International Journal of Advance in Computer Science & its application – IJCSIA 2018
Copyright © Institute of Research Engineers and Doctors , SEEK Digital Library
Volume 7 : Issue 2 [ISSN : 2250-3765] - Publication Date: 25 June , 2018

The New proposed Non-Coprime moduli set using forward conversion in Residue Number System : Mathematical Proof

Mansour Bader[1], Andraws Swidan[2]

***Abstract*- In this paper a mathematical proof of the new Binary-to-RNS Non-Coprime moduli set in**

RNS [1] of the form { $2^n - 2, 2^n, 2^n + 2$ } is presented. The modulies $2^n - 2, 2^n + 2$ are known to be called conjugates of each other and has been discussed in previous literature [1 - 4]. Co-prime moduli sets are known to offer these benefits: 1) Large dynamic ranges. II) Fast RNS arithmetic.

III) Simple and efficient RNS processing hardware. IV) Efficient weighted-to-RNS and RNS-to-Weighted converters. When comparing the Non-Coprime ones to them the DR (Dynamic Range) is the dominant. The dynamic range achieved by the set above is defined by the least common multiple (LCM) of the moduli and the non-coprime set was carefully chosen to do the mathematical calculations upon. This new non-coprime moduli set is unique and the only one of its shape.

.

***Keywords*-Algorithm, Arithmetic, Dynamic Range , Forward conversion, RNS**

I. Introduction

All standard papers look at RNS as a subfield of finite field arithmetic [5]. It is widely used in digital signal processing, image processing, FIR (Finite Impulse Response) filters, and IIR (Infinite Impulse Response) filters because it is considered a carry-free system that is highly efficient in addition and multiplication [2].

RNS is used also by most applications that need a high degree of concurrency. A lot of researches in computer systems are enthusiastic to go through RNS because of its characteristics such as, modularity, error detection and correction (fault tolerant) [3], and embedded parallelism.

RNS allows the division of a large number into smaller sub numbers called "tipples". Numbers are then represented by tipples that need less number of bits. These bits can be pr ocessed individually and in parallel as RNS properly job without carry between them [4]. Being carry-free improves computation time and simplifies hardware cost.

In [4] it is stated that " Non-coprime moduli sets are a field in Residue Numbering System (RNS) which is little studied. That's why this work was devoted to them. The resources that discuss non-coprime in RNS are very limited". Based on that this paper tries to discuss the mathematical proof of the new non-coprime moduli set. This new moduli set is represented as $\{2^n - 2, 2^n, 2^n + 2\}$, where $n \in \{2,3,\ldots..,\infty\}$.

Which shows that:

$$\gcd(m_i, m_j) \neq 1 \text{ for } i \neq j. \qquad (1)$$

The calculations among the moduli are done with this ' n ' value. Being 2 spaces apart on the numbers line from each other (i.e. the modulus values), this range helped in the algorithm's calculations as will be shown in next sections.

The rest of this paper is organized as follows. In Section 2, overview of the new Non-coprime moduli is proposed. Section 3 presents the mathematical calculations of the proposed forward converter of the new non-coprime moduli . Finally the paper is concluded in Section 4.

Mansour Bader

Department of Computer Engineering
Al-Balqa'a Applied University
Jordan

International Journal of Advance in Computer Science & its application – IJCSIA 2018
Copyright © Institute of Research Engineers and Doctors , SEEK Digital Library
Volume 7 : Issue 2 [ISSN : 2250-3765] - Publication Date: 25 June , 2018

mansoor259@yahoo.com ,
mansoor259@bau.edu.jo

Andraws Swidan

Department of Computer Engineering
Jordan University
Jordan
sweidan@ju.edu.jo

II. Overview of the new Non-coprime moduli

"The basis for an RNS is a set of relatively prime integers; that is: P = {q1,q2,... ,qL}, where (qi,qj) = 1 for i≠j (2) with (qi , qj) indicating the greatest common divisor of qi and qj .

The set P is the moduli set while the dynamic range of the system (i.e. M) is the product Q of the moduli qi in the set P.

Any integer X belonging to ZQ = { 0, 1 2, ... , Q -1 } has an RNS representation" [6] .

$$X \xrightarrow{\text{RNS}} (X1, X2, \dots, XL) \quad (3)$$

$$Xi = \langle X \rangle qi , \quad i = 1, 2, ... , L \quad (4)$$

Where <X>q is X mod q.

For both cases (i.e. coprime and non-coprime) any integer x ϵ [0, M – 1] has an RNS representation X = (x1 , … , xk), where xi = X mod mi.

The new thing here is the work with a full non-prime moduli set (i.e. for this case same as equation 1 condition) ; gcd (mi, mj) ≠ 1 for i ≠ j .

RNS systems based on non coprime moduli have also been studied in the literature [4] –[8].

