Earthline Journal of Mathematical Sciences
E-ISSN: 2581-8147
Volume 14, Number 5, 2024, Pages 1159-1172
https://doi.org/10.34198/ejms.14524.11591172

A Generalized Reverse Conversion Algorithm for Six-Moduli Set

Yakubu Abdul-Wahab Nawusu[1,*], Abukari Abdul Aziz Danaa[2], Kubuga Kennedy[3] and Asiedu Daniel[1]

[1] Department of Computer Science, Tamale Technical University, Tamale, Ghana
e-mail: nabdul-wahab@tatu.edu.gh

[2] Department of Computer Science, Tamale Technical University, Tamale, Ghana
e-mail: azizdanaa@tatu.edu.gh

[3] Department of Computer Science, Tamale Technical University, Tamale, Ghana
e-mail: kkubuga@tatu.edu.gh

[4] Department of Computer Science, Tamale Technical University, Tamale, Ghana
e-mail: asiedudaniel@tatu.edu.gh

Abstract

Residue Number System has emerged as an alternative number system with advantages in many real-life systems including in digit signal processing devices. Computational systems built on residue number system require both forward and reverse conversion processes. These converters respectively convert a given integer into its corresponding residues and calculate the original integer from its residues. While forward conversion is pretty straight forward, reverse conversion poses challenges often requiring difficult procedures. Much of residue number system research has therefore been devoted to design and implementation of efficient reverse conversion algorithm. The Chinese Reminder Theorem and the Mixed-Radix Conversion are the two popular ones. The Chinese Reminder Theorem results in complex circuitry that requires difficult computation involving large modulo-M values. The Mixed-Radix Conversion offers simplicity in designs although its steps are sequential. This paper proposes a generalized reverse conversion algorithm tailored for a six-moduli set with a large dynamic range. This innovative algorithm minimises the difficult multiplicative inverse operations found in the traditional reverse conversion methods paving the way for a more efficient reverse conversion processes for systems that requires high dynamic ranges. The new algorithm has been meticulously evaluated numerically on a proposed six-moduli set $\{2^{n+1} -$

Received: March 13, 2024; Accepted: May 3, 2024; Published: August 8, 2024

2020 Mathematics Subject Classification: 68-XX.

Keywords and phrases: residue number system, moduli set, CRT, MRC, reverse conversion.

[*] Corresponding author

$1, 2^{2n}+1, 2^{2n+1}-1, 2^{3n}+1, 2^{3n+1}-1, 2^{4n}+1\}$ for even values of n, to ensure its correctness and simplicity. The approach holds great promise for enhancing the development of reverse converters allowing the expansion of the landscape of residue number system.

1. Introduction

There has been renewed interest in residue number system (RNS) over the past six decades due to its discovered beneficial features and its ability to design systems that require fast processing speed and high levels of fault tolerance. The residue number system is an alternative number system to conventional number systems such as the decimal and binary number systems that represents a given integer into a set of smaller residues by performing a modulo operation on the given integer with respect to a chosen moduli set. The residues (remainders) resulting from such operation represents the integer in the residue number system.

RNS has been successfully used in applications such as in digital filtering, convolution, communication technologies, cryptography, image and speed processing, stenographic and cryptographic methodologies, wireless sensor networks, rain fade mitigation and more [1]. The realization of RNS's widespread use especially in general-purpose computing is however challenged by a number of bottlenecks. Reverse conversion is one of the first arithmetic limitations of residue number system to be studied [2, 3]. The reverse conversion procedure is an essential block in an RNS processor which takes a given set of residues and a given set of moduli set and calculates the binary or decimal equivalent [4]. Current procedures for reverse conversion are computationally intensive. The Chinese Remainder Theorem (CRT) for instance rely on the use of a large Modulo-M during the conversion process adding to its computational load. Similarly, the Mixed Radix Conversion (MRC) is time consuming because of its sequential computational process, which could additionally lead to error propagation from one mixed radix digit to another [5, 6]. These challenges militate against the seamless integration of RNS for digital processor technologies [7]. Consequently, there is the need to develop RNS reverse converters that offers efficient RNS processors to address the computational burdens associated with existing methods.

