Extending and applying garners law for four different modulator representation of codes used in cryptography

Imad Matti Bakko
imad.m.bko@almamonuc.edu.iq
AL_Ma'moon University College

Abstract

The scientist Garner introduced three laws and a method to convert modular arithmetic representation of any decimal code to its corresponding conventional representation of decimal code by using three different modules; he does not talk about the possibility of using this method to four different modules or more.

Without extending Garner's laws more than three laws, it is impossible to this method to be applicable to more than three different modules. In this paper we extend Garner's laws and an application is presented using four different modules to prove and support the correctness of our extension.

Keywords: Modular arithmetic, Garner's laws, four different modular representation, division residues.

Introduction

H. L. Garner [1][2] , introduced a usable method for converting any decimal code from modular arithmetic representation to its corresponding conventional representation

of decimal, therefore we must present something about modular arithmetic operations.

A modular arithmetic operation is a method for doing arithmetic operations besides the conventional method used (i.e. the decimal representation of numbers). This method is based on some principles of modular representation of numbers [1] [2][3].

The idea is to have several modules such as $m_1, m_2, \dots, m_r$ that have no common factors among them, and to work indirectly with residues of u mod m_1, u mod m_2, …, u mod m_r, instead of directly working with decimal number u [4][5]. We can find the representation of u in modular form by means of division, as follows:

$u_1 = u \bmod m_1$, $u_2 = u \bmod m_2$, $u_3 = u \bmod m_3$, where u_1, u_2, u_3, are called residues, hence the modular representation of u will be:

$u = (u_1 \bmod m_1 , u_2 \bmod m_2 , u_3 \bmod m_3)$ [1][2][3].

The method suggested by Garner is carried out by using constants C_{ij} for $1 \leq i \leq j \leq r$, where

$$\mathbf{C_{ij} * m_i \equiv 1 \ (modulo\ m_j)\ ,\ and\ g.c.d\ (m_i, m_j) = 1} \quad \mathbf{\dots\dots\dots\dots\dots\dots\dots\dots\ (1)}$$

(Note: g.c.d stands for greatest common divisor) [3].

Once the constants C_{ij} have been determined and satisfying (1), we can get:

$$v_1 = u_1 \bmod m_1 ,$$

…….. (2)

$$v_2 = (u_2 - v_1) * C_{12} \bmod m_2 ,$$

… ……. (3)

$$v_3 = ((u_3 - v_1) * C_{23} \bmod m_3 ,$$

……. (4)

$$u = v_3 * m_2 * m1 + v_2 * m_1 + v_1$$

…….. (5)

Garner applied these laws for three different module, since he uses u1, u2, u3, and m1, m2, m3.

1. Applying practical work on three different modules of Garner's laws:

Suppose we have (1 mod 2, 1 mod 3, 4 mod 5) as a modular representation, where:

u1 = 1, m1 = 2, u2 = 1, m2 = 3, u3 = 4, m3 = 5

By using these laws the decimal equivalence of the modular representation (1 mod 2, 1 mod 3, 4 mod 5) will be the decimal 19 , and as follows:

First we find C_{12}, C_{13}, C_{23} according to Garner's law(1) :

$C_{12} \times m_1 \equiv 1 \bmod m_2$

$C_{12} \times 2 \equiv 1 \bmod 3 \quad \rightarrow C_{12} = 2$

$C_{13} \times m_1 \equiv 1 \bmod m_3$

$C_{13} \times 2 \equiv 1 \bmod 5 \quad \rightarrow C_{13} = 3$

$C_{23} \times m_2 \equiv 1 \bmod m_3$

$C_{23} \times 3 \equiv 1 \bmod 5 \quad \rightarrow C_{23} = 2$

Secondly, we find v_1, v_2, v_3, and according to Garner's laws (2, 3, 4), and as follows:

$v_1 = u_1 \bmod m_1$

$v_1 = 1 \bmod 2 \quad \rightarrow v_1 = 1$

$v_2 = (u_2 - v_1) \times C_{12} \bmod m_2$

$v_2 = (1 - 1) \times 2 \bmod 3$

$= 0 \bmod 3 = 0 \quad \rightarrow v_2 = 0$

$v_3 = ((u_3 - v_1) \times C_{13} - v_2) C_{23} \bmod m_3$

$= ((4 - 1) \times 3 - 0) \times 2 \bmod 5$

$= 18 \bmod 5 \quad \rightarrow v_3 = 3$

Finally, by using Garner's law(5), we find the decimal number u as follows:

$u = v_3 \times m_2 \times m_1 + v_2 \times m_1 + v_1$

$= 3 \times 3 \times 2 + 0 \times 2 + 1$

$u = 19$.

i.e. $u = 19 = (1 \bmod 2, 1 \bmod 3, 4 \bmod 5)$.

