International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 12 | Dec. 2018 www.irjet.net p-ISSN: 2395-0072

AN EFFICIENT REVERSE CONVERTER FOR THE THREE NON-COPRIME MODULI SET $\{4, 2n-1, 2n\}$

Valentine, Aveyom[1], Mohammed, .I., Daabo (PhD)[2], Abdul-Barik, Alhassan (PhD)[3]

[1]Tutor, Notre Dame Seminary SHS, Box 10, Navrongo.
[2]HOD, Computer Science Department, University for Development Studies, Navrongo.
[3]Senior Lecturer, Computer Science Department, University for Studies, Navrongo.

Abstract - *In this paper, residue to binary conversion is discussed for the three moduli set $\{4, 2n-1, 2n\}$ sharing a common factor. A new and efficient converter for the moduli set is proposed. Larger multipliers in (Premkumar, 1995) are replaced by smaller multipliers and adders reducing the hardware required by the proposed converter. The hardware implementation and comparison with other state-of- the- art schemes shows that the proposed scheme performed better.*

Key Words: **Residue Number System(RNS), Chinese Remainder Theorem (CRT), Mixed Radix Conversion (MRC), Reverse Conversion, Non coprime Moduli set.**

1. INTRODUCTION

Residue Number Systems (RNS) are considered suitable for the implementation of high-speed digital signal processing devices due to their inherent parallelism, modularity, fault tolerance and localized carry propagation properties (Garner, 1959). Some arithmetic operations, such as addition and multiplication, can be carried out more efficiently in RNS than in conventional two's complement systems.

The traditional moduli set $\{2^n+1,\ 2^n,\ 2^n-1\}$ has been one of the most popular studied in RNS. However, these moduli set does not offer some of the advantages that moduli sets with common factors offer such as consecutiveness and ability to allow for equal width adders and multipliers. The moduli set $\{4, 2n-1, 2n\}$ which shares a common factor of 2 is therefore of study significance since it offers these advantages. It however, will have a limitation in high performance Digital Signal Processing (DSP) applications as it has a smaller dynamic range.

2. FUNDAMENTALS OF RESIDUE NUMBER SYSTEM (RNS)

RNS is defined in terms of a set of relatively prime moduli set $\{m_i\}_{i=1,k}$ such that the *greatest common divisoor*(gcd) $(m_i, m_j) = 1$ for $i \neq j$, where gcd means the greatest common divisor (gcd) 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 $X = (x_1, x_2, x_3, \dots, x_k)$, $0 \leq x_i \leq m_i$. 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 $(x_1, x_2, \dots, x_n)$ of the moduli set $\{m_1, m_2, \dots, m_n\}$ to its decimal number (X) as follows;

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

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

Where,

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

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

(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. This method also used to perform `residue to binary conversion of (x_1, x_2, x_3) based on the moduli set $\{m_1, m_2, \dots m_3\}$ as follows;

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

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

$$a_1 = x_1$$

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

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

⋮

$$a_k = \left|\left((x_k - a_1)|m_1^{-1}|_{m_k} - a_2\right)|m_2^{-1}|_{m_k} - \ldots - a_{k-1}\right)|m_{k-1}^{-1}|_{m_k}\Big|_{m_k}$$

(Gbolagade et al, 2008).

2.3 Revised CRT for Moduli Set with Common Factors

The revised CRT which is used for moduli set with factors is stated as;

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

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 $|\propto_i|_{\mu_1}$=1and $\{\mu_i\}_{i=1,K}$ 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.

3. PROPOSED CONVERSION TECHNIQUES

Two conversion methods are discussed by the paper. These are m_3-Modulus Conversion Technique and 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;

$$X = (x_1 + x_2) + m_1 m_2 |k_1 x_1 + k_2 x_2 + m_3^{-1}|m_3 x_3|_{m_3} \quad (3)$$

Where; m_3^{-1} is the multiplication inverse of m_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 values involved in the computation.

Proof:

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

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

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

Lemma 3: $|m_2|M_2^{-1}|_{m_2} = 1 + k_2 m_1 m_2$ where k is

Expanding equation (1) for $k = 3$ gives;

$$X = |m_1|M_1^{-1}|_{m_1} x_1 + m_2|M_2^{-1}|_{m_2} x_2 + m_3|M_3^{-1}|_{m_3} x_3|_{m_1 m_2 m_3} \qquad (4)$$

Putting Lemmas 2 and 3 into equation (4) results in;

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

Simplifying further yields;

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

Thus applying Lemma 1, gives;

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

Here $m_3^* = \frac{m_3}{m_1 m_2} = 1$, the above equation reduces to the form:

$$X = (x_1 + x_2) + m_1 m_2 |k_1 x_1 + k_2 x_2 + |M_3^{-1}|_{m_3} x_3|_{m_3} \qquad (8)$$

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 $\{m_i\}$ $for\ i = 1,3$ 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;

$$|X|_{M_L} = \sum_{i=1}^{k} \beta_i |\beta_i^{-1}| \quad (9)$$

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 (9) to equation (2) 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 (9)

It can then be shown 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 (9) is a more formal way of representing equation (2).