This paper extends the algorithm proposed in [7] by presenting a reverse conversion algorithm for a six-moduli set. The algorithm particularly delves into dealing with the complexity that arise when performing reverse conversion using the Chinese Remainder

Theorem (CRT) which requires large Modulo-M operations as well as the sequential processing steps characteristic of the Mixed Radix Conversion (MRC) technique. The paper also proposes a six-moduli set, $\{2^{n+1}-1, 2^{2n}+1, 2^{2n+1}-1, 2^{3n}+1, 2^{3n+1}-1, 2^{4n}+1\}$ with a larger dynamic range than those presented in [7] and [8]. This ensures that the resulting RNS implementation is able to handle a large range of numbers.

2. The Concept of Residue Number System

The idea of residue number system first appeared in the ancient manuscript of Sun Tzu [9, 10]. Its practical use however gained momentum in the 1950s emerging as a viable number system number system for applications requiring fast processing and for fault-tolerant operations [11]. In the residue number system, numbers are encoded as small residues relative to a given set of co-prime numbers. RNS's boost of many inherent features making it advantageous for specialized computational tasks. Notably, the lack of carry propagation, enables addition and multiplication in RNS to be done without need for inter-digits interactions. This feature results in fast arithmetic operations than in conventional numbers systems [1]. Additionally, there is the lack of error propagation from one residue position to another making it suitable for identifying and correcting errors in digital processing devices [1, 11-13] and many others.

Mathematically, a residue number system is defined by a set of co-prime integers known as moduli set. A moduli set is defined by the set $\{m_1, m_2, \ldots, m_n\}, i = 1, \ldots, n$, such that $GCD(m_i, m_j) = 1$, for $i \neq j$, where $GCD(m_i, m_j)$ denotes the greatest common divisor of m_i and m_j. An integer in an RNS can therefore be encoded as a set of residues denoted as $\{x_1, x_2, \ldots, x_n\}$, where x_i is the ith residue derived from Equation (1)

$$x_i = X \, mod \, m_i. \tag{1}$$

The residues of the integer, 17 with respect to the moduli set $\{7, 15, 16, 17, 31\}$, will be $\{3, 2, 1, 0, 14\}$ using Equation (1).

The dynamic range of a given RNS defines the representable range of all legitimate integers [14]. The dynamic range of the moduli set $\{m_1, m_2, \ldots, m_n\}, i = 1, \ldots, n$, is given in Equation (2). It ensures the valid representation of all positive numbers between 0 and $M-1$ in the given RNS.

$$M = \prod_{i=1}^{n} m_i. \tag{2}$$

An RNS processor is shown in Figure 1.

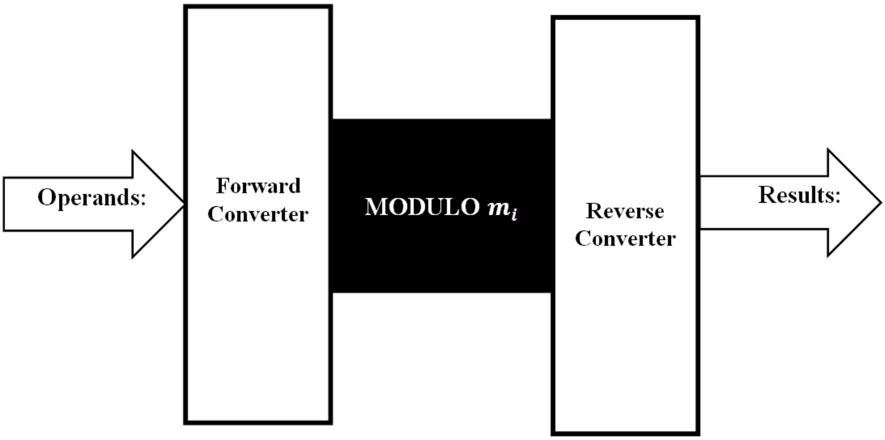

Figure 1. The general makeup of an RNS processor [4].

The function of the RNS processor is in two-folds. At the forepart, the forward converter takes a number (either in binary or decimal) and converts it into its equivalent residues. At the opposite end, a reverse converter takes the residues and computes the original integer value relative to a chosen moduli set. The forward conversion is often simple compared with the reverse conversion which requires complicated computation steps. There are numerous reverse conversion techniques, popular of which are the Chinese Remainder Theorem and the Mixed Radix Conversion [7, 8, 5].

