications in Digital Signal Processing. New York, IEEE press, 1986.
[3] A. B. Premkuma, An RNS to Binary Converter in a Three Moduli Set with Common Factors, IEEE Trans. on Circuits and Systems-II: Analog and Digital Processing, Vol. 42, No. 4, pp 298-301, April, 1995.
[4] Y. Wang, M.N.S. Swamy , M.O. Ahmad, Residue to Binary number Converters for three moduli sets, IEEE Trans. Circuits Syst. II, vol. 46, pp. 180-183, Feb., 1999.
[5] A. B. Premkuma, Corrections to "An RNS to Binary Converter in a Three Moduli Set with Common Factors", IEEE Trans. on Circuits and Systems-II: Analog and Digital Processing, Vol. 51, No.1, pp 43, January, 2004.
[6] W. Wang, M.N.S. Swamy, M.O. Ahmad and W. Wang, A study of Residue to Binary Converters for the Three-Moduli Sets, IEEE Trans. on Circuits and Syst-Fundamental Theory and Applications, Vol. 50, No. 2, pp 235-245, 2003.
[7] Y. Wang, New Chinese Remainder Theorems, in Proc. Asilomar Conference, USA, pp. 165-171, Nov., 1998.
[8] H.M. Yassine and W.R. Moore, Improved Mixed Radix Conversion for Residue Number System Architectures, proceedings of IEEE pt-G, Vol. 138, No. 1, pp. 120-124, Feb., 1991.
[9] A. B. Premkumar, An RNS to Binary Converter in $2n+1$, $2n$, $2n-1$ Moduli Set, IEEE Trans. on Circuits and Systems-II: Analog and Digital Signal Processing, Vol. 39, No. 7, pp. 480-482, July, 1992.