NEW CHINESE REMAINDER THEOREM AND MODULI SETS

RAMANANDA H. S

Abstract: In this paper, mathematical proof for "New Chinese remainder theorem (New CRT-I)", proposed by Yuke Wang, is given. A new moduli set is proposed for converting from residue to binary number system. For the new moduli set , the reverse converter sets are also obtained using the Chinese remainder theorem as well as using The New CRT-I.

Keywords: RNS, Moduli set, The Chinese Remainder Theorem.

Introduction: There has been interest in Residue Number Systems (RNS) since the 1950's [1], [2]. During the past 20 years, the RNS has received more attention in arithmetic computation and signal processing applications [3], [4]. The conversion from residue to binary numbers is the crucial step for any RNS application. For general set of relatively prime numbers(called moduli set), the residue to binary conversion is based on the Chinese Remainder Theorem (CRT). However, it is found that [5], a direct implementation of CRT is uncomfortable since it is based on moduli M operation where M is large. Therefore in the paper [6], Yuke Wang proposed a new remainder theorem and he called it as New Chinese Remainder Theorem -I (New CRT-I). In that paper, the proof of the theorem is not clear. So in section 2,of this paper, a mathematical proof of New CRT-I is given.

Several types of moduli sets have been considered by RNS researchers. A large number of different parameterized moduli sets have been suggested in the literature. The parameterized sets consist of a small number of low-cost moduli on a fix form, where each moduli is expressed as a function of a parameter, say n. Few well-known parameterized moduli sets are

$S_1 = \{2^n-1, 2^n+1\}$

$S_2 = \{2^n-1, 2^n, 2^n+1\}$

$S_3 = \{2^n-1, 2^n, 2^n+1, 2^{2n}+1\}$.

In section 3, a new parametrized moduli set is given and its reverse converter set (inverse set) using the CRT and reverse converter set using the New CRT-I is obtained.

2. The New Chinese remainder theorem – I:

Theorem 2.1: *Let $m_1, m_2, \ldots, m_n$ be positive integers such that $gcd(m_i, m_j) = 1$ for $i \neq j$*

Then the system of linear congruences

$$\begin{aligned} x &\equiv x_1 (\mathrm{mod}\, m_1) \\ x &\equiv x_2 (\mathrm{mod}\, m_2) \\ &\vdots \\ x &\equiv x_n (\mathrm{mod}\, m_n) \end{aligned} \qquad (1)$$

has a unique solution modulo $m_1 m_2 \ldots m_n$.

The solution is

$$\bar{x} \equiv [x_1 + k_1 m_1 (x_2 - x_1) + k_2 m_1 m_2 (x_3 - x_2) \ldots + k_{n-1} m_1 m_2 \ldots m_{n-1} (x_n - x_{n-1})] (\mathrm{mod}\, m_1 m_2 \ldots m_n) \qquad (2)$$

where $k_1, k_2, \ldots, k_{n-1}$ satisfy

$$\begin{aligned} m_1 k_1 &\equiv 1 (\mathrm{mod}\, m_2 m_3 \ldots m_n) \\ m_1 m_2 k_2 &\equiv 1 (\mathrm{mod}\, m_3 \ldots m_n) \\ &\vdots \\ m_1 m_2 \ldots m_{n-1} k_{n-1} &\equiv 1 (\mathrm{mod}\, m_n). \end{aligned} \qquad (3)$$

Before proving the theorem we recall some elementary results of number theory.

Proposition 2.2: *If $a \equiv 1 (mod\, m_1 m_2 \ldots m_n)$ then $a \equiv 1 (mod\, m_1)$, $a \equiv 1 (mod\, m_2)$,..., $a \equiv 1 (mod\, m_n)$.*

Proposition 2.3: *If $gcd(m_1, m_2)=1$ then there is a k such that $m_1 k \equiv 1 (mod\, m_2)$.*

Proposition 2.4. *If $gcd(m_1, m_2)=1$ and $gcd(m_1, m_3)=1$, then $gcd(m_1, m_2 m_3)=1$.*

Now we prove the Theorem.