3. Related Algorithms

Numerous RNS research endeavors have been dedicated to reverse conversion methodologies. In the following section, we present the reverse conversion algorithms that bear relevance to the algorithm presented in this paper.

3.1. The Chinese Remainder Theorem

Definition 1. Given the moduli set $\{m_i\}_{i\,=\,1,\ldots,n}$, a legitimate integer, X can be calculated from its residues set $\{x_1, x_2, \ldots, x_k\}$, using the CRT (Agbedemnab et al. [15]) as follows:

$$X = \left| \sum_{i=1}^{n} x_i \left| M_i^{-1} \right|_{m_i} M_i \right|_M \tag{3}$$

M is the dynamic range computed as in Equation (2), M_i^{-1} is the multiplicative inverse of M_i with respect to m_i. Each M_i is computed as $\frac{M}{m_i}$.

3.2. The Mixed Radix Conversion

The Mixed Radix Conversion is a reverse conversion technique in RNS which sequentially determines a decimal number from its residues and a set of moduli [4]

Definition 2. Given the moduli set $\{m_i\}_{i=1,\ldots,n}$, a legitimate integer, X can be determined from its residues set $\{x_1, x_2, \ldots, x_k\}$, using the MRC [15] as follows:

$$X = a_1 + a_2 m_1 + a_3 m_1 m_2 + \cdots + a_k m_1 m_2 m_3 \ldots . m_{k-1}, \tag{4}$$

where $\{a_i\}_{i=1,\ldots,n}$, are the mixed radix digits sequentially computed using the Equations below:

$$a_1 = x_1,$$

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

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

$$\vdots$$

$$a_n = \left|((((((x_n - a_1)|m_n^{-1}|_{m_n}) - a_2)\left|m_2^{-1}\right|_{m_n})) \ldots - a_{n-1})\left|m_{n-1}^{-1}\right|_{m_n}\right|_{m_n}. \tag{5}$$

3.3. The Algorithm in Salifu [7] and Asiedu and Salifu [8]

The proposed reverse conversion algorithm in this paper is motivated by the contributions of [7] as well as in [8]. Salifu in [7] presented a reverse conversion technique for both four-moduli set and five-moduli set extending the groundwork laid by Asiedu and Salifu in [8]. The initial concept was introduced by [8] with a proposed reverse conversion for a two-moduli set and three-moduli set providing the foundational framework for the subsequent extension in the work of [7] and for that matter the extension in this paper.

4. Proposed Reverse Conversion for Six-Moduli Set

The proposed reverse conversion algorithm is presented next.

Theorem. *Consider the six-moduli set* $\{m_1, m_2, m_3, m_4, m_4, m_6\}$, *and the residue set* $\{r_1, r_2, r_3, r_4, r_5, r_6\}$. *The general decimal equivalent of any six-moduli set is given as*:

$$\begin{aligned} X = {} & m_1m_2m_3m_4m_5\partial \\ & + m_1m_2m_3m_4\left(|(r_5 - \rho)(m_1m_2m_3m_4)^{-1})|_{m_5}\right) + \rho, \end{aligned} \tag{6}$$

where $\vartheta \in [0, r_6]$, $\rho = m_1m_2m_3\left(|r_4 - (i+j)(m_1m_2m_3)^{-1}|_{m_4} + i + j\right)$

$$i = (m_1m_2\left|(r_3 - \left(\left(m_1\left|(r_2 - r_1)m_1^{-1}\right|_{m_2}\right) + r_1\right))(m_1m_2)^{-1}\right|_{m_3},$$

$$j = m_1\left|(r_2 - r_1)m_1^{-1}\right|_{m_2}) + r_1.$$

Proof. Given the six-moduli set $\{m_1, m_2, m_3, m_4, m_4, m_6\}$, and the residue set $\{r_1, r_2, r_3, r_4, r_5, r_6\}$. The following congruences holds true.