To perform reverse conversion using equation (3) 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 $\{4, 2n-1, 2n\}$ 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. $\{m_1, m_2, m_3\} = \{\frac{m_1}{2}, m_2, m_3\}$

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

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

   $= \{4, 2n-1, n\}$, when n is odd and $n \geq 3$

Note that, the conditions $(n > 2)$ and $(n \geq 3)$ are very important as it is based on them that $(\mu_i > 1)$ 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 $(x_1 x_2 x_3)$ 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 $\{4, 2n-1, 2n\}$ into Theorem 1, gives;

Corollary 1: For the moduli set $\{4, 2n-1, 2n\}$ 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;

$$X = (x_1 + x_2) + \frac{m_1 m_2}{2} k_1 x_1 + k_2 x_2 + \frac{m_1}{2} x_3 | m_3 \quad (10)$$

Where;

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

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

2. If n is odd:

$$X = (x_1 + x_2) + m_1 m_2 | k_1 x_1 + k_2 x_2 + \frac{m_1}{4} x_3 | \frac{m_3}{2}) \quad (11)$$

Where $k_1 = \frac{[\frac{m_2 m_3}{2}(m_1 - \frac{m_3}{2})-1]}{(m_1 m_2)}$ and $k_2 = \frac{[\frac{m_1 m_3}{2}(m_2-2)-1]}{m_1 m_2}$

Table -1: For even $n > 2$

n	Multiplicative Inverses	Equivalent Values
1	$\|\mu_1^{-1}\|\mu_2$	2
2	$\|\mu_2^{-1}\|\mu_3$	1
3	$\|\mu_1^{-1}\|\mu_3$	$\frac{m_1}{2}$
4	$\|(\mu_1\mu_2)^{-1}\|\mu_3$	$\frac{m_1}{2}$
5	$\|(\mu_2\mu_3)^{-1}\|\mu_1$	$\frac{m_3}{4}+1$
6	$\|(\mu_1\mu_3)^{-1}\|\mu_2$	$m_2 - 2$

Table -2: For odd $n > 2$

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

Table -3: For even $n > 2$

n	Multiplicative Inverses	Equivalent Values
4	{4, 7, 8}	{2, 7, 8}
6	{4, 11, 12}	{2, 11, 12}
8	{4, 15, 16}	{2, 15, 16}
10	{4, 19, 20}	{2, 19, 20}
12	{4, 23, 24}	{2, 23, 24}
14	{4, 27, 28}	{2, 27, 28}

Table 4: For odd $n \geq 3$

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

3.2 Computation Without Modulo Operation

Given the Residue Number System (RNS) number (x_1, x_2, x_3) for the moduli set $\{4, 2n-1, 2n\}$ 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 $\{4, 2n-1, 2n\}$ 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. $\{m_1, m_2, m_3\} = \{\frac{m_1}{2}, m_2, m_3\}$
   $= \{2, 2n-1, 2n\}$, when n is even , $n > 2$
2. $\{m_1, m_2, m_3\} = \{m_1, m_2, \frac{m_3}{2}\}$
   $= \{4, 2n-1, n\}$, 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 $(\mu_i > 1)$ and $\propto_i$ exists.

Case 1: For $n > 2$ even,

$\{4, 2n-1, 2n\}$ will have a relatively prime moduli set $\{\frac{m_1}{2}, m_2, m_3\}$.

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

Case 2: For $n \geq 3$ odd,

$\{4, 2n-1, 2n\}$ will have a relatively prime moduli set $\{m_1, m_2, \frac{m_3}{2}\}$.

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

Theorem 3:

Given the moduli set $\{4, 2n-1, 2n\}$ for $n > 2$ being even,

Thus $\{m_1, m_2, m_3\} = \{4, 2n-1, 2n\}$, implying $m_1 = 4$, $m_2 = 2n-1$, $m_3 = 2n$. There exists a compact form of multiplicative inverses for any even integer n > 2 as follows:

$$\left|\left(\frac{m_1}{2} m_2\right)^{-1}\right|_{m_3} = n - \frac{1}{2} \qquad (12)$$

$$|(m_2 m_3)^{-1}|_{\frac{m_1}{2}} = 2n - \frac{1}{2n} \qquad (13)$$

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

Proof:

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

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

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

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

$$0+0+1=1$$

$$1=1$$

Thus equation (12) holds true.