Now, the question is: what about four different modules ?

can these laws be applied for four different modules ?

The answer to these questions is certainly no. We cannot applied these laws , since it deals with only three different modules.

From this point, we started to develop a method to expand and deals with higher modular arithmetic representation.

2. Applying four different modules (researcher theory part and practical work):

2.1 Theoritical part:

To deal with four different modular representation, we must extend Garner's laws. We extend Garner's laws as follows:

First, we extend $\mathbf{C_{ij}\, m_i \equiv 1 \ (modulo\ m_j)}$ as follows and as illustrated in bold types**:**

1. $C_{12} \times m_1 \equiv 1 \bmod m_2$ **2.** $C_{13} \times m_1 \equiv 1 \bmod m_3$

3. $C_{23} \times m_2 \equiv 1 \bmod m_3$

4. $\mathbf{C_{14} \times m_1 \equiv 1 \bmod m_4}$ **5.** $\mathbf{C_{24} \times m_2 \equiv 1 \bmod m_4}$

6. $\mathbf{C_{34} \times m_3 \equiv 1 \bmod m_4}$

Secondly, we extend the following also as illustrated in bold type :

$v_1 = u_1 \bmod m_1$,

$v_2 = (u_2 - v_1) \times C_{12} \bmod m_2$,

$v_3 = ((u_3 - v_1) \times C_{23} \bmod m_3$

$$v_4 = (((u_4 - v_1) \times C_{14} - v_2) \times C_{24} - v_3) \times C_{34} \bmod m_4 \quad \text{..... (6)}$$

Finally, we extend,

$u = v_3 m_2 m_1 + v_2 m_1 + v_1$

as the following:

$$u = v_4 \times m_3 \times m_2 \times m_1 + v_3 \times m_2 \times m_1 + v_2 \times m_1 + v_1 \quad \text{..... (7)}$$

2.2 Practical part:

to show, and prove the correctness of the extended laws, which we are mentioned above, we take the following four different modules to represent the decimal number 19, as an example:

(1 mod 2, 1 mod 3, 4 mod 5, 5 mod 7)

Where,

u1 = 1, m1 = 2, u2 = 1, m2 = 3, u3 = 4, m3 = 5, u4 = 5, m4 = 7.

We use the extended laws from 1 to 7, and as follows:

First we find C_{12}, C_{13}, C_{23}, C_{14}, C_{24}, C_{34}

$C_{12} \times m_1 \equiv 1 \bmod m_2$

$C_{12} \times 2 \equiv 1 \bmod 3 \rightarrow C_{12} = 2$

$C_{13} \times m_1 \equiv 1 \bmod m_3$

$C_{13} \times 2 \equiv 1 \bmod 5 \rightarrow C_{13} = 3$

$C_{23} \times m_2 \equiv 1 \bmod m_3$

$C_{23} \times 3 \equiv 1 \bmod 5 \rightarrow C_{23} = 2$

$\mathbf{C_{14} \times m_1 \equiv 1 \bmod m_4}$

$C_{14} \times 2 \equiv 1 \bmod 7 \rightarrow C_{14} = 4$

$\mathbf{C_{24} \times m_2 \equiv 1 \bmod m_4}$

$C_{24} \times 3 \equiv 1 \bmod 7 \rightarrow C_{24} = 5$

$\mathbf{C_{34} \times m_3 \equiv 1 \bmod m_4}$

$C_{34} \times 5 \equiv 1 \bmod 7 \rightarrow C_{34} = 3$

Secondly, we find v_1, v_2, v_3, and v_4 :

$v_1 = u_1 \bmod m_1$

$v_1 = 1 \bmod 2 \rightarrow v_1 = 1$

$v_2 = (u_2 - v_1) \times C_{12} \bmod m_2$

$v_2 = (1 - 1) \times 2 \bmod 3$

$= 0 \bmod 3 = 0 \rightarrow v_2 = 0$

$v_3 = ((u_3 - v_1) \times C_{13} - v_2) C_{23} \bmod m_3$

$= ((4 -1) \times 3 - 0) \times 2 \bmod 5$

$= 18 \bmod 5 \rightarrow v_3 = 3$

$\mathbf{v_4 = (((u_4 - v_1) \times C_{14} - v_2) \times C_{24} - v_3) \times C_{34} \bmod m_4}$