$$X \equiv r_1 mod m_1 \tag{7}$$

$$X \equiv r_2 mod m_2 \tag{8}$$

$$X \equiv r_3 mod m_3 \tag{9}$$

$$X \equiv r_4 mod m_4 \tag{10}$$

$$X \equiv r_5 mod m_5 \tag{11}$$

$$X \equiv r_6 mod m_6. \tag{12}$$

Equation (6) can be expressed as:

$$X = m_1\alpha + r_1. \tag{13}$$

Equation (12) must satisfy Equation (7) such that:

$$m_1\alpha + r_1 = r_2 \, mod m_2$$
$$m_1\alpha = (r_2 - r_1) mod \, m_2$$

$$\alpha = (r_2 - r_1)m_1^{-1} mod \, m_2$$

$$\alpha = m_2\beta + (r_2 - r_1)m_1^{-1} mod \, m_2.$$

Therefore, Equation (12) can be simplified as:

$$\begin{aligned} X &= m_1(m_2\beta + (r_2 - r_1)m_1^{-1} mod \, m_2) + r_1 \\ X &= m_1m_2\beta + m_1(r_2 - r_1)m_1^{-1} mod \, m_2) + r_1. \end{aligned} \tag{14}$$

Now, Equation (13) must satisfy Equation (8)

$$m_1m_2\beta + m_1(r_2 - r_1)m_1^{-1} mod\, m_2) + r_1 = r_3 modm_3$$

$$m_1m_2\beta = r_3 - \Big((m_1\big|(r_2 - r_1)m_1^{-1}\big|_{m_2}) + r_1\Big) modm_3$$

$$\beta = (r_3 - \Bigg(\Big(m_1\big|(r_2 - r_1)m_1^{-1}\big|_{m_2}\Big) + r_1\Bigg))(m_1m_2)^{-1} modm_3$$

$$\beta = m_3\gamma + \Bigg|(r_3 - \Bigg(\Big(m_1\big|(r_2 - r_1)m_1^{-1}\big|_{m_2}\Big) + r_1\Bigg))(m_1m_2)^{-1}\Bigg|_{m_3}. \qquad (15)$$

Therefore, Equation (13) can be simplified further as;

$$X = m_1m_2(m_3\gamma + \Bigg|(r_3 - \Bigg(\Big(m_1\big|(r_2 - r_1)m_1^{-1}\big|_{m_2}\Big) + r_1\Bigg))(m_1m_2)^{-1}\Bigg|_{m_3})$$
$$+ m_1\big|(r_2 - r_1)m_1^{-1}\big|_{m_2}) + r_1,$$

$$X = m_1m_2m_3\gamma + m_1m_2\Bigg|(r_3 - \Bigg(\Big(m_1\big|(r_2 - r_1)m_1^{-1}\big|_{m_2}\Big) + r_1\Bigg))(m_1m_2)^{-1}\Bigg|_{m_3})$$
$$+ m_1\big|(r_2 - r_1)m_1^{-1}\big|_{m_2}) + r_1. \qquad (16)$$

Equation (15) must satisfy Equation (9):

$$m_1m_2m_3\gamma + m_1m_2\Bigg|(r_3 - \Bigg(\Big(m_1\big|(r_2 - r_1)m_1^{-1}\big|_{m_2}\Big) + r_1\Bigg))(m_1m_2)^{-1}\Bigg|_{m_3})$$
$$+ m_1\big|(r_2 - r_1)m_1^{-1}\big|_{m_2}) + r_1 = r_4 modm_4$$

$$m_1m_2m_3\gamma = r_4 - (m_1m_2\Bigg|(r_3 - \Bigg(\Big(m_1\big|(r_2 - r_1)m_1^{-1}\big|_{m_2}\Big) + r_1\Bigg))(m_1m_2)^{-1}\Bigg|_{m_3})$$
$$+ m_1\big|(r_2 - r_1)m_1^{-1}\big|_{m_2}) + r_1)modm_4 \qquad (17)$$

$$\gamma = \Bigg|(r_4 - (m_1m_2\Bigg|(r_3 - \Bigg(\Big(m_1\big|(r_2 - r_1)m_1^{-1}\big|_{m_2}\Big) + r_1\Bigg))(m_1m_2)^{-1}\Bigg|_{m_3})$$
$$+ m_1\big|(r_2 - r_1)m_1^{-1}\big|_{m_2}) + r_1))(m_1m_2m_3)^{-1}\Bigg|_{m_4},$$

$$\begin{aligned}\gamma = m_4\delta + \Bigg|(r_4 - (\, m_1m_2 \Bigg|(r_3 - \bigg(\Big(m_1\big|(r_2 - r_1)m_1^{-1}\big|_{m_2}\Big) + r_1\bigg))(m_1m_2)^{-1}\Bigg|_{m_3}) \\ +\; m_1\big|(r_2 - r_1)m_1^{-1}\big|_{m_2}) + r_1))(m_1m_2m_3)^{-1}\Bigg|_{m_4} .\end{aligned}$$