Proof: By the Proposition 2.3 and Proposition 2.4 there exists k_i's satisfying congruences in (3). We prove that $\bar{x}$ in (2), satisfies every congruence in (1).

Clearly $\bar{x} \equiv x_1 (\mathrm{mod}\, m_1)$.

Next

$$\bar{x} \equiv [x_1 + k_1 m_1 (x_2 - x_1)] (mod\, m_2)$$
$$\bar{x} \equiv x_1 (mod\, m_2) + k_1 m_1 (x_2 - x_1) (mod\, m_2)$$

Since $m_1 k_1 \equiv 1 (mod\, m_2 m_3 \ldots m_n)$,

from Proposition 2.2, $m_1 k_1 \equiv 1 (mod\, m_2)$. Therefore

$$\bar{x} \equiv x_1 (mod\, m_2) + (x_2 - x_1) (mod\, m_2)$$
$$\equiv x_2 (mod\, m_2).$$

Similarly,

$$\bar{x} \equiv [x_1 + k_1 m_1 (x_2 - x_1) + k_2 m_1 m_2 (x_3 - x_2)] (mod\, m_3)$$
$$\bar{x} \equiv x_1 (mod\, m_3) + k_1 m_1 (x_2 - x_1) (mod\, m_3) + k_2 m_1 m_2 (x_3 - x_2) (mod\, m_3).$$

From Proposition 2.2,

$k_1 m_1 \equiv 1 (mod\, m_3)$ and

$k_2 m_1 m_2 \equiv 1 (mod\, m_3)$. Therefore

$\bar{x} \equiv x_1 (mod\, m_3) + (x_3 - x_2) (mod\, m_3) \equiv x_3 (mod\, m_3)$.

Extending the above to the larger dimensions,

$$\bar{x} \equiv [x_1 + k_1 m_1 (x_2 - x_1) + k_2 m_1 m_2 (x_3 - x_2) \ldots + k_{n-1} m_1 m_2 \ldots m_{n-1} (x_n - x_{n-1})] (\mathrm{mod}\, m_n)$$

$$\equiv x_1 (mod m_n) + k_1 m_1 (x_2 - x_1) (mod m_n) + \cdots + k_{n-1} m_1 m_2 \ldots m_{n-1} (x_n - x_{n-1}) (\mathrm{mod}\, m_n)$$

$$\equiv x_1 (mod m_n) + (x_2 - x_1) (mod m_n) + \cdots + (x_n - x_{n-1}) (\mathrm{mod}\, m_n)$$

$$\equiv x_n (mod m_n).$$

Reader can easily verify uniqueness of the solution under modulo $m_1 m_2 \ldots m_n$.

Illustartive example 2.5: Consider a weighted number x=256 and the moduli set {3, 4, 5, 7}. Then

$x \equiv 1 \ (mod\ 3)$

$x \equiv 0 \ (mod\ 4)$

$x \equiv 1 \ (mod\ 5)$

$x \equiv 4 \ (mod\ 7)$.

We have to find k_1, k_2, k_3 satisfying

$3k_1 \equiv 1 (mod\ 4 * 5 * 7)$

$3^*4k_2 \equiv 1 (mod\ 5 * 7)$

$3^*4^*5k_3 \equiv 1 (mod\ 7)$.

We obtain k_1=47, k_2=3, k_3=2 satisfying the above congruences.

By the new CRT-I,

$$\bar{x} \equiv [x_1 + k_1 m_1 (x_2 - x_1) + k_2 m_1 m_2 (x_3 - x_2) + k_3 m_1 m_2 m_3 (x_4 - x_3)] (\mathrm{mod}\, m_1 m_2 m_3 m_4)$$

=256.