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

$$\left|(2n-\frac{1}{2n})*(m_2m_3)^{-1}\right|_{\frac{m_1}{2}}=1$$

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

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

$$0-0+1=1$$

$$1=1$$

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.

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

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

$$0+1=1$$

$$1=1$$

Thus equation (14) holds true.

Theorem 4:

Given the moduli set $\{4, 2n-1, 2n\}$ for $n>2$ being odd,

Thus; $\{m_1,m_2,m_3\}=\{4, 2n-1, 2n\}$, it implies $m_1=4,\ m_2=2n-1,\ m_3=2n$. There exists a compact form of multiplicative inverses for any even integer n > 2 as follows:

$$|(m_1m_2)^{-1}|_{\frac{m_3}{2}}=n-\frac{1}{4} \qquad (15)$$

$$\left|\left(m_2\frac{m_3}{2}\right)^{-1}\right|_{m_1}=4n-\frac{1}{n} \qquad (16)$$

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

Proof:

If we can show that $|(n-1)*(m_1m_2)^{-1}|_{\frac{m_3}{2}}=1$, then $(n-1)$ is the multiplicative inverse of (m_1m_2) with respect to $\frac{m_3}{2}$.

$$\left|(n-\frac{1}{4})*(m_1m_2)^{-1}\right|_{\frac{m_3}{2}}=1$$

$$\left|(n-\frac{1}{4})*\left(\ 8n-4\right)\right|_{n}=1$$

$$|8n^2-4n-2n+1|_{n}=1$$

$$0-0+1=1$$

$$1=1$$

Thus equation (15) holds true.

Similarly, if we can show that $\left|(4n-\frac{1}{n})*\left(m_2\frac{m_3}{2}\right)^{-1}\right|_{m_1}=1$, then $(4n-\frac{1}{n})$ is the multiplicative inverse of $(m_2\frac{m_3}{2})$ with respect to m_1.

$$\left|(4n-\frac{1}{n})*\left(m_2\frac{m_3}{2}\right)^{-1}\right|_{m_1}=1$$

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

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

$|8n^3 - 4n^2 - 2n + 1|_4 = 1$

$0 - 0 + 1 = 1$

$1 = 1$

Thus equation (16) 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.

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

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

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

$1 + 0 = 1;$

$1 = 1$

Thus equation (17) holds true.

Proposed Converter

Using the Chinese Remainder Theorem (CRT) on the selected moduli set $\{P_1, P_2, P_3\} = \{4, 2n-1, 2n\}$ X is defined as follows;

$$X = \{(2n-1)(2n)[(n-1)x_1]_4 + (4)(2n)[(4)x_2]_{2n-1} + (4(2n-1)[(n)x_3]_{2n}\}_{(4)(2n-1)(2n)} \quad (18)$$

The CRT cannot directly be used since the selected moduli set shares a common factor. We therefore adopt the following relations from (Premkumar, 1995) using the weight concept.

Given that; $x_1 + x_3$ is even, then

$$X = \left|\begin{matrix}(n)(2n+1)x_1 - (2n)(4)x_2 + \\ (2)\ (2n+1)x_3\end{matrix}\right|_{(4)(2n-1)(n)} \quad (19)$$

For $x_1 + x_3$ not being even, then

$$X = |(2)(2n+1)(n) + (n)(2n+1)x_1 - (2n)(4)x_2 + (4)(2n+1)x_3|_{(4)(2n-1)(n)} \quad (20)$$

Proposition 1

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

An RNS number X for the moduli set $(P_1, P_2, P_3) = \{4, 2n-1, 2n\}$ represented by (x_1, x_2, x_3). the integer X will represent a valid number if and only if $x_1 + x_3$ is even and can be computed by the following formula;

$$X = x_2 + (2n-1)\{(x_2 - x_3) + (x_1 - 2x_2 + x_3)(n)\}_{4(n)} \quad (21)$$

Proof

The prove is done by showing that if (x_1, x_2, x_3) represents a valid number, then $x_1 + x_3$ is even. There exist some k_1 *and* k_2 such that $x_1 = X + k_1 * 4$, $x_3 = X + k_2 * (2n)$. Therefore $x_1 + x_3 = 2X + k_1 * 4 + k_2 * (2n)$, which must be even.

If $x_1 + x_3$ is not even, then (x_1, x_2, x_3) does not represent a valid RNS number and should not be decoded.