Equation (15) can be simplified further as;

$$\begin{aligned}&X = m_1m_2m_3(m_4\delta + \\ &\Bigg|(r_4 - (\, m_1m_2 \Bigg|(r_3 - \bigg(\Big(m_1\big|(r_2 - r_1)m_1^{-1}\big|_{m_2}\Big) + r_1\bigg))(m_1m_2)^{-1}\Bigg|_{m_3}) + m_1\big|(r_2 - \\ &r_1)m_1^{-1}\big|_{m_2}) + r_1))(m_1m_2m_3)^{-1}\Bigg|_{m_4}) \quad + \quad m_1m_2 \Bigg|(r_3 - \bigg(\Big(m_1\big|(r_2 - r_1)m_1^{-1}\big|_{m_2}\Big) + \\ &r_1\bigg))(m_1m_2)^{-1}\Bigg|_{m_3}) + m_1\big|(r_2 - r_1)m_1^{-1}\big|_{m_2}) + r_1,\end{aligned}$$

$$\begin{aligned}&X = m_1m_2m_3m_4\delta + m_1m_2m_3(\Bigg|(r_4 - (\, m_1m_2 \Bigg|(r_3 - \bigg(\Big(m_1\big|(r_2 - r_1)m_1^{-1}\big|_{m_2}\Big) + \\ &r_1\bigg))(m_1m_2)^{-1}\Bigg|_{m_3}) + m_1\big|(r_2 - r_1)m_1^{-1}\big|_{m_2}) + r_1))(m_1m_2m_3)^{-1}\Bigg|_{m_4}) + m_1m_2 \Bigg|(r_3 - \\ &\bigg(\Big(m_1\big|(r_2 - r_1)m_1^{-1}\big|_{m_2}\Big) + r_1\bigg))(m_1m_2)^{-1}\Bigg|_{m_3}) + m_1\big|(r_2 - r_1)m_1^{-1}\big|_{m_2}) + r_1.\end{aligned}$$

$$\therefore X = m_1m_2m_3m_4\delta + m_1m_2m_3\big(|r_4 - ((i + j)(m_1m_2m_3)^{-1})|_{m_4}\big) + i + j, \quad (18)$$

where;

$$i = (\, m_1m_2 \Bigg|(r_3 - \bigg(\Big(m_1\big|(r_2 - r_1)m_1^{-1}\big|_{m_2}\Big) + r_1\bigg))(m_1m_2)^{-1}\Bigg|_{m_3} \quad (19)$$

$$j = m_1\big|(r_2 - r_1)m_1^{-1}\big|_{m_2}) + r_1. \quad (20)$$

Equation (17) must satisfy Equation (10). That is,

$$m_1m_2m_3m_4\delta + m_1m_2m_3\big(|r_4 - (i + j)(m_1m_2m_3)^{-1}|_{m_4}\big) + i + j = r_5 mod m_5,$$

$$m_1m_2m_3m_4\delta = r_5 - \big(m_1m_2m_3\big(|r_4 - (i + j)(m_1m_2m_3)^{-1}|_{m_4}\big) + i + j\big) mod m_5, \quad (21)$$

$$\delta = \left|(r_5 - (m_1m_2m_3\left(|(r_4 - (i+j))(m_1m_2m_3)^{-1}|_{m_4}\right) + i + j)(m_1m_2m_3m_4)^{-1})\ _{m_5}\right|.$$

δ can be rewritten as:

$$\delta = m_5\vartheta + \left|(r_5 - (m_1m_2m_3\left(|(r_4 - (i+j))(m_1m_2m_3)^{-1}|_{m_4}\right) + i \\ + j)(m_1m_2m_3m_4)^{-1})\ _{m_5}\right|.$$

