INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

PROPOSING A METHOD TO PERFORM MODULAR ARITHMETIC OPERATIONS ON INTEGER NUMBERS WITH DIFFERENT MODULI

Imad Matti Bakko [1]

[1] *Lecturer in Computer Science Dep. Alma'moon University College, Baghdad, Iraq*
E-mail: emad_matti@yahoo.com

Abstract: - The mathematician H.L. Garner wrote three laws concerning modular arithmetic operations on integer numbers, i.e. addition, multiplication, and subtraction. These laws are true when the modular representation of the numbers to be added, multiplied, or subtracted are in the same moduli. Garner and others did not mentioned about a case when the modular representation of the numbers are different, which is a general case. In such a case we proved in this paper with many examples that these laws cannot be applied when the modular representation of the numbers to be added, multiplied, or subtracted are in different moduli. In this paper also we introduced a perfect solution to this problem. The solution proposes a method including a role when applied on numbers with different moduli; the Garner's laws will be true. In this paper we proposed also a number of tables including sets of numbers with their moduli, these tables are important to apply our method. The paper includes also a lot of examples which proves the trueness of our method; also we wrote a program to transfer integer numbers to their modular representation.

Keywords: - Garner's Laws, Modular Arithmetic Operations, modulo (mod), Moduli, Residue

1. Introduction

Modular Arithmetic can be handled mathematically by introducing a Congruence relation ($\equiv$). First, we introduce some definitions:

Definition (1):

For a positive integer n, two integers a and b are said to be congruent modulo n, written: $a \equiv b \pmod{n}$, if their deference a - b is an integer multiple of n (or n divides (a – b)). The number n is called the modulus of the congruence, for example $38 \equiv 14 \pmod{12}$, i.e.

38 is equivalent to 14 modulus 12.

Because 38 – 14 = 24, which is a multiple of 12.

The same rule holds for negative values:

-8 $\equiv$ 7 (mod 5), 2 $\equiv$ -3 (mod 5), -3 $\equiv$ -8 (mod 5) **[1].**

Definition (2):

A Residue Number System is defined by a set of N integer constants, {m_1, m_2, m_3, … , m_N }, referred to as the moduli. Let M be the least common multiple of all the m_i, (i.e. M = $\prod_{i=1}^{N} m_i$).

Any arbitrary integer X smaller than M can be represented in the defined residue number system as a set of N smaller integers { x_1, x_2, x_3, … , x_N } with X $\equiv$ x_i modulo m_i **[2], [3],** for example:

3 $\equiv$ 1 mod 2,

3 $\equiv$ 0 mod 3, → **Residue Number System**, where,

3 $\equiv$ 3 mod 5 . m_1=2, m_2=3, m_3=5, and x_1=1, x_2=0, x_3=3.

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 arithmetic representation of numbers [**1**] , [**2**] , [**4**] , [**6**] , [**7**].

The idea is to have several " moduli " , m_1 , m_2 , … , m_r that contain no common factors, and to work indirectly with " residues " **u mod m_1**, **u mod m_2** , **… , u mod m_r** , instead of directly with the number **u [4].**

For convenience, let

u_1 = u mod m_1, u_2 = u mod m_2, … , u_r = u mod m_r . **(1)**

The advantages of modular representation is that addition, subtraction, and multiplication are very simple, as follows :

$(u_1,…,u_r) + (v_1,…,v_r) = ((u_1 + v_1) \bmod m_1 ,…,(u_r + v_r) \bmod m_r)$, **(2)**

$(u_1,…,u_r) - (v_1,…,v_r) = ((u_1 - v_1) \bmod m_1 ,…,(u_r - v_r) \bmod m_r)$, **(3)**

$(u_1,…,u_r) \times (v_1,…,v_r) = ((u_1 \times v_1) \bmod m_1 ,…,(u_r \times v_r) \bmod m_r)$ [1][2]. **(4)**

1.1 Converting integers from Decimal to Modular representation

Suppose we have an integer number u , and we have three moduluses m_1 , m_2 , m_3 . We can find the representation of u in modular form by means of division [**1**] , [**2**], and as follows:

u_1 = u mod m_1 , u_2 = u mod m_2 , u_3 = u mod m_3 , where, u_1, u_2, u_3, are called residues, hence ,The modular representation of u is :

$u = (\ u_1 \bmod m_1\ ,\ \ u_2 \bmod m_2\ ,\ \ u_3 \bmod m_3\ )$

Example (1): let u = 1, and let we have the moduluses m_1=2, $m_{2=}$3, m_3=5.