The Mathematical proof is to be shown for this proposed Non-coprime moduli set :

$$S = \{ 2^n - 2, 2^n, 2^n + 2\}. \quad (5)$$

Example 1 shows what is meant by the spaces:

Ex.1 Let n = 3 for the set S.

Then the set S = { 6, 8, 10 }.

Numbers (6 , 8) and (8 , 10) are consequently 2 spaces apart from each other on the numbers line. This is true for any value taken for "n", noticing that n >= 2.

Least Common Multiple (LCM) is must be used for the non-coprime case, since there is a common factor among the modulus numbers, as previous literature researches showed.

III. mathematical calculations of the New proposed non-coprime moduli set

Non-coprime has been studied recently in research and literature. The process of converting the data from conventional representation (binary in this case) to RNS representation is also known widely as residue generation, binary-to-residue conversion or (FC) Forward Conversion.

The initial inputs are in binary representation, this could also be done through the bit rewiring block of the proposed method of [12] block diagram.

These Calculations are easy to understand if they were divided into 3 parts regarding to the modulus numbers of the moduli set.

Working with each part alone, showing the mathematics of resolving its value, after that they will be gathered again to make the full shape algorithm.

III.1 Non-coprime pre-modulus general algorithm

The parameters for this part are:

$X = 2^{n+m} + k$, where $(n, m) \in \{0,1,2,\dots\infty\}$, and $k \in \{0,1,2,\dots\dots,2n - 3\}$.

$$|2^{n+m} + k\,|2^n - 2 = ||2^n|2^n - 2 * |2^m|2^n - 2 + |k|2^n - 2|\, 2^n - 2. \quad (6)$$

International Journal of Advance in Computer Science & its application – IJCSIA 2018
Copyright © Institute of Research Engineers and Doctors , SEEK Digital Library
Volume 7 : Issue 2 [ISSN : 2250-3765] - Publication Date: 25 June , 2018

This equation has 3 cases upon values of m,n , that need a focus on their Integrations.

Case1: m < n

$|2^n|2^n - 2 = |2^n - 2 + 2|2^n - 2 = \Big| |2^n - 2|2^n - 2 + |2|2^n - 2 \Big| 2^n - 2 = 0 + 2 = 2.$ (7)

$|\mathbf{2^m}|_{2^n - 2} = 2^m.$

The last part which is k, $|\mathbf{k}|_{2^n - 2} = k.$

Thus $\Big| 2^{n+m} + k \Big| 2^n - 2 = 2m + 1 + k$ (8)

Case 2: m = n

The number here is of the form $2^{n+m} + k = 2^{n+n} + k = 2^{2n} + k$. From the knowledge of Fermat's theorem that $2^{\alpha n} + k \bmod 2^n$ is equal to k, the result should be $2*2 + k = \Big| 4 + k. \Big|$

Case 3: m > n

$|2^{n+m} + k|2^n - 2 = \Big| |2^n|2^n - 2 * |2^m|2^n - 2 + |k|2^n - 2 \Big| 2^n - 2$

Taking each part alone, the $|2^n|2^n - 2$ gives us 2, multiplied by a number which is greater than $2^n - 2$ so it is important to take the difference among them (i.e. m – n), so the final shape would be $2*(2^{m-n+1})$, when adding k , the final shape would be $2*(2^{m-n+1}) + k$, and it could be simpler as of $2\text{^}(m-n+2) + k$ (9)

The final shape of the suggested general formula is:

$$|2(m+n) + k|2n - 2 = \begin{cases} |2^m + 1 + k|2^n - 2 & ; \ m < n \\ |4 + k|2^n - 2 & ; \ m = n \\ |2^{(m - n + 2)} + k|2^n - 2 & ; \ m > n \end{cases} \quad (10)$$

III.2 Non-coprime post-modulus general algorithm

Again the general number equation used is $2^{n+m} + k$, where (n, m) ∈ {0,1,2,….,∞},and k ∈ {0,1,2,……,2n + 1} at last.

Finishing at post-modulus, $|2^{n+m} + k|2^n + 2 = \Big| |2^n|2^n + 2 * |2^m|2^n + 2 + |k|2^n + 2 \Big| 2^n + 2$ (11)

This equation has also three cases of it, they are m < n, m = n and finally m > n.

Case 1: n > m

$|2^n|2^n + 2 = |2^n + 2 - 2|2^n + 2 = \Big| |2^n + 2|2^n + 2 - |2|2^n + 2 \Big| 2^n + 2 = 0 - 2 = -2.$ (12)

the second part of the first assumption; $|2^m|2^n + 2 = 2^m$, and the last part $|k|2^n + 2 = k$.

Case 2: m = n

Has same calculation of the pre-modulus part, the result is 4 + k.

Case 3: m > n

$|2^{n+m} + k|2^n + 2 = \Big| |2^n|2^n + 2 * |2^m|2^n + 2 + |k|2^n + 2 \Big| 2^n + 2$. (13)

If we take each part alone, the $|2^n|2n + 2$ give us -2 as calculated in equation 12, multiplied by $(-2+2^{m-n})$, when the last part of the formula which makes different numbers (i.e. k) is added the

final shape would be $-2*(-2+2^{m-n}) + k$, and it could be simpler as of $2^{m-n+2} + k$.