Equation (17) can be simplified as:

$$X = \ m_1m_2m_3m_4\big(m_5\vartheta \\ + \left|(r_5 - (m_1m_2m_3\left(|r_4 - (i+j)(m_1m_2m_3)^{-1}|_{m_4}\right) + i \\ + j)(m_1m_2m_3m_4)^{-1})\ _{m_5}\right|\big) \\ + \left(m_1m_2m_3\left(|r_4 - (i+j)(m_1m_2m_3)^{-1}|_{m_4}\right) + i + j\right),$$

$$X = \ m_1m_2m_3m_4m_5\partial + m_1m_2m_3m_4\left(\left|(r_5 - \rho)(m_1m_2m_3m_4)^{-1}\right)\ _{m_5}\right|\big) + \rho, \quad (22)$$

where;

$$\rho = m_1m_2m_3\left(|(r_4 - (i+j))(m_1m_2m_3)^{-1}|_{m_4} + i + j\right). \quad (23)$$

Equation (21) is the general form that satisfies Equation (11) such that,

$$X = \ m_1m_2m_3m_4m_5\partial + m_1m_2m_3m_4\left(\left|(r_5 - \rho)(m_1m_2m_3m_4)^{-1}{}_{m_5}\right|\right) + \rho = r_6, \quad (24)$$

where $\vartheta\ \in [0, r_6]$, ρ is defined in Equation (23), i and j are defined in Equation (19) and (20) respectively.

Note that if $|\rho|_{m_6} = r_6$, then the decimal value of the given residue number is ρ. Otherwise, Equation (22) is evaluated in its entirety.

This completes the proof.

5. Numerical Illustrations

In order to ascertain the correctness of the proposed algorithm, we will consider two examples using the six-moduli set $\{2^{n+1} - 1, 2^{2n} + 1, 2^{2n+1} - 1, 2^{3n} + 1, 2^{3n+1} - 1, 2^{4n} + 1\}$, for even values of n.

Example 1. Find the decimal equivalent of the residue set $\{2, 24, 24, 0, 12, 6\}$ with respect to the moduli set $\{2^{n+1} - 1, 2^{2n} + 1, 2^{2n+1} - 1, 2^{3n} + 1, 2^{3n+1} - 1, 2^{4n} + 1\}$ for $n = 2$.

Solution. A decimal value equivalent of a residue number can be calculated using Equation (22). Therefore,

$$X = m_1m_2m_3m_4m_5\partial + m_1m_2m_3m_4\left(\left|(r_5-\rho)(m_1m_2m_3m_4)^{-1}\right)_{m_5}\right|\right) + \rho = r_6.$$

The moduli set $\{2^{n+1}-1, 2^{2n}+1, 2^{2n+1}-1, 2^{3n}+1, 2^{3n+1}-1, 2^{4n}+1\}$ for $n=2$, reduces to $\{7, 16, 31, 65, 127, 257\}$

$$X = (7\times 16\times 31\times 65\times 127)\partial$$
$$+ (7\times 16\times 31\times 65)\left(\left|(12-\rho)(7\times 16\times 31\times 65)^{-1}\right)_{m_5}\right|\right) + \rho = 6.$$

But,

$$\rho = m_1m_2m_3\left(|(r_4-(i+j))(m_1m_2m_3)^{-1}|_{m_4} + i + j\right),$$

where $i = (\, m_1m_2 \left|(r_3 - \left(\left(m_1|(r_2-\ r_1)m_1^{-1}|_{m_2}\right) +\ r_1\right))(m_1m_2)^{-1}\right|_{m_3}$;

$$i = 7\times 16\left|(24-\left((7|(24-\ 2)7^{-1}|_{16}) +\ 2\right))(7\times 16)^{-1}\right|_{31},$$

$$i = 112\left|(24-\left((7|(24-\ 2)7|_{16}) +\ 2\right))18\right|_{31},$$

$$i = 112|(24-72)18|_{31},$$

$$i = 112\times 4,$$

$$i = 448.$$

$$j =\ m_1\left|(r_2-\ r_1)m_1^{-1}\right|_{m_2}) +\ r_1,$$

$$j = 7|(24-2)7^{-1}|_{16}) +\ 2,$$

$$j =\ 7|(22)\times 7|_{16}) +\ 2,$$

$$j = 7(10) + 2,$$

$$j = 72.$$

Therefore,

$$\rho = 7\times 16\times 31(|(0-(448+72))(7\times 16\times 31)^{-1}|_{65} + 448 + 72),$$