Now, 1 mod 2 = 1 , 1 mod 3 = 1 , 1 mod 5 = 1 , hence , the modular representation of u = 1 is :

u = (1 mod 2 , 1 mod 3 , 1 mod 5)

Example (2) : let u = 2 , m_1 = 2 , m_2 = 3 , m_3 = 5.

Now, 2 mod 2 = 0 , 2 mod 3 = 2 , 2 mod 5 = 2 , hence ,

The modular representation of u = 2 is:

u = (0 mod 2 , 2 mod 3 , 2 mod 5)

Example (3): let u = 3 , m_1 = 2 , m_2 = 3 , m_3 = 5

Now, 3 mod 2 = 1 , 3 mod 3 = 0 , 3 mod 5 = 3 , hence ,

The modular representation of u = 3 is:

u = (1 mod 2 , 0 mod 3 , 3 mod 5)

1.2 Converting Modular number to Decimal number.

H. L. Garner [**4**] , [**5**] , introduced a usable method for conversion from ($u_1, \dots, u_r$) to u , such a method can be carried out using

Constants C_{ij} for $1 \le i < j \le r$, where ,

$$\mathbf{C_{ij}\, m_i \equiv 1\ (modulo\ m_j)\ ,\ and\ \ gcd(m_i, m_j) = 1} \qquad \mathbf{(5)}$$

(**Note 1**: the symbol $\equiv$ stand for congruence).

(**Note 2**: **gcd** stand for greatest common divisor) **[3].**

Once the constants C_{ij} have been determined satisfying (5) , we can get

$$\mathbf{v_1 = u_1 \bmod m_1\ ,}$$

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

$$\mathbf{v_3 = ((u_3 - v_1)\, C_{13} - v_2)\, C_{23} \bmod m_3\ .} \qquad \mathbf{(6)}$$

…

$$v_r = (\dots((u_r - v_1)\, C_{1r} - v_2)\, C_{2r} - \dots - v_{r-1})\, C_{r-1} \bmod m_r$$

$$\mathbf{then\ ,\ u = v_r m_{r-1} \dots m_2 m_1 + \dots + v_3 m_2 m_1 + v_2 m_1 + v_1} \qquad \mathbf{(7)}$$

u is the number satisfying the conditions :

$$\mathbf{0 \le u < m\ ,\quad u \equiv u_j\ (mod\ m_j)\quad for\ \ 1 \le j \le r} \qquad \mathbf{(8)}$$

Example (**4**): Referring to example (1), we recompute the decimal u from the following modular representation of u:

u = (1 mod 2 , 1 mod 3 , 1 mod 5)

i.e. $u \equiv 1 \bmod 2$

$u \equiv 1 \mod 3$

$u \equiv 1 \mod 5$

Where, $u_1 = u_2 = u_3 = 1$, are the residues , and

$m_1 = 2$, $m_2 = 3$, $m_3 = 5$, are the module (moduluses).

First, we must find the constants C_{12} , C_{13} , C_{23} from law (5) as follows:

$C_{12}\, m_1 \equiv 1 \mod m_2$

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

To find C_{13} :

$C_{13}\, m_1 \equiv 1 \mod m_3$

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

To find C_{23} :

$C_{23}\, m_2 \equiv 1 \mod m_3$

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

Secondly , we use Garner 's laws (6) , to find v_1 , v_2 , v_3 as follows :

$v_1 = u_1 \mod m_1$

$v_1 = 1 \mod 2 \rightarrow v_1 = 1$

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

$v_2 = (1 - 1) \times 2 \mod 3 \rightarrow v_2 = 0$

$v_3 = ((u_3 - v_1)\, C_{13} - v_2)\, C_{23} \mod 5$

$v_3 = ((1 - 1) \times 3 - 0) \times 2 \mod 5 \rightarrow v_3 = 0$

Now , according to Garner's law (7) :

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

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

$u = 1$ in decimal representation.

Example (5) : Referring to example (2), the modular rep. of decimal 2 is:

$u = (\ 0 \mod 2\ ,\ \ 2 \mod 3\ ,\ \ 2 \mod 5\ )$

where , $u_1 = 0$, $u_2 = 2$, $u_3 = 2$, and $m_1 = 2$, $m_2 = 3$, $m_3 = 5$.

