A New Moduli Set $\{3^n-1, 3^n+1, 3^n+2, 3^n-2\}$ in Residue Number System

Mehdi Hosseinzadeh
Young Research Club of Islamic Azad University Science and Research branch, Tehran, Iran
hosseinzadeh@sr.iau.ac.ir

Somayyeh Jafarali Jassbi
Islamic Azad University Science and Research branch, Tehran, Iran
a.jassbi@sr.iau.ac.ir

Keivan Navi
Department of Electrical and Computer Engineering, Shahid Beheshti University, Tehran, Iran
navi@sbu.ac.ir

Abstract- The Residue Number System (RNS) is non weighted system. This system is a useful tool for Digital Signal Processing (DSP) since it can support parallel, carry-free, high-speed, low power and secure arithmetic. One of the most important considerations when designing RNS systems is the choice of the moduli set. This is due to the fact that the system's speed, its dynamic range, as well as its hardware complexity depend on both the forms and the number of the chosen moduli.

Researchers have considered many moduli sets to be the basis of a RNS processor: $\{2^n-1, 2^n, 2^n+1\}$, $\{2^n, 2^n-1, 2^{n-1}-1\}$, $\{r^n-2, r^n-1, r^n\}$, $\{r^a, r^b-1, r^c+1\}$ and many others. In this paper a new moduli set $\{3^n - 1, 3^n + 1, 3^n + 2, 3^n - 2\}$ is introduced.

Comparisons demonstrate that we have achieved a significant improvement in terms of speed, security, dynamic range and simple of selection moduli.

Keywords- Computer Arithmetic, Residue Number System, Multi-Level Residue Number System, VLSI.

1- Residue Number System

Residue Number System is unconventional and non-Weighted Number System in which the additions, subtractions and multiplication are inherently carry free. As a result we may add, subtract and multiply numbers in one step regardless of the length of the number involved. An integer X is represented in the Residue Number System by an n-tuple $(x_1, x_2, x_3, \dots, x_n)$ where x_i is a nonnegative integer satisfy $X = m_i q_i + r_i$ .This causes an increase in calculation speed and a reduction in its power consumption.

Residue Number System is specified by moduli set like $\{m_1, m_2, m_3, \dots, m_n\}$ in which all the moduli are positive integers. If all the moduli are relatively pair wise prime the system will have the largest possible dynamic range which equals $[\alpha, \alpha+M)$ in which α is an integer and M is:

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

The integer X in $\alpha \le X < \alpha + M$ has a single representation in Residue Number System which is shown by the set of remainders $(x_1, x_2, x_3, \dots, x_n)$. In this way:

$$x_i = X \mod m_i,\ i = 1,2,3,\dots,n \tag{2}$$

In order to reconstructing the specified number X the remainders $(x_1, x_2, x_3, \dots, x_n)$ the Chinese Remainder Theorem is applied as follows:

$$X = \left\langle \sum_{i=1}^{n} (x_i N_i)_{m_i} \times M_i \right\rangle_M$$

$$M = \prod_{i=1}^{n} M_i$$

$$M_i = \frac{M}{m_i} \quad ,N_i = \left\langle M_i^{-1} \right\rangle_{m_i}, i = 1,2,3,\dots,n \tag{3}$$

In which $\left\langle M_i^{-1} \right\rangle$ is defined as multiplicative inverse with m_i moduli [1].

Due to its special features, the Residue Number System has many applications in arithmetic functions such as Digital Signal Processing, Digital Filtering, Coding, RSA ciphering system, digital communications, Ad-hoc network, storing and retrieving information, Error detection and Correction, and fault tolerant systems. This system is generally used in those areas where addition, subtraction and multiplication operations of numbers are being repeated. Moreover, since in this system the calculations on the remainders are done independently if one error occurs on one remainder it won't be transferred to other moduli. In other words, the architecture of RNS is inherently tolerant against faults and error detection and correction are quite possible [2-6].

In the second and third chapters of this article, Multi-Level Residue Number System and Ternary Valued Logic will be examined respectively. In the fourth chapter, A New Moduli Set $\{3^n-1, 3^n+1, 3^n+2, 3^n-2\}$ in Residue Number System is represented. In chapter five New Moduli Set will be compared to other moduli Set. Finally an overall conclusion will be represented.