$$\rho = 3472(|520(21)|_{65}) + 520),$$

$$\rho = 3472(0) + 520),$$

$$\rho = 520.$$

Since $|\rho|_{m_6} = r_6$, it implies that decimal value of the residue set $\{2, 24, 24, 0, 12, 6\}$ with respect to the moduli set $\{2^{n+1} - 1, 2^{2n} + 1, 2^{2n+1} - 1, 2^{3n} + 1, 2^{3n+1} - 1, 2^{4n} + 1\}$ for $n = 2$ is 520.

End of example.

Example 2. Find the decimal equivalent of the residue set $\{0, 14, 46, 6, 18, 13\}$ with respect to the moduli set $\{2^{n+1} - 1, 2^{2n} + 1, 2^{2n+1} - 1, 2^{3n} + 1, 2^{3n+1} - 1, 2^{4n} + 1\}$ for $n = 4$.

Solution. A decimal value equivalent of a residue number can be calculated using Equation (22). Therefore,

$$X = m_1m_2m_3m_4m_5\partial + m_1m_2m_3m_4\big(\big|(r_5 - \rho)(m_1m_2m_3m_4)^{-1})\,_{m_5}\big|\big) + \rho = r_6.$$

The moduli set $\{2^{n+1} - 1, 2^{2n} + 1, 2^{2n+1} - 1, 2^{3n} + 1, 2^{3n+1} - 1, 2^{4n} + 1\}$ for $n = 4$, reduces to $\{31, 256, 511, 4097, 8191, 65537\}$

$$X = \ m_1m_2m_3m_4m_5\partial + m_1m_2m_3m_4\left(\left|(r_5 - \rho)(m_1m_2m_3m_4)^{-1}{}_{m_5}\right|\right) + \rho = r_6$$

But,

$$\rho = m_1m_2m_3\big(|(r_4 - (i + j))(m_1m_2m_3)^{-1}|_{m_4} + i + j\big),$$

where $i = (\ m_1m_2\left|\left(r_3 - \left(\left(m_1\left|(r_2 - \ r_1)m_1^{-1}\right|_{m_2}\right) + \ r_1\right)\right)(m_1m_2)^{-1}\right|_{m_3}$;

$$i = 31 \times 256\big|(132 - \big((31|(4 - \ 6)31^{-1}|_{256}) + \ 6\big))(31 \times 256)^{-1}\big|_{511},$$

$$i = 7936\big|(132 - \big((31|(-2)223|_{256}) + \ 6\big))7936^{-1}\big|_{511},$$

$$i = 7936\big|(132 - \big((31 \times 66) + \ 6\big))66\big|_{511},$$

$$i = 7936|(132 - 2052)66|_{511},$$

$$i = 7936|-126720|_{511},$$

$$i = 7936 \times 8,$$

$$i = 63488.$$

$$j = m_1\left|(r_2 - r_1)m_1^{-1}\right|_{m_2}) + r_1,$$

$$j = 31|(4 - 6)31^{-1}|_{256}) + 6,$$

$$j = 31|(-2) \times 223|_{256}) + 6,$$

$$j = 31|-446|_{256}) + 6,$$

$$j = 3(66) + 6,$$

$$j = 2052.$$

Therefore,

$$\rho = 31 \times 256 \times 511(|4085 - (63488 + 2052)(7 \times 16 \times 31)^{-1}|_{4097} + 63488 + 20522),$$

$$\rho = 4055296|(4085 - 65540) \times 0|_{4097}) + 65540,$$

$$\rho = 0 + 65540,$$

$$\rho = 65540.$$

Since $|\rho|_{m_6} = r_6$, it implies that the decimal value of the residue set $\{0, 14, 46,6,18,13\}$ with respect to the moduli set $\{2^{n+1} - 1, 2^{2n} + 1, 2^{2n+1} - 1, 2^{3n} + 1, 2^{3n+1} - 1, 2^{4n} + 1\}$ for $n = 4$ is 65540.

End of example.