To find C_{12} , C_{13} , C_{23} , we use Garner's law (5) :

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

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

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

To find v_1 , v_2 , and v_3 , we use Garner's law (6) :

$v_1 = u_1 \mod m_1$

$v_1 = 0 \mod 2 \rightarrow v_1 = 0$

$v_2 = (u_2 - v_1)\, C_{12} \mod m_3$

$v_2 = (2 - 0) \times 2 \mod 3$

$v_2 = 4 \mod 3 \rightarrow v_2 = 1$

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

$v_3 = ((2 - 0) \times 3 - 1) \times 2 \mod 5$

$v_3 = 10 \mod 5 \rightarrow v_3 = 0$

Hence, by using Garner's law (7) :

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

$u = 0 \times 3 \times 2 + 1 \times 2 + 0 \rightarrow u = 2$ in decimal.

Example (6): referring to example (3) , the modular representation of the decimal number 3 is:

$u = (1 \mod 2 ,\ 0 \mod 3 ,\ 3 \mod 5)$

Where , $u_1 = 1$, $u_2 = 0$, $u_3 = 3$, and $m_1 = 2$, $m_2 = 3$, $m_3 = 5$.

To find C_{12} , C_{13} , C_{23} we us Garner's law (5) , as follows:

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

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

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

Now , finding v_1 , v_2 , v_3 , by using Garner's law (6):

$v_1 = u_1 \mod m_1$

$= 1 \mod 2 \rightarrow v_1 = 1$

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

$= (0 - 1) \times 2 \mod 3$

$= -2 \mod 3 = (-2 + 3) \mod 3 \rightarrow v_2 = 1$

$v_3 = ((u_3 - v_1)\, C_{13} - v_2)\, C_{23} \mod 5$

$= ((3 - 1) \times 3 - 1) \times 2 \mod 5$

$= 10 \mod 5 \rightarrow v_3 = 0$

Finding the decimal number u , by using Garner's law (7):

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

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

$u = 3$ in decimal representation .

2. Applying Modular Arithmetic Operations with different moduli

Garner supposed in his laws , 2 , 3 , and 4 , that the modular numbers to be added , subtracted , and multiplied , with their results , must be of the same

moduli , otherwise , these laws cannot be applied , since they will lead to error results . Consider the following situations:

Example (7): add the decimal numbers 8 , 10 , and 15 in modular rep.

8 = (0 mod 2 , 2 mod 3 , 3 mod 5)

10 = (0 mod 2 , 1 mod 3 , 0 mod 5)

15 = (1 mod 2 , 0 mod 3 , 0 mod 5)

According to the addition law (2) , the result of the addition must be:

= ((0 + 0 + 1) mod 2 , (2 + 1 + 0) mod 3 , (3 + 0 + 0) mod 5)

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

= (1 mod 2 , 0 mod 3 , 3 mod 5) → modular addition result

This modular number is not the decimal number 33 .

To check the above modular number is not 33 , let us use Garner's law (5) , (6) , and (7) , to convert it to a decimal number.

From the above modular result of addition, we have :

$u_1 = 1$, $u_2 = 0$, $u_3 = 3$, and $m_1 = 2$, $m_2 = 3$, $m_3 = 5$

To find C_{12} , C_{13} , C_{23} we us Garner's law (5) , as follows:

$C_{12} \times 2 \equiv 1 \mod 3$ → $C_{12} = 2$

$C_{13} \times 2 \equiv 1 \mod 5$ → $C_{13} = 3$

$C_{23} \times 3 \equiv 1 \mod 5$ → $C_{23} = 2$

Now , finding v_1 , v_2 , v_3 , by using Garner's law (6):

$v_1 = u_1 \mod m_1$

$= 1 \mod 2$ → $v_1 = 1$

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

$= (0 - 1) \times 2 \mod 3$

$= -2 \mod 3 = (-2 + 3) \mod 3$ → $v_2 = 1$

$v_3 = ((u_3 - v_1) C_{13} - v_2) C_{23} \mod 5$

$= ((3 - 1) \times 3 - 1) \times 2 \mod 5$

$= 10 \mod 5$ → $v_3 = 0$

Finding the decimal number u , by using Garner's law (7):

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

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

u = 3 in decimal representation , which is error result ($33 \neq 3$).