2- Multi-Level RNS

Considering the impact of Residue Number System in increasing calculation speed, reducing power consumption, and increasing the security and fault tolerance, it would be possible to perform arithmetic calculations on each modulus with a new Residue Number System. It is possible to repeat this procedure until we reach very small moduli, in other words this procedure could be repeated in several levels. The system which is achieved form the above mentioned procedure is called Multi-Level Residue Number System. The only restriction that should be considered in Multi-Level Residue is that the Residue Number System dynamic range that is considered for i level of each (i-1) moduli-level should be greater or equal to those moduli[7-10].

In this article, for having a more simple representation two-level Residue Number System is being analyzed. It should be mentioned that this method could be generalized to more than two levels.

In two-level Residue Number System, two symmetrical coding key algorithms are used inside each other; therefore the system has a much higher security level than the Residue Number System. The other advantage of two-level Residue Systems is the simple selection of moduli set for a large dynamic range that is by selecting a few large moduli and applying a new Residue Number System with a lower power for second level this capability is achieved. By having few moduli with higher power in the first level; first the need for moduli to be relatively pair wise prime is eliminated and there is no obligation for the moduli to be symmetric and regular, second as the number of moduli is reduced the concerning conversion circuits, become simple and the operation is done rapidly. Also, in the second level since the moduli are small because of the limited propagation of carries, the internal calculations of the Residue Number System are done faster.

3- Ternary Valued Logic

Despite binary logic in which logical levels are restricted to two possible states, namely false and true, there exists an alternative named Multiple Valued Logic. In this system, theoretically, one can define an unlimited number of logical levels, but in reality it is limited and this limitation mainly depends on the used technology. In Ternary valued logic with 3 levels comprising $\{0,1,2\}$, we can introduce a new era.

It is obvious that the positional weights of any two succeeding columns are power of 3. Figure 1 represents the positional value of each location.

$$\begin{array}{c} a_{n-1}a_{n-2}a_{n-3} \ldots a_2a_1a_0 \\ \_\ \_\ \_ \qquad \_\ \_\ \_ \\ \ldots \\ 3^{n-1}3^{n-2}3^{n-3} \ldots 3^2 3^1 3^0 \end{array}$$

Fig. 1. Positional weight value of each location

Each location in an TVL component can store much more information than a binary logic component can, the dynamic range of the moduli set $\{3^n - 2, 3^n - 1, 3^n\}$ is much greater than its equivalent in the binary representation. Now the question is how to present the related hardware which is clearly answered in [11-13]. For example if we compare two different moduli sets with equal number of locations, the results illustrated in Table 1 will be obtained.

Table 1. Comparison of dynamic range and number of location

Moduli set	Number of position	M
$\{3^n - 2, 3^n - 1, 3^n\}$	$3n$	$3^{3n} - 3^{2n+1} + 2 \times 3^n$
$\{2^n - 1, 2^n, 2^{n-1} - 1\}$	$3n$	$2^{3n-1} - 1.5(2^{2n}) + 2^n$
$\{2^n - 1, 2^n, 2^n + 1\}$	$3n + 1$	$2^{3n} - 2^n$

Table 2. Comparison of dynamic with different n.

M \ n	5	10
$3^{3n} - 3^{2n+1} + 2 \times 3^n$	14172246	$\approx 2 \times 10^{14}$
$2^{3n-1} - 1.5 \times 2^{2n} + 2^n$	14880	$\approx 5 \times 10^{8}$
$2^{3n} - 2^n$	32736	$\approx 10^{9}$

Based on these comparisons, we conclude that the TVL with the same number of locations has a much larger dynamic range.

4- A New Moduli Set $\{3^n - 1, 3^n + 1, 3^n + 2, 3^n - 2\}$

In this paper a Two-Level moduli set $\{3^n - 1, 3^n + 1, 3^n + 2, 3^n - 2\}$ in ternary logic is presented. In first level the moduli set $\{3^{2n} - 1, 3^{2n} - 4\}$ is used this moduli are relatively prime. Then for the second level the moduli set $\{\{3^n - 1, 3^n + 1\}, \{3^n + 2, 3^n - 2\}\}$ is considered for $3^{2n} - 1, 3^{2n} - 4$.

For RNS conversion, first we convert to the first level and then we convert the remainder of first level to the second level. In order to do the reverse conversion we do the same job but from bottom to up. Which means, first we convert the second level to the first level and then we convert the remainder of first level to weighted number system.