6. Conclusion

Reverse conversion is an essential process in the full realization of residue number systems. This paper presented a new reverse conversion algorithm for a six-moduli set, $\{2^{n+1} - 1, 2^{2n} + 1, 2^{2n+1} - 1, 2^{3n} + 1, 2^{3n+1} - 1, 2^{4n} + 1\}$, for even values on n, that aims at simplifying the computation overhead inherent in the traditional methods. Through several numerical evaluations, the proposed method has demonstrated to be correct and offers a reduction in the reliance on complex multiplicative inverses as pertains with other methods. An interesting advantage of the choice of the six-moduli set is the offer of a larger dynamic range as compared to related algorithms. This work contributes to expanding the frontiers of residue number system research including its widespread practical use. The actual hardware implementation of this new algorithm will be an interesting avenue for further research.

References

[1] Nawusu, Y.A.-W., Abdul-Barik, A., & Salifu, A.-M. (2022). Residue number system-based approach to minimize energy consumption in wireless sensor networks. *Asian Journal of Research in Computer Science, 14*(4), 46-65. https://doi.org/10.9734/ajrcos/2022/v14i4291

[2] Tanaka, R. (1962). *Modular arithmetic techniques*. Tech. Rep. ASTDR, Lockheed Missiles and Space Co., (2-38-62-1A).

[3] Keir, Y.A., Cheney, P.W., & Tannenbaum, M. (1962). Division and overflow detection in residue number systems. *IRE Transactions on Electronic Computers*, *EC-11*, 501-507. https://doi.org/10.1109/TEC.1962.5219389

[4] Nawusu, A.-W.Y., Alhassan, A.-B., & Salifu, A.-M. (2021). A new approach to detecting and correcting single and multiple errors in wireless sensor networks. *Journal of Advances in Mathematics and Computer Science*, *36*(8), 27-43. https://doi.org/10.9734/jamcs/2021/v36i830388

[5] Omondi, A., & Premkumar, B. (2007). *Residue Number System: Theory and Implementation*. Imperial College Press, London. https://doi.org/10.1142/p523

[6] Reddy, Y.A., & Sekhar, B. (2016) An efficient reverse converter design for five moduli set RNS. *International Journal of Advanced Research in Computer and Communication Engineering*, *5*, 208-212.

[7] Salifu, A.-M. (2021). New reverse conversion for four-moduli set and five-moduli set. *Journal of Computer and Communications*, *9*, 57-66. https://doi.org/10.4236/jcc.2021.94004

[8] Asiedu, D., & Salifu, A.-M. (2021). New algorithm for reverse conversion in residue number system. *Asian Journal of Computer Science and Technology*, *10*(1), 1-4. https://doi.org/10.51983/ajcst-2021.10.1.2693

[9] Baagyere, F. Y. (2011). Application of residue number system to Smith-Waterman algorithm, MPhil. dissertation. Kwame Nkrumah University of Science and Technology.

[10] Bankas, E., & Gbolagade, K. (2013). A new efficient FPGA design of residue-to-binary converter. *International Journal of VLSI Design & Communication Systems* (*VLSICS*), *4*(6). https://doi.org/10.5121/vlsic.2013.4601

[11] Roshanzadeh, M., & Saqaeeyan, S. (2012). Error detection & correction in wireless sensor networks by using residue number systems, *International Journal of Computer Network and Information Security*, *4*(2), 29-35. https://doi.org/10.5815/ijcnis.2012.02.05

[12] Jenkins, W., & Leon B. (1977). The use of residue number systems in the design of finite impulse response digital filters. *IEEE Trans. on Circuits and Systems*, *24*(4), 191-200. https://doi.org/10.1109/TCS.1977.1084321

[13] Beckmann P, & Musicus B. (1993). Fast fault-tolerant digital convolution using a polynomial residue number system. *IEEE Transactions on Signal Processing*, *41*(7), 2300-2313. https://doi.org/10.1109/78.224241

[14] Taylor, F.J. (1984). Residue arithmetic: A tutorial with examples. *Computer*, *17*(5), 50-62. https://doi.org/10.1109/MC.1984.1659138

[15] Agbedemnab, P.A.N., Baagyere, E.Y, & Daabo, M.I. (2019). A new image encryption and decryption technique using genetic algorithm and residual numbers. *IEEE AFRICON Conference*, 2019, 20-31. https://doi.org/10.1109/AFRICON46755.2019.9133919