……. (6)

$= (((5 - 1) \times 4 - 0) \times 5 - 3) \times 3 \bmod 7$

$= ((4 \times 4 - 0) \times 5 - 3) \times 3 \bmod 7$

$= (16 \times 5 - 3) \times 3 \bmod 7$

$= 77 \times 3 \bmod 7$

$= 231 \bmod 7 \rightarrow v_4 = 0$

Finally, we find the corresponding decimal number u as follows:

$$\mathbf{u = v_4 \times m_3 \times m_2 \times m_1 + v_3 \times m_2 \times m_1 + v_2 \times m_1 + v_1}$$

…….. (7)

$$u = 0 \times 5 \times 3 \times 2 + 3 \times 3 \times 2 + 0 \times 2 + 1$$

$$u = 0 + 18 + 0 + 1$$

u = 19 , which is the same decimal number previously we used for the three different modular representation of the decimal number 19:

19 = (1 mod 2, 1 mod 3, 4 mod 5).

3. Summary of the results.

a. we applied our work on a single code to show the strength of the method, however, in the same way we can applied this method on a stream of text codes, (i.e. encryption of a text and decryption of cipher text, this is left for future work) [6][7].

b. Applying three different or four different module representation to the same code give us the same result, but the benefit of applying four different modular representation to any code will be more secure in all cryptographic applications, since it will become more harder in decryption of the cipher text [8][9][10].

Conclusion

1. In this work, we extend garner's laws to four different moduli suitable to be more secure in encrypt plain text codes and to decrypt a cipher text codes.

2. Ciphering a text by using four different module and deciphering will be more secure.

3. we recommend to other researchers to extend this subject to be more secure to five , six or more different modulus's for the same purpose, but the subject need to further extension of Garner's laws, for example the modular representation of the decimal number 19 maybe in the following different modular representations:

19 = (1 mod 2, 1 mod 3, 4 mod 5)

……. format 1

19 = (1 mod 2 , 1 mod 3 , 4 mod 5 , 5 mod 7)

…….. format 2

19 = (1 mod 2, 1 mod 3, 4 mod 5, 5 mod 7, 1 mod 9)

…… format 3

19 = (1 mod 2 , 1 mod 3 , 4 mod 5 , 5 mod 7 , 1 mod 9 , 8 mod 11) ……. format 4

Format 3 and 4 need for more extension for Garner's laws therefore its recommended.

4. The choice of these formats are not random, In case of module and format 1, there are three different residues; hence the number of permutations is 3! = 6. In case of format 2, there are four different module and residues; hence the number of permutations is 4! = 24. In case of format 3, there are five different module and residues; hence the number of permutations is 5! = 120. In case of format 6, there are six different moduli and residues; hence the number of permutations is 6! = 720. In general it's n! , this makes the problem harder to decipher the codes but this needs to build tables for each kind of permutation used to cipher plain text.

References

[1] BAKKO. I.M , " Proposing a method to perform modular arithmetic operations on integer numbers with different moduli ", international journal of research in computer application and robotics, Volume 3, Issue 3, March 2015.

[**2**] ALFRED. J. MENEZES, PAUL C. VAN OORSCHET, SCOTT A. VANSTONE, "Hand book of Applied Cryptography", CRC PRESS, India, 1997.

[**3**] DONALD KNUTH, “The Art of Computer Programming”, volume 2: Semi Numerical Algorithms. Third Edition, Addison-Wesley, 1997.

[**4**] GARNER .H.L., “The Residue Number System”, IRE Trans. Electro Comp. vole EC8, 1959.

[**5**] History of Residue Number System – University of Jordan-A www.yahoo.com.

[**6**] HOFFSTEIN, J., PIPHER, J., SIVERMAN., J.H., and SILVERMA, J.H." An introduction to mathematical cryptography" (Vol. 1). New York: Springer (2008).

[**7**] NEAL kABLITZ, “A Course in Number Theory and Cryptography”, Springer-verlag, Second Edition, 2011, Page 19, 21, 24,

[**8**] BALDONI M.W., CILIBERTO C., PIACENTINI CATTANEO G.M. “Elementary Number theory, Cryptography and Codes” Springer-verlag Berlin Heidelberg, 2008, Page 122.

[**9**] THOMAS KOSHY, “Elementary Number Theory with Applications”, ELSEVIER INC. Page 212,241, second Edition 2007.

[**10**] HANS DELFS, HELMUT KNEBL,”Introduction to Cryptography, Principles and Applications”, Springer-verlag Berlin Heidelberg, 2007, page 35.