Consider
$X = |(n)(2n+1)x_1 - (2n)(4)x_2 + (2)(2n+1)x_3|_{(4)(2n-1)(n)}$
being even. It is easy to see that $X mod(2n+1) = x_2$, $X mod(2n) = x_2 - (x_2 - x_3) = x_3$

Since $(2n) mod 4 = 2$, therefore $X mod 4 = x_2 + (x_2 - x_3) + \frac{(x_1 - 2x_2 + x_3) * 2}{2} = x_1$

Therefore;

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

Which implies that, there exists a number m such that $0 \le X < (4)(2n-1)(n)$ and

$$X = x_2 + (x_2 - x_3)(2n-1) + (x_1 - 2x_2 + x_3)(n)(2n-1) + m * (4)(2n-1)(n)$$

$$X = x_2 + (x_2 - x_3)(2n-1) + (x_1 - 2x_2 + x_3)(n) + m * (4)(n)$$

Where
$(x_2 - x_3)(2n-1) + (x_1 - 2x_2 + x_3)(n) + m * (4)(n)$ must be in the interval $[0, 4(2n-1)]$.

Therefore;
$X = \{x_2 + (x_2 - x_3)(2n-1) + (x_1 - 2x_2 + x_3)(n)\}_{4(n)}$
which is same as formula (21) .

4. 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;

$$Y_{11} = \left\lfloor \frac{(x_1 - x_3) + 2z_0 n}{2} \right\rfloor,$$

$$Y_{12} = \left\lfloor \frac{(x_1 - 2x_2 + x_3) + 2z_0 n}{2} \right\rfloor,$$

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

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

$M_i = (4)(n)$

X can then written as shown;

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

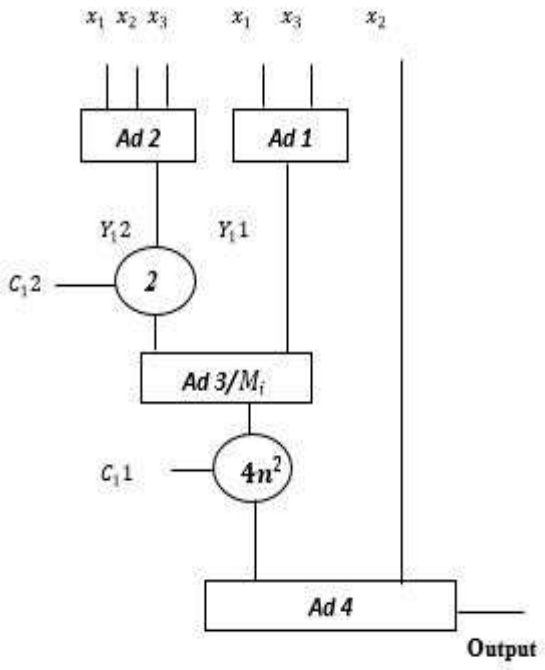

Fig -1: Architecture for the proposed Scheme

From the diagram, the two circles represent multipliers of ranges $2n$ *and* $4n^2$ respectively whiles ***Ad* 1** *and* ***Ad* 2**are adder/subtractor units to generate the values of Y_i1 and Y_i2. The ***Ad* 3**unit is a modulo M adder and ***Ad* 4**is a normal adder unit.

Table -1: Comparison with some Proposed Converter

	Proposed Converter	Converter (Premkumar , 1995)	Converter (Gbolagade. 2009)
No. of Adder units	$3 * 2n + M$ $(4\ adders)$	$2n + M$ $(2\ adders)$	*No* architecture
No. of Multiplier units	$2 + 4n^2$ $(2\ multipliers)$	$3 * 4n^2$ $(3\ multipliers)$	*No* architecture

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

5. CONCLUSION

This paper proposes a new converter for the special moduli set $\{4, 2n-1, 2n\}$ 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 converters.

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 Circuits & Communication.

[3] 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.

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

[5] 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.

[6] 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.

[7] 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.

[8] Garner, H.L. (1959). The residue Number System, IRE Trans. On Electronic Computers, pp. 140-147.

BIOGRAPHIES

Valentine Aveyom is an MSc. Computational Mathematics Student at the Faculty of Mathematical Sciences, UDS, Ghana and an ICT Tutor at Notre Dame Sem. SHS, Navrongo. He has research interest in the area of Residue Number System (RNS).

Dr. Mohammed I. Daabo is a senior lecturer in Computer Science at the Department of Computer Science, UDS, Ghana. He has over (15) years teaching experience in Tertiary Education and has conducted academic research in the fields of Overflow Detection, Reverse conversion, Error Detection, Sensor Networks and Epidemiological Modeling.

Dr. Abdul-Barik Alhassan is a senior Lecturer and Exams Officer of the Computer Science Department of UDS Ghana. He has research interest in the areas of Computer Hardware and Architecture, Residue Number System (RNS), Information Security/ Cryptography, Algorithm Design and Analysis and Statistical Computing.