Compare to the CRT, the converter based on New CRT-I require no big size moduli adders. The numbers involved in the conversion are smaller than the numbers in the CRT. Therefore the New CRT-I is more useful than the CRT for practical purposes.

3. The moduli set {3^n, 3^n+1, 3^n+2}:

One of the most important considerations in the design of RNS system is the choice of moduli set. The parametrized moduli set {m_1, m_2, … , m_n }should be chosen such that

1. Each mi should be as small as possible.
2. Moduli set should have simple reverse converter set.
3. The moduli product should be large enough to implement desired number.
4. Difference between two moduli product for two consecutive values of n should be as small as possible.

We propose the parametric moduli set

$S_1 = \{3^n, 3^n+1, 3^n+2\}$ for n>=1 and it satisfy the above requirements. First we prove that S_1 is a relatively prime set, for any n.

Theorem 3.1. *The set S_1 = = {3^n, 3^n+1, 3^n+2} is a relatively prime set.*

Proof: We prove that (1) gcd(3^n, 3^n+ 1) = 1, (2) gcd(3^n+1, 3^n+2) = 1, (3)gcd(3^n, 3^n+2) = 1.

Obviously, (1) gcd(3^n, 3^n+ 1) = 1,

(2) gcd(3^n+1, 3^n+2) = 1. Suppose that p|3^n and p|3^n+2. Then by the properties of divisibility, p|3^n+2-3^n. That is p|2. But 3^n is always odd and p|3^n implies p is an odd number. Hence p = 1 proving (3).

Theorem 3.2: *For the set S_1, the multiplicative inverse set based on the Chinese Remainder Theorem (CRT) is I_1 = {(1/2)(3^n+ 1),3^n ,(1/2)(3^n+ 3)}.*

Proof: Let M = 3^n (3^n+1)(3^n +2), M_1= (3^n +1)(3^n +2), M_2= 3^n (3^n +2) and M_3= 3^n (3^n +1).

Let x ≡x_1(mod 3^n), Let x ≡x_2(mod 3^n +1),and x ≡x_3(mod 3^n+2). By the CRT we shall show that

x≡ $[M_1K_1x_1+M_2K_2x_2+M_3K_3x_3]$(mod M)

for K_1=(1/2)(3^n+1), K_2=3^n and K_3=(1/2)(3^n+3).

Claim 1: $M_1K_1 \equiv 1 (\mathrm{mod}\ 3^n)$.

We have M_1K_1=(3^n+1)(3^n +2) (1/2)(3^n+1)

=(1/2)(3^{3n}+4*3^{2n}+5*3^n+2)

and M_1K_1-1=3^{3n}/2+2*3^{2n}+(5/2)3^n=3^n(3^{2n} /2+2*3^n+(5/2)).

This prove the claim.

Claim 2: $M_2K_2 \equiv 1 (\mathrm{mod}\ 3^n+1)$.

We have M_2K_2 =3^{3n}+2*3^{2n}

and M_2K_2 -1=3^{3n}+2*3^{2n}-1

=(3^n+1)(3^{2n} +3^n-1).

This prove the claim.

Claim 3: $M_3K_3 \equiv 1 (\mathrm{mod}\ 3^n+2)$.

We have M_3 K_3=(3^n)(3^n +1)(1/2)(3^n+3)

=3^{3n}/2+2*3^{2n}+(3/2)*3^n

and M_3 K_3-1=(3^n+2)(3^{2n} /2+3^n-(1/2)).

This proves the claim.

Theorem 3.3: *For the set S_1, the multiplicative inverse set based on the New Chinese Remainder Theorem -I (New CRT-I) is I_2 = {3^n+1, (1/2)(3^n+1)}.*

Proof: Let M_1=3^n+1, M_2=3^n+2 and M_3=3^n. Let $x \equiv x_1 \ (mod 3^n)$, $x \equiv x_2 \ (mod 3^n + 1)$and $x \equiv x_3 \ (mod 3^n + 2)$. By the New CRT-I we shall show that

$$x \equiv \begin{bmatrix} x_1 + K_1 M_1 (x_2 - x_1) \\ + M_1 M_2 K_2 (x_3 - x_2) \end{bmatrix} (mod M_1 M_2 M_3)$$

for K_1=3^n+1 and K_2=(1/2)(3^n+1).