The last shape of the general formula of $2^n + 2$ is:

$$|2(m+n)+k|2n+2 = \begin{cases} |-2^{m}+1+k|2^{n}+2 & ; \ m < n \\ |4+k|2^{n}+2 & ; \ m = n \\ |2^{m-n}+2+k|2^{n}+2 & ; \ m > n \end{cases} \quad (14)$$

IV. CONCLUSIONS

A new non-coprime moduli set has been proposed. A general formula for the mathematical calculations was derived. The mathematics computations for the new special non-coprime moduli set just as the co-prime one's has been verified too.

This research revealed that non-coprime moduli set may be suitable for wide variety of cases not limited to co-prime ones only.

ACKNOWLEDGEMENTS

The authors would like to thank everyone.

REFERENCES

[1] Mansour Bader, Andraws Swidan and Mazin Al-hadidi (2017), "NEW NON-COPRIME CONJUGATE-PAIR BINARY TO RNS MULTI-MODULI FOR RESIDUE NUMBER SYSTEM ". Third International Conference on Cryptography and Information Security (CRIS 2017).

[2] Chaves, R., and Sousa, L. (2007) "Improving residue number system multiplication with more balanced moduli sets and enhanced modular arithmetic structures". Computers &Digital Techniques IET, Volume 1, Issue 5, pages 472-480.

[3] Modiri, Samira, Movaghar, and Barati (2012) "Study of error control capability for the new moduli set {22n+ 1+ 2n-1, 22n+ 1-1, 2n-1, 23n, 23n+ 1-1}". Journal of Advanced Computer Science & Technology, Vol. 1, Pages: 176-186.

[4] Mansour Bader, Andraws Swidan, Mazin Al-Hadidi and Baha Rababah, "A binary to residue conversion using new proposed non-coprime moduli set", Signal & Image Processing : An International Journal (SIPIJ) Vol.7, No.3, June 2016 .

[5] Neha Singh, (2008), "An overview of Residue Number System". National Seminar on Devices, Circuits & Communication.

[6] Y. Wang.(1998) "New Chinese Remainder Theorems". In proceedings of the Thirty Second Asilomar Conference on Signals, Systems and Computers, Pages: 165-171.

[7] M. Abdallah, A. Skavantzos, "On the binary quadratic residue system with non coprirne moduli", *IEEE Trans. On Signal Processing*, vol. 45, no. 8, pp. 2085-2091, Aug. 1997.

[8] A. Skavantzos ; Yuke Wang, "Application of new Chinese Remainder Theorems to RNS with two pairs of conjugate moduli", IEEE Pacific Rim Conference on Communications,

Computers and Signal Processing (PACRIM 1999). Conference Proceedings, 1999.

[9] Shende, Radha, and Zode.(2012) "Efficient design $2^k - 1$ binary to residue converter." On proceedings of International Conference IEEE, Devices, Circuits and Systems (ICDCS), Pages: 482 – 485.

[10] Omondi, Amos, and Premkuar.(2007) "Residue number systems: theory and implementation". Imperial College Press.

[11] Hiasat, and Sweidan(2003) "Residue number system to binary converter for the moduli set ($2^n - 1$, 2^n, $2^n + 1$)". Journal of systems architecture,Vol.49, Pages: 53-58.

[12] Vidhyalakshmi.M,Prof.Satyabama . (2014) "Design and Implementation of Efficient Binary to Residue Converter Using Moduli Method". **International Journal of Innovative Research in Computer and Communication Engineering,** Vol. 2, Special Issue 1, March 2014.

Authors

Mansour Bader holds a MSc in computer engineering and networks, University of Jordan, Jordan, 2016. BSc Computer Engineering, Al-Balqa Applied University, Jordan, 2008. He is a technical support engineer of computer networks at computer center of Al-Balqa Applied University for 8 years and a half.

Dr. Andraws I. Swidan was born in Al-Karak Jordan in 1954. He received his diploma in Computer Engineering (with honours) and Ph.D. in Computer Engineering from LETI Ulianov Lenin, Sanct Peterburg (Leningrad), Russia in 1979 and 1982 respectively. He Joined the Electrical Engineering Department at the University of Jordan in 1983 and was one of the founders of the Computer Engineering Department at the University of Jordan in 1999. Since then he is a professor at the department. He is also an Adjunct Professor with the ECE department of the McGill University, Montreal, Canada.

He holds several technical certifications among which the CISSP. He is an IEEE member, Jordanian Engineering Association member Quebec College of engineers member. He is a Canada Professional Engineer (The province of Quebec). He was member of several national and international scientific committees. He holds several patents and tens of publications.

His main areas of research interest are: computer arithmetic, computer security, encryption algorithms.