5- Comparison

In table 1 the comparison of the dynamic range, security and RNS to TVL conversion between moduli set $\{r^n - 2, r^n - 1, r^n\}$ presented in [11], moduli set $\{r^a, r^b - 1, r^c + 1\}$ presented in [13] and moduli set $\{3^n - 1, 3^n + 1, 3^n + 2, 3^n - 2\}$ is presented (In order to have a simple comparison we consider a=b=c=n and r=3).

Table3: Comparison between moduli sets

	Dynamic Range	Security	RNS to TVL
$\{r^n - 1, r^n,, r^n - 2\}$	$r^{3n} - 3r^{n+1} + 2r^n$	Medium	τ_{3CRT}
$\{r^a, r^b - 1,, r^c + 1\}$	$(r^{3n} - r^n)/4$	Medium	$\tau_{3CRT} + \tau_{Scale-Down\ factor}$
$\begin{Bmatrix} 3^n - 1, 3^n + 1, \\ 3^n + 2, 3^n - 2 \end{Bmatrix}$	$r^{4n} - 5r^{2n} + 4$	High	$2\tau_{2CRT}$

6- Conclusion

In this paper a Two-Level moduli set $\{3^n - 1, 3^n + 1, 3^n + 2, 3^n - 2\}$ in ternary logic is presented. In Two-Level RNS, two symmetrical key encryption algorithms are used together, so the system has a high security. Another advantage of Two-Level RNS is the simple selection moduli set for large dynamic range. Comparisons demonstrate that we have achieved a significant improvement in terms of speed, security, dynamic range and simplicity of moduli selection.

References

[1] N. S. Szabo and R. I. Tanaka, "Residue Arithmetic and Its Applications to Computer Technology," New York :McGraw-Hill, 1967.

[2] Jean-Claude Bajard, Laurent Imbert, "A Full Implementation RSA in RNS," *IEEE Transactions on Computer*, Vol. 53, No.6, Jun. 2004.

[3] J. Ramirez, et al., "Fast RNS FPL-Based Communications Receiver Design and Implementation," *Proc. 12th Int'l Conf. Field Programmable Logic*, pp. 472-481, 2002.

[4] H. Krishna, K.-Y. Lin, and J.-D. Sun, "A coding theory approach to error control in redundant Residue Number Systems - Part I: theory and single error correction," *IEEE Trans. Circuits Syst.*, Vol. 39, pp. 8-17, Jan. 1992.

[5] J.-D. Sun and H. Krishna, "A coding theory approach to error control in redundant Residue Number Systems -Part II: multiple error detection and correction," *IEEE Trans. Circuits Syst.*, Vol.39, pp. 18-34, Jan. 1992.

[6] Parhami B., "RNS Representation with Redundant Residues," *Proc. of the 35th Asilomar Conference on Signals, Systems, and Computers*, Pacific Grove, CA, pp. 1651-1655, Nov. 2001.

[7] H. M. Yassine, "Hierachical Residue Number System suitable for VLSI Arithmetic Architectures" *IEEE International Symposium on Circuits and Systems,* Vol. 2, pp. 811-814, May 1992.

[8] A. Skavantzos and M. Abdallah, "Implementation Issues of the Two-Level Residue Number System with Pairs of Conjugate Moduli," *IEEE Transactions On Signal Processing*, Vol. 47, No. 3, Mar. 1999.

[9] S. Timarchi, K. Navi and M. Hosseinzadeh, "New Design of RNS Subtractor for modulo $(2^n + 1)$," 2th *IEEE International Conference on Information & Communication Technologies: From Theory To Applications*, Apr. 2006.

[10] M. Hosseinzadeh, S. J. Jassbi and K. Navi, "A Novel Multiple Valued Logic OHRNS Moduli r^n Adder Circuit," *International Conference on ENGINEERING AND TECHNOLOGY,* Vol. 25, pp. 128-132, Nov. 2007.

[11] M. Hosseinzadeh, K. Navi, S. Gorgin, "A New Moduli Set for RNS: $\{r^n - 2, r^n - 1, r^n\}$," *International Conference on Electrical Engineering 2007*, Apr. 11-12, 2007.

[12] M. Hosseinzadeh and K. Navi, "A New Moduli Set for Residue Number System in Ternary Valued Logic," *Journal of Applied Sciences*, Vol. 7, No. 23, pp. 3729-3735, 2007.

[13] M. Abdallah and A. Skavantzos, "On Multi Moduli Residue Number Systems With Moduli of Forms $\{r^a, r^b - 1, r^c + 1\}$," *IEEE Transactions Circuits System I: Regular Paper*, Vol. 52, No. 7, pp. 1253-1266, 2005.