Example (8): multiply the decimal numbers 7 by 8 in modular forms:

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

8 = (0 mod 2 , 2 mod 3 , 3 mod 5)

According to the multiplication law (4) , the result of the above multiplication in modular representation must be equal to: (

$(1 \times 0) \bmod 2 , \quad (1 \times 2) \bmod 3 , \quad (2 \times 3) \bmod 5)$

$= (0 \bmod 2 , \quad 2 \bmod 3 , \quad 6 \bmod 5)$

$= (0 \bmod 2 , \quad 2 \bmod 3 , \quad 1 \bmod 5)$

This modular number is not the decimal number 56. To check it's not 56 , let's use Garner's laws 5 , 6 , and 7 , respectively:

The modular number above has the following residues, and moduli

$u_1 = 0 , \ u_2 = 2 , \ u_3 = 1 , \text{ and } m_1 = 2 , \ m_2 = 3 , \ m_3 = 5$

Finding C_{12} , C_{13} , and C_{23} as follows:

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

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

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

Finding v_1 , v_2 , and v_3 , as follows:

$v_1 = u_1 \bmod m_1$

$v_1 = 0 \mod 2 \rightarrow v_1 = 0$

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

$= (2 - 0) \times 2 \mod 3$

$= 4 \mod 3 \rightarrow v_2 = 1$

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

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

$= 4 \mod 5 \rightarrow v_3 = 4$

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

$= 4 \times 3 \times 2 + 1 \times 2 + 0.$

$= 24 + 2 = 26 \neq 56$

2.1 Proposed Method To Get Correct Results In Modular Arithmetic Operations.

To get correct results, We carried out many trial and error operations on samples of decimal numbers from 1 to 150 , and converting them to modular representation , and back again to decimal by using Garner's laws (1) ,(5) ,(6) and (7).

To get right answers by applying Garner's laws 2 , 3 , and 4 , the paper propose to classify the decimal numbers into groups of sets , each set of numbers have its own moduli , as listed in Tables (1) , and (2).

Table (1): Decimal Number Sets With Their Moduli Type (2, 3, ---)

Set number	Decimal number set	Moduli Set
1	{ 0 , 1 , 2 , . . . , 29 }	(2, 3, 5)
2	{ 0 , 1 , 2 , . . . , 41 }	(2, 3, 7)
3	{ 0 , 1 , 2 , . . . , 65 }	(2, 3, 11)
4	{ 0 , 1 , 2 , . . . , 77 }	(2, 3, 13)
5	{ 0 , 1 , 2 , . . . ,101 }	(2, 3, 17)
6	{ 0 , 1 , 2 , . . ., 113 }	(2, 3, 19)
7	{ 0 , 1 , 2 , . . . , 137 }	(2, 3, 23)
8	{ 0 , 1 , 2 , . . . , 149 }	(2, 3, 25)
. . . .	. . .	. . .

Table (2): Decimal Number Sets With Their Moduli Type (1, 2, ---)

Set number	Decimal number set	Moduli Set
1	{ 0, 1, 2, . . . , 5 }	(1 , 2 , 3)
2	{ 0, 1, 2, . . . , 9 }	(1 , 2 , 5)
3	{ 0, 1, 2, . . . , 13 }	(1 , 2 , 7)
4	{ 0, 1, 2, . . . , 17 }	(1 , 2 , 9)
5	{ 0, 1, 2, . . . , 21 }	(1 , 2 , 11)
6	{ 0, 1, 2, . . . , 25 }	(1 , 2 , 13)
7	{ 0, 1, 2, . . . , 29 }	(1 , 2 , 15)
8	{ 0, 1, 2, . . . , 33 }	(1 , 2 , 17)
9	{ 0, 1, 2, . . . , 37 }	(1 , 2 , 19)
10	{ 0, 1, 2, . . . , 41 }	(1 , 2 , 21)
. . .	. . .	. . .

Table (3), and Table (4), summarize some of the work we done on a samples of decimal numbers and their different residues with respect to their moduli. The results in the tables are successfully achieved by the division operation and recomputed back by Garner's laws.

Table (3): Numbers and their Residues with respect to Moduli (2,3,--)

Decimal No u	Residue (u1,u2,u3)	Moduli (m1,m2,m3)	Decimal No u	Residue (u1,u2,u3)	Moduli (m1,m2,m3)
0	(0, 0, 0)	(2, 3, 5)	16	(0, 1, 1)	(2, 3, 5)
1	(1, 1, 1)	(2, 3, 5)	17	(1, 2, 2)	(2, 3, 5)
2	(0