Claim 1: $M_1K_1 \equiv 1 (\mathrm{mod}\ M_2M_3)$.

We have M_1K_1=(3^n+1)^2

and M_1K_1-1=3^{2n} +2*3^n=3^n(3^n +2).

This proves the claim.

Claim 2: $M1M2K2 \equiv 1 (\mathrm{mod}\ M_3)$.

We have M1M2K2=3^{3n}/2+2*3^{2n}+(5/2)*3^n+1

and have M1M2K2-1=3^{3n}/2+2*3^{2n}+(5/2)*3^n

=(3^n)(3^{2n}/2+2*3^n+(5/2)).

This proves the claim.

4. Conclusion: The main aim of this paper is to give mathematical proof of New CRT-I which may be further studied by mathematicians so that more improvement will help the RNS conversion process. Also proposed 3 element parametric moduli set surely do better in the RNS conversion.

References:

1. N. S.Szabo and R. I.Tanaka, *Residue Arithmetic and Its Application to Computer Technology*New York: McGrew-Hill, 1997.
2. H. L. Graner, "The residue number system," IRE Trans. Electron. Comput.,vol. EC-8, June 1959, pp. 140-147.
3. *Ritu Agarwal,* Sets of the Generating Functions for the Polynomials ...; Mathematical Sciences International Research Journal ISSN 2278 – 8697 Vol 2 Issue 1 (2013), Pg 9-12
4. C. Chiang and L. Johnsson,"Residue arithmetic and VLSI," Proc. IEEE ICCD, 1983, pp. 80-83.
5. P. W. Beame, S. A. cook, and H. J.Hoover, "Log depth circuits for division and related problems," SIAMJ.Comput., vol.15, , 1986, pp.994-1003.
6. G. Dmauro, S. Impdedovo, and G. Pirlo, " A new technique for number comparison in the residue number systems, " IEEE Trans. Comput., vol.42, May 1993, pp. 608-612.
7. Yuke Wang, "Residue-to-Binary Converters Based On New Chinese Remainder Theorems", IEEE Trans. On Circuits and Systems II: Analog and Digital Signal Processing, vol. 47, No. 3, March 2000, pp.197-205,.
8. E. Al-Radadi and P.Siy, "Four-Moduli Set (2, 2^n-1, 2^n+2^{n-1}-1, $2^{n+1}+2^n$-1) Simplifies the Residue To Binary Converters Based on CRT II, PERGAMON Computers and Mathematics with Applications, vol. 44, no. 12, Dec. 2002, pp. 1581-1587.
9. *Huda Khan, Deven Shah,* Proposal of Webapps Scanner on Cloud; Mathematical Sciences International Research Journal ISSN 2278 – 8697 Vol 2 Issue 2 (2013), Pg 159-162
10. 8. Mohan, P.V.A. and Premkumar, A.B., "RNS-to-Binary Converters for Two Four-Moduli Sets {2^n-1, 2^n, 2^n+1, 2^{n+1}-1} and {2^n-1, 2^n, 2^n+1, 2^{n+1}+1}", IEEE Transactions on Circuits and Systems I: Regular Papers, vol.54,no.6,June2007,pp.1245-1254.
11. C. Balasubramanyam, Ajay M.S, Amogh B. Shetty, K R Spandana, K N Seetharamu, Curve Fitting for Coarse and Fine Data Using Artificial; Mathematical Sciences international Research Journal ISSN 2278 – 8697 Vol 3 Issue 2 (2014), Pg 519-537

***

Ramananda H. S/Department of Mathematics/
St. Joseph Engineering College/ Vamanjoor/ Mangalore-575028/ Karnataka State/ INDIA.