International Journal of Electrical Engineering.
ISSN 0974-2158 Volume 12, Number 1 (2019), pp. 21-35
© International Research Publication House
http://www.irphouse.com

Efficient Reverse Converter for Three Moduli Set $\{2n-2, 2n-3, 2n-4\}$ Sharing a Common Factor

Valentine Aveyom [1,2], M.I. Daabo (PhD)[2], Abdul- Barik, Alhassan (PhD)[2]

[1] Notre Dame Seminary SHS, Box 10, Navrongo.
[2] University for Development Studies, Department of Computer Science, Navrongo.

Abstract

This paper presents a reverse converter for the non-coprime three moduli set $\{2n-2, 2n-3, 2n-4\}$ based on the Chinese Remainder Theorem (CRT) approach. The paper introduces the Residue Number System (RNS) sub-field of study and presents a least modulus conversion technique for the stated moduli set. It also presents in summarized tables, the computation of multiplicative inverses as well as generated relatively prime moduli sets for both even and odd cases of $n \geq 3$ for the stated set. A new converter is implemented based on a simplified CRT approach. Area and delay comparison with the hardware proposed in (Premkumar, 1995) are also carried out.

I. INTRODUCTION

Residue Number System (RNS) is a sub-area under finite field arithmetic (Neha, 2008). This area is widely used in digital signal processing, image processing, Finite Impulse Response (FIR) filters, and Infinite Impulse Response(IIR) filters because of its carry-free property and high efficiency in addition and multiplication (Chaves & Sousa, 2007).

A lot of computer systems researchers are interested in RNS because of its benefits such as error detection and correction (Modern et al, 2012), its inherent parallelism, modularity, fault tolerance and localized carry propagation properties. Therefore, RNS is used in some arithmetic operations such as addition and multiplication for more efficient results than in conventional two's complement systems.

II. FUNDAMENTALS OF RNS

Residue Number System (RNS) is defined in terms of a set of relatively prime moduli set $\{m_i\}_{i=1,k}$ such that the $\gcd(m_i, m_j) = 1$for $i \neq j$, where gcd means the greatest common divisor of m_i, and m_j, while $M = \prod_{i=1}^{k} m_i$, is the dynamic range. The residues

of a decimal number X can be obtained as $x_i = |X|_{m_i}$, thus X can be represented in RNS as $X = (x_1, x_2, x_3, \dots, x_k)$, $0 \le x_i \le m_i$. This representation is unique for any integer $X \in [0, M-1]$. $|X|_{m_i}$is the modulo operation of X with respect to m_i (Gbolagade, 2011).

2.1 Chinese Remainder Theorem (CRT)

The Chinese Remainder Theorem (CRT) can be used to backward convert the residue digits $(x_1, x_2, x_3, \dots, x_N)$ of the moduli set $\{m_1, m_2, m, \dots, m_N\}$ to its decimal number (X) as shown;

For a moduli set $\{m_i\}_{i=1,N}$ with the dynamic range $M = \prod_{i=1}^{k} m_i$, then the residue number $(x_1, x_2, x_3, \dots, x_N)$ can be converted into the decimal number X, based on the CRT, as follows:

$$X = \left| \sum_{i=1}^{N} \ell_i \, |k_i x_i|_{m_i} \right|_M \tag{1}$$

Where;

$$M = \prod_{i=1}^{N} m_i \ ;$$

$$\ell_i = \frac{M}{m_i} \ ; \ |k_i \times \ell_i|_{m_i} = 1$$

(Gbolagade et al., 2009).

2.2 Mixed Radix Conversion (MRC)

The Mixed Radix Conversion (MRC) approach serves as an alternative method to the CRT as it does not involve the use of the large modulo-M computation. The conversion process is carried out by converting the residue digits (x_1, x_2, x_3) of the moduli set $\{m_1, m_2, \dots m_3\}$ to its decimal equivalent (X) as follows;

$$X = a_1 + a_2 m_1 + a_3 m_1 m_2 + a_n m_1 m_2 m_3 \dots m_{k-1} \tag{2}$$

Where; $a_{i,i=1,k}$ are the Mixed Radix Digits (MRDs) are computed as;

$$a_1 = x_1$$

$$a_2 = \left| (x_2 - a_1) |m_1^{-1}|_{m_2} \right|_{m_2}$$

$$a_3 = \left| ((x_3 - a_1) |m_1^{-1}|_{m_3} - a_2) |m_2^{-1}|_{m_3} \right|_{m_3}$$

$$\vdots$$

(Gbolagade et al., 2008).

2.3 Revised Chinese Remainder Theorem (CRT) for Moduli Set with Common Factors

The revised CRT is stated as;

$$|X|_{M_L} = \left| \sum_{i=1}^{k} \propto_i X_i \right|_{M_L} \tag{3}$$

Where M_L is the Least Common Multiple (LCM) of $\{M_i\}_{i=1,k}$, the moduli set sharing a common factor.

X is the decimal equivalent of $\{x_i\}_{i=1,k}$

$\propto_i$ is any integer such that $| \propto_i |_{M_L} = 0$ and $| \propto_i |_{\mu_1}$=1 and $\{\mu_i\}_{i=1,K} is$ a set of integers such that

$M_L = \prod_{i=1}^{k} \mu_i$ and μ_i divides M_i

Note however that, $\propto_i$ may not exist for some values of i.

III. PROPOSED CONVERSION TECHNIQUES

The presented conversion techniques are based on two approaches. These are the m_3-Modulus Conversion Technique and the computation without modulo arithmetic.

3.1 m_3-Modulus Conversion Technique

This technique seeks to reduce the cost of computing by eliminating the computation of the dynamic Range (M) from the Chinese Remainder Theorem (CRT). The technique first presents the modified CRT for general 3-moduli set $\{m_1, m_2, m_3\}$ which does not use the dynamic range (M) in computations.

Theorem 1:

For any moduli set $\{m_i\}_{i=1,3}$ with common factors, the decimal equivalent X of the residue number $(x_{1,}x_{2,}x_3)$ can be computed using ;

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

Where m_3^{-1} is the multiplication inverseofm_3

$$K_1 = \frac{(m_1 | m_1^{-1} | m_1 - 1)}{m_1 m_2} \text{and}$$

$$K_2 = \frac{(m_2 | m_2^{-1} | m_2 - 1)}{m_1 m_2}$$

The theorem aims at reducing the magnitude of the values involved in the computation.

Proof:

The lemmas as presented by (Wang, 1998) are used to achieve the proof as follows:

Lemma 1: $|am_1|_{m_1m_2} = m_1|a|_{m_2}$

Lemma 2: $|m_1|M_1^{-1}|_{m_1} = 1 + k_1m_1m_2$

Lemma 3: $|m_2|M_2^{-1}|_{m_2} = 1 + k_2m_1m_2$

Expanding equation (1) for $k = 3$ we obtain:

$$X = |m_1|M_1^{-1}|_{m_1}x_1 + m_2|M_2^{-1}|_{m_2}x_2 + m_3|M_3^{-1}|_{m_3}x_3|_{m_1m_2m_3} \quad (5)$$

Putting Lemmas 2 and 3 into equation (5) we obtain:

$$X = |(1 + k_1m_1m_2)x_1 + |(1 + k_2m_1m_2)x_2 + m_3|M_3^{-1}|_{m_3}x_3|_{m_1m_2m_3} \quad (6)$$

Simplifying further gives;

$$X = (x_1 + x_2) + |k_1m_1m_2x_1 + k_2m_1m_2x_2 + m_3|M_3^{-1}|_{m_3}x_3|_{m_1m_2m_3} \quad (7)$$

Thus applying Lemma 1, we obtain;

$$X = (x_1 + x_2) + m_1m_2|k_1x_1 + k_2x_2 + m_3^*|M_3^{-1}|_{m_3}x_3|_{m_3} \quad (8)$$

Here $m_3^* = \frac{m_3}{m_1m_2} = 1$, then equation (8) reduces to the form;

$$X = (x_1 + x_2) + m_1m_2|k_1x_1 + k_2x_2 + |M_3^{-1}|_{m_3}x_3|_{m_3} \quad (9)$$

This equation uses only mod- m_3 for computation instead of mod- M. The approach then further proceeds to eliminate M_i^{-1} from the computations.

Theorem 2:

For any moduli set $\{m_i\}_{I=1,3}$ sharing a common factor which is being mapped to a relatively prime moduli set $\{\mu_1\}_{i=1,3}$,(x_1, x_2, x_3) is computed as ;

$$|X|_{M_L} \sum_{i=1}^{k} \beta_i|\beta_i^{-1}|\mu_i x_i|_{M_L} \quad (10)$$

Where;

M_L=LCM$\{m_i\}_{i=1,3}$ $\prod_{i=1}^{3}\mu_i$, $\beta_i = \frac{M_L}{\mu_i}$, $|\beta_i^{-1}|_{\mu_i}$ is the multiplication inverse of β_i with respect to μ_i.

Proof:

This is proved by relating equation (10) to equation (3) where all the conditions are present except for $\propto_i$ being an integer such that $|\propto_i|_{\frac{M_L}{u_i}}$ =0 and $|\propto_i|_{u_i}$=1.

Assume that $\propto_i = \beta_i * p$. It implies that $|\beta_i * p|_{u_i}$=1, which implies that $p = |\beta_i{}^{-1}|_{u_i}$. Therefore it can be written that $\propto_i = \beta_i * |\beta_i{}^{-1}|_{u_i}$ as is in equation (10)

We then show that $| \propto_i |_{\frac{M_L}{u_i}}$=0. $| \propto_i |_{\frac{M_L}{u_i}} = |\beta_i * |\beta_i{}^{-1}|_{u_i}|_{\frac{M_L}{u_i}}$, which implies that;

$$| \propto_i |_{\frac{M_L}{u_i}} = |\frac{M_L}{u_i} * |\beta_i{}^{-1}|_{u_i}|_{\frac{M_L}{u_i}}$$

Since $\beta_i = \frac{M_L}{u_i}$, $| \propto_i |_{\frac{M_L}{u_i}} = 0$, hence equation (10) is a more formal way of representing equation (3).

To perform reverse conversion using equation (4) however requires a method of computing the relatively prime $\{m_i\}_{i=1,3}$ of the moduli set with common factor $\{m_i\}_{i=1,3}$.

According to (Ahmad et al.,1999), the moduli set $\{2n-2, 2n-3, 2n-4\}$ sharing a common factor of 2 can be mapped to a set of relatively prime moduli set,$\{ u_i\}_{i=1,3}$ by using the given relations as shown;

1. $\{m_1, m_2, m_3\}$=$\{\frac{m_1}{2}, m_2, m_3\}$

   i.e. $\{2n-2, 2n-3, 2n-4\}$ =$\{n-1, 2n-3, 2n-4\}$, when n is even , $n > 2$

2. $\{m_1, m_2, m_3\}$=$\{m_1, m_2, \frac{m_3}{2}\}$,

   i.e. $\{2n-2, 2n-3, 2n-4\}$ =$\{2n-2, 2n-3, n-2\}$, when n is odd, $n \geq 3$

Note that, the conditions($n > 2$) and ($n \geq 3$) are very important as it is based on it that (μ_i>1) and $\propto_i$ exists.

For moduli sets with common factors, not all residues are valid numbers. For a 3-moduli set sharing a common factor to represent a valid number, the following proposition must hold;

Proposition 1:

For any RNS moduli set $\{m_i\}_{i=1,3}$ sharing a common factor, then $(x_1x_2x_3)$ will represent a valid number if and only if $(x_1 + x_3)$ is even.

The Prove to this proposition can be seen in (Ahmad et al., 1999).

Substituting the proposed moduli set $\{2n-2, 2n-3, 2n-4\}$ into Theorem 1 gives;

Corollary 1:

For the moduli set $\{2n-2, 2n-3, 2n-4\}$ sharing a common factor 2, the decimal equivalent X of a residue number (x_1, x_2, x_3) for even and odd as stated in proposition 1 are computed as shown:

1. If n is even, then;

$$X = (x_1 + x_2) + \frac{m_1 m_2}{2} |k_1 x_1 + k_2 x_2 \frac{m_1}{2} x_3 | m_3 \qquad (11)$$

Where;

$$k_1 = \frac{2[(m_2 m_3)\left(\frac{m_2}{4}+1\right)-1]}{m_1 m_2}$$

$$k_2 = \frac{2[\left(\frac{m_1 m_3}{2}\right)(m_2-2)-1]}{m_1 m_2}$$

2. If n is odd;

$$X = (x_1+x_2) + m_1 m_2 \left| k_1 x_1 + k_2 x_2 + \frac{m_1}{4} x_3 \right| \frac{m_3}{2} \quad (12)$$

Where $k_1 = \frac{\left[\frac{m_2 m_3}{2}\left(m_1 - \frac{m_3}{2}\right)-1\right]}{(m_1 m_2)}$ and

$k_2 = \frac{[\frac{m_1 m_3}{2}(m_2-2)-1]}{m_1 m_2}$

Table 1: For Even $n > 2$

S/N	Multiplicative Inverses	Equivalent Values
1	$\lvert\mu_1^{-1}\rvert\mu_2$	2
2	$\lvert\mu_2^{-1}\rvert\mu_3$	1
3	$\lvert\mu_1^{-1}\rvert\mu_3$	$\frac{m_1}{2}$
4	$\lvert(\mu_1\mu_2)^{-1}\rvert\mu_3$	$\frac{m_1}{2}$
5	$\lvert(\mu_2\mu_3)^{-1}\rvert\mu_1$	$\frac{m_3}{4}+1$
6	$\lvert(\mu_1\mu_3)^{-1}\rvert\mu_2$	m_2-2

Table 2: For odd $n \geq 3$

S/N	Multiplicative Inverses	Equivalent Values
3	$\lvert\mu_1^{-1}\rvert\mu_2$	1
5	$\lvert\mu_2^{-1}\rvert\mu_3$	1
7	$\lvert\mu_1^{-1}\rvert\mu_3$	$\frac{m_1}{4}$
9	$\lvert(\mu_1{\mu_2}^{-1})\rvert\mu_3$	$\frac{m_1}{4}$
11	$\lvert(\mu_2{\mu_3}^{-1})\rvert\mu_1$	$m_1-\frac{m_3}{2}$
13	$\lvert(\mu_1{\mu_3}^{-1})\rvert\mu_2$	m_2-2

Table 3: For Even $n > 2$

n	Given Set	Relatively Prime New Set	$\|(\mu_1\mu_2)^{-1}\|\mu_3$
4	{6, 5, 4}	{3, 5, 4}	3
6	{10, 9, 8}	{5, 9, 8}	5
8	{14, 13, 12}	{7, 13, 12}	7
10	{18, 17, 16}	{9, 17, 16}	9
12	{22, 21, 20}	{11, 19, 18}	11
14	{26, 25, 24 }	{13, 21, 20}	13

Table 4: For odd $n \geq 3$

n	Given Set	Relatively Prime New Set (μ)	$\|(\mu_1\mu_2)^{-1}\|\mu_3$
3	{6, 5, 4}	{4, 3,1}	0
5	{10 ,9, 8}	{8, 7, 3}	2
7	{14, 13,12}	{12, 11, 5}	2
9	{18, 17,16}	{16, 15, 7}	2
11	{22, 21, 20}	{20, 19, 9}	2
13	{26, 25, 24}	{24, 23, 11}	2

Theorem 3:

Given the residue number (x_1, x_2, x_3) for the moduli set$\{m_1,m_2,m_3\}$ in the $\{2n-2, 2n-3, 2n-4\}$, then decimal equivalent X of the RNS number (x_1, x_2, x_3) for any even integer $n > 2$ can be computed as follows:

$$X = \left|\frac{m_2m_3}{2}x_1 - m_1m_3x_2 + \frac{m_1m_2}{2}x_3\right|_{M_L} \quad (13)$$

Where $M_L = \frac{m_1m_2m_3}{2}$

3.2 Computation Without Modulo Operation

Given the RNS number (x_1, x_2, x_3) for the moduli set$\{2n-2, 2n-3, 2n-4\}$ which shares a common factor of 2 between $m_1$and m_3, the proposed algorithm calculates the decimal equivalent of an RNS number using a simplified version of the CRT stated in equation (2) as shown. Sets of relatively prime moduli sets are selected for the moduli set for $n > 2$ being even and odd. As given by (Ahmad et al., 1999) the moduli set $\{2n-2, 2n-3, 2n-4\}$ with a common factor of 2 can be mapped to a set of relatively prime moduli set,$\{u_i\}_{i=1,3}$ given by;

1. $\{m_1, m_2, m_3\}=\{\frac{m_1}{2}, m_2, m_3\}$

   $=\{n-1, 2n-3, 2n-4\}$, when n is even , $n > 2$

2. $\{m_1, m_2, m_3\}=\{m_1, m_2, \frac{m_3}{2}\}$

   $=\{2n-2, 2n-3, n-2\}$, when n is odd, $n \geq 3$

Note that, the conditions ($n > 2$) and ($n \geq 3$) are very important as it is based on it that (μ_i>1) and $\propto_i$ exists.

Case 1:

For n> 2 even,

$\{2n-2, 2n-3, 2n-4\}$will have a relatively prime moduli set $\{\frac{m_1}{2}, m_2, m_3\}$.

Thus $\{\frac{2n-2}{2}, 2n-3 , 2n-4\}= \{n-1, 2n-3 , 2n-4\}$

Case 2:

For n > 2 odd,

$\{2n-2, 2n-3, 2n-4\}$will have a relatively prime moduli set $\{m_1, m_2, \frac{m_3}{2}\}$.

Thus; $\{2n-2, 2n-3 , \frac{2n-4}{2}\}= \{2n-2, 2n-3, n-2\}$

Theorem 4:

Given the moduli set $\{2n-2, 2n-3, 2n-4\}$ for $n > 2$ being even,

Thus $\{m_1, m_2, m_3\}= \{2n-2, 2n-3, 2n-4\}$, it implies $m_1 = 2n-2,\ m_2 = 2n-3\ and\quad m_3 = 2n-4$. There exists a compact form of multiplicative inverses for any even integer n > 2 as follows:

$$\left|\left(\frac{m_1}{2} m_2\right)^{-1}\right|_{m_3} = n+2 \tag{14}$$

$$|(m_2 m_3)^{-1}|_{\frac{m_1}{2}} = \frac{n}{2} \tag{15}$$

$$\left|\left(\frac{m_1}{2}m_3\right)^{-1}\right|_{m_2} = n-2 \tag{16}$$

Proof:

If we can show that $\left|(n+2)*\left(\frac{m_1}{2}m_2\right)^{-1}\right|_{m_3} = 1$, then $(n+2)$ is the multiplicative inverse of $(\frac{m_1}{2}m_2)$ with respect to m_3.

$$\left|(n+2)*\left(\frac{m_1}{2}m_2\right)^{-1}\right|_{m_3} = 1$$

$$\left|(n+2)*\left(\ 2n^2-n\right)\right|_{2n-2} = 1$$

$$|2n^3-n^2+4n^2-2n|_{2n-2} = 1$$

$$1 = 1$$

Thus equation (12) holds true.

Similarly, if we can show that $\left|(\frac{n}{2})*(m_2m_3)^{-1}\right|_{\frac{m_1}{2}} = 1$, then $(\frac{n}{2})$ is the multiplicative inverse of (m_2m_3) with respect to $\frac{m_1}{2}$.

$$\left|(\frac{n}{2})*(m_2m_3)^{-1}\right|_{m_3} = 1$$

$$\left|\left(\frac{n}{2}\right)*\left(\ 2n-1\right)*(2n-2)\right|_{n} = 1$$

$$\left|\left(\frac{n}{2}\right)*(4n^2-6n+2)\right|_{n} = 1$$

$$0-0+1 = 1$$

$$1 = 1$$

Thus equation (13) holds true.

Again, If it can be shown that $\left|(n-1)*\left(\frac{m_1}{2}m_3\right)^{-1}\right|_{m_2} = 1$, then $(n-1)$ is the multiplicative inverse of $(\frac{m_1}{2}m_3)$ with respect to m_2.

$$\left|(n-1)*\left(\frac{m_1}{2}m_3\right)^{-1}\right|_{m_2} = 1$$

$$\left|(n-1)*\left(\ 2n^2-2n\right)\right|_{2n-1} = 1$$

$$1+0 = 1;$$

$$1 = 1$$

Thus equation (14) holds true.

Theorem 5:

Given the moduli set $\{2n, 2n-1, 2n-2\}$, for $n > 2$ being odd,

Thus $\{m_1, m_2, m_3\} = \{2n, 2n-1, 2n-2\}$, it implies $m_1 = 2n,\ m_2 = 2n-1,\ m_3 = 2n-2$. There exists a compact form of multiplicative inverses for any even integer n > 2 as follows:

$$|(m_1 m_2)^{-1}|_{\frac{m_3}{2}} = n - 1 \tag{17}$$

$$\left|\left(m_2 \frac{m_3}{2}\right)^{-1}\right|_{m_1} = 2n + 1 \tag{18}$$

$$\left|\left(m_1 \frac{m_3}{2}\right)^{-1}\right|_{m_2} = 2n - 2 \tag{19}$$

Proof:

If we can show that $|(n-1) * (m_1 m_2)^{-1}|_{\frac{m_3}{2}} = 1$, then $(n-1)$ is the multiplicative inverse of $(m_1 m_2)$ with respect to $\frac{m_3}{2}$.

$$|(n-1) * (m_1 m_2)^{-1}|_{m_3} = 1$$

$$\left|(n-1) * \left(\ 4n^2 - 2n\right)\right|_{n-1} = 1$$

$$0 + |2n(n+1)|_{n-1} = 1$$

$$1 = 1$$

Thus equation (17) holds true.

Similarly, if we can show that $\left|(2n+1) * \left(m_2 \frac{m_3}{2}\right)^{-1}\right|_{m_1} = 1$, then $(2n+1)$ is the multiplicative inverse of $(m_2 \frac{m_3}{2})$ with respect to m_1.

$$\left|(2n+1) * \left(m_2 \frac{m_3}{2}\right)^{-1}\right|_{m_1} = 1$$

$$\left|(2n+1) * \left(\ 2n-1\right) * (n-1)\right|_{2n} = 1$$

$$|(2n+1) * (2n^2 - 2n - n + 1)|_{2n} = 1$$

$$0 - 0 - 0 + 1 = 1$$

$$1 = 1$$

Thus equation (18) holds true

Again, If it can be shown that $\left|(2n-2) * \left(m_1 \frac{m_3}{2}\right)^{-1}\right|_{m_2} = 1$, then $(2n-2)$ is the multiplicative inverse of $\left(m_1 \frac{m_3}{2}\right)$ with respect to m_2.

$$\left|(2n-2) * \left(m_1 \frac{m_3}{2}\right)^{-1}\right|_{m_2} = 1$$

$$\left|(2n-2) * \left(\ \ 2n * (n-1)\right)\right|_{2n-1} = 1$$

$$|2n^3 - 4n(2n-1)|_{2n-1} = 1$$

$$1 + 0 = 1;$$

$$1 = 1$$

Thus equation (19) holds true.

Theorem 6:

Given the moduli set $\{2n - 2, 2n - 3, 2n - 4\}$

$X = \{2n(2n+1)nx_1 + (2n-1)(2n+1)(2n-1)x_2 + (2n-1)2n(n+1)x_3\}(2n-1)2n(2n+1)$ (20)

Given that $x_1 + x_3$ is even;

$X = |n(2n+1)x_1 - (2n-1)(2n+1)x_2 + n(2n-1)x_3|(2n-1)2n(2n+1)$ (21)

$$X = \left|\frac{p1}{2}(P_3)x_1 - (p_2)(p_3)x_2 + \frac{p1}{2}(P_2)x_3\right| M$$

Else;

$X = |(2n-1)n(2n+1) + n(2n+1)x_1 - (2n-1)(2n+1)x_2 + n(2n-1)x_3|\, M$ (22)

$$X = \left|(p_2)\left(\frac{p1}{2}\right)(P_3) + \frac{p1}{2}(p_3)x_1 - (p_2)(p_3)x_2 + \frac{p1}{2}(2n-1)x_3\right| M$$

From (Prenkumar, 1995)

If $x_1 + x_3$ even; then for $(2n, 2n + 1, 2n + 2)$

$X = |(n+1)(2n+1)x_1 - (2n+1)2nx_2 + n(2n+1)x_3|2n(2n+1)(n+1)$ (23)

$$X = \left|\left(\frac{p3}{2}\right)(P_2)x_1 + (p_3)(p_1)x_2 + \frac{p1}{2}(p_2)x_3\right| p_1p_2p_{\frac{3}{2}}$$

Else;

$X = |n(2n+1)(n+1) + (n+1)(2n+1)x_1 - n(2n+2)2nx_3 + \mathrm{n}(2\mathrm{n}+1)x_3|2n(2n-1)(n+1)$

$$X = \left|\frac{p1}{2}(P_2)\left(p_{\frac{3}{2}}\right) + p_{\frac{3}{2}}(p_2)x_1 - (p_3)p_1x_2 + \frac{p1}{2}(p_2)x_3\right| p_1p_2p_{\frac{3}{2}} \quad (24)$$

3.1 Proposed Converter

The proposed converter seeks to reduce the hardware size than the converter presented by (Premkumar, 1995). To achieve this, fewer multipliers are used.

Proposition 2:

$\left(\frac{a}{2}\right) + b = \left(\frac{a+2b}{2}\right)$ where a and b are integers

Proof:

$$a = 2 * \left(\frac{a}{2}\right) + a_{0,}$$

$$a + 2b = 2 * \left(\frac{a}{2}\right) + a_0 + 2b$$

$$= 2 * \left(\left(\frac{a}{2}\right) + b\right) + a_{0,}$$

Proposition 3:

Given the moduli set $\{2n - 2, 2n - 3, 2n - 4\}$, the number X represented by $(x_1, x_{2,}x_3)$ can be computed by the following formula;

$$X = x_2 + p_2\left\{(x_2 - x_3) + (x_1 - 2x_2 + x_3)\frac{p2}{2}(p_3)\right\}p_1p_3 \quad (25)$$

Proof:

First let;

$$X = \left\{\begin{matrix} x_2 + p_2(x_2 - x_3) + \\ (x_1 - 2x_2 + x_3)\frac{p2}{2} * (p_2)(p_3) \end{matrix}\right\}p_2p_1p_3 \quad (26)$$

It is easy to see that $Xmodp_2 = x_{2,}$ and $\frac{p2}{2}(p_3)\text{mod}\, p_1 = 1$,

$$Xmod(p_1) = x_{2,} + (x_2 - x_3) + (x_1 - 2x_2 + x_3) = x_1$$

$$Xmod(p_3) = x_{2,} - (x_2 - x_3) = x_3$$

Therefore, there exists a number m such that

$$0 \leq X < M = p_2p_1p_3$$

$$X = \{x_2 + p_2(x_2 - x_3) + (x_1 - 2x_2 + x_3)\frac{p2}{2} * (p_2)(p_3)\} + m * p_2p_1p_3$$

$$= x_2 + p_2\left\{(x_2 - x_3) + (x_1 - 2x_2 + x_3)\frac{p2}{2} * (p_3)\right\} + m(p_1)(p_3)$$

Since $0 \leq X < p_2p_1p_3$ and $0 \leq x_2 < p_2$, we have

$$0 \leq (x_2 - x_3) + (x_1 - 2x_2 + x_3)\frac{p2}{2} * (p_3) + m(p_1)(p_3) < (p_1)(p_3)$$

Which implies formula (8).

Corollary:

X can be computed by the use of the formula;

$$X = x_2 + p_1\{\left[\frac{(x_1 - x_3) + 2z_0\frac{p1}{2}}{2}\right] + \left[\frac{(x_1 + x_2 + x_3) + 2z_0\frac{p1}{2}}{2}\right]\}p_2p_3 \quad (27)$$

$$X = x_2 + (2n-2)\{\left[\frac{(x_1 - x_3) + 2z_0(n-1)}{2}\right] + (2n-2)[(x_1 - 2x_2 + x_3) + 2z_0(n-1)]\}p_2p_3$$

Since $(x_1 - 2x_2 + x_3) = 2 * \left[\frac{(x_1 + x_2 + x_3)}{2}\right] + (x_1 - 2x_2 + x_3)_2$ comparing with Proof shown,

we denote $(x_1 - 2x_2 + x_3)_2 = (x_{10} + x_{30}) = z_0$

$\left[\frac{(x_1 - 2x_2 + x_3)}{2}\right] = z$, therefore we have

$$X = x_2 + (2n-2)\{(x_2 - x_3) + (x_1 - 2x_2 + x_3)(n-1) * (2n-4)\}(2n-3)(2n-4)$$

$$= x_2 + (2n-2)\left\{(x_2 - x_3) + \left[\frac{(x_1 - 2x_2 + x_3)}{2}\right](2n-2)(2n-4) + z_0(n-1)(2n-4)\right\}(2n-3)(2n-4) \quad (28)$$

IV Hardware Implementation

In this section, the paper implements the proposed hardware design for the converter by mainly using carry save adders, multipliers and a modular adder.

The formula;

$X = \{x_2 + (x_2 - x_3)(2n-1) + (x_1 - 2x_2 + x_3)(n)\}_{4(n)}$ can be represented by;

$$Y_{11} = \left\lfloor\frac{(x_1 - x_3) + 2z_0n}{2}\right\rfloor, Y_{12} = \left\lfloor\frac{(x_1 - 2x_2 + x_3) + 2z_0n}{2}\right\rfloor,$$

$Y_{21} = (x_2 - x_3), Y_{22} = (x_1 - 2x_2 + x_3)$

We let $c_{11} = c_{12} = 4$, $c_{21} = (2n-1)c_{22} = n$ and $M_i = (4)(n)$

We can then write X as shown;

$X = x_2 + c_{i1}(Y_{i1} + c_{i2}Y_{i2})_{M_i}$ for $i = 1\ or\ 2$

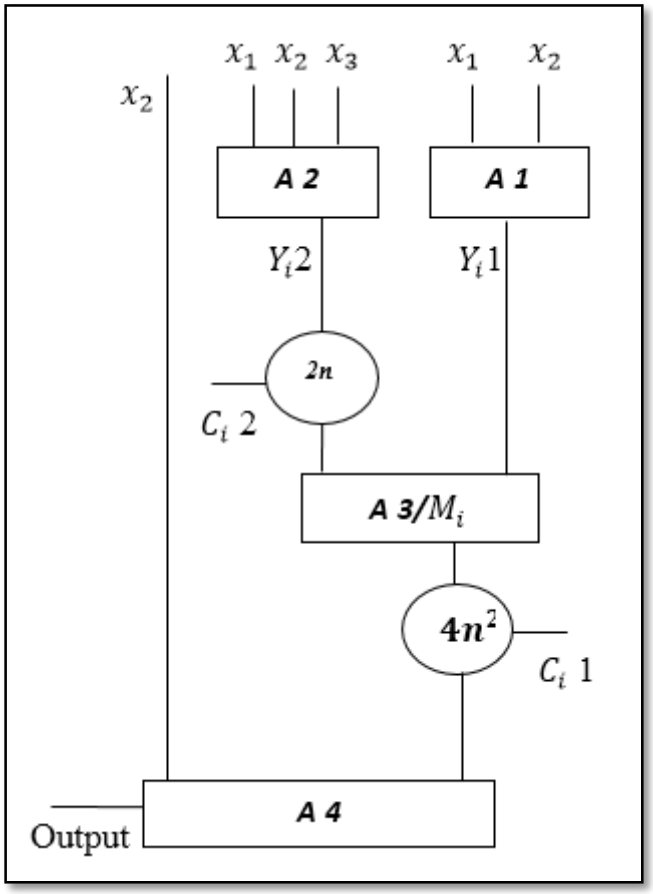

Figure 1: Architecture for the Proposed Scheme

From figure 1, the two circles represent multipliers of ranges $2n\ and\ 4n^2$ respectively whiles $\boldsymbol{A1}\ and\ A\ \mathbf{2}$ are adder/subtractor units to generate the values of Y_i1 and Y_i2. The $\boldsymbol{A}\ \mathbf{3}$ unit is a modulo M adder and $\boldsymbol{A4}$ is a normal adder unit.

Table 5: Comparison with some Proposed Converter.

	Proposed Converter	**Converter (Premkumar, 1995)**

No. of Adder units	$3 * 2n + M$ $(4\ adders)$	$2n + M$ $(2\ adders)$
No. of Multipliers	$2n + 4n^2$ $(2\ multipliers)$	$3 * 4n^2$ $(3\ multipliers)$

The hardware sum of the Adders $\boldsymbol{A\ 1}$ *and* $\boldsymbol{A\ 2}$ and the multiplier of range $\boldsymbol{2n}$ is less than 2 multipliers of range $\boldsymbol{2n}$. That is if $\boldsymbol{2n}$ takes $\boldsymbol{r}$ bits, then $\boldsymbol{4n^2}$will take $2\boldsymbol{r}$ bits.

Therefore, in terms of hardware size, the new converter is much smaller than the one proposed in (Premkumar, 1995) because of the fewer multipliers used since adders are much smaller that multipliers.

V. CONCLUSION

This paper proposes a new converter for the special moduli set $\{2n-2, 2n-3, 2n-4\}$ sharing a common factor of 2. The proposed converter is more efficient and smaller in hardware size than the converter presented in (Premkumar, 1995). The converter reduces cost of implementation and improves on the speed gain of earlier converter in (Premkumar, 1995).

REFERENCES

[1] Abdelfattah, (2011) "Data Conversion in Residue Number System". McGill University. Balanced moduli sets and enhanced modular arithmetic structures". Computers &Digital Techniques.

[2] Chaves, R., and Sousa, L. (2007) "Improving residue number system multiplication with more

[3] Circuits & Communication.

[4] Gbolagade, K. A. and Cotofana, S.D. (2008). MRC Techniques for RNS to Decimal Conversion Using the Moduli set $\{2n+2, 2n+1, 2n\}$. Proceedings of the 16th Annual Workshop on Circuits, Systems and Signal processing, Veldhoven, the Netherlands.

[5] Gbolagade, K. A. and Cotofana, S.D. (2009a). Residue-to-Decimal Converters for Moduli Sets with Common Factors. IEEE, Pp.624-627, 2009.

[6] Gbolagade, K. A. and Cotofana, S.D. (2009b). A Reverse Converter for the new 4 –Moduli set $\{2n+3, 2n+2, 2n+1, 2n\}$. Submitted to IEEE Newcastaisa Toulouse, France. July, 2009. IET, Volume 1, Issue 5, pages 472-480.

[7] Premkumar, A.B., (1992). "An RNS to Binary converter in $\{2n+l, 2n, 2n-1\}$moduli set", IEEE Transactions on Circuits and Systems - I1 Vol. 39, No. 7, pp. 480-482.

[8] Premkumar, A.B., (1995). "An RNS to Binary converter in a three moduli set with common factors", IEEE Transactions on Circuits and Systems -11, Vol. 42, No. 4, pp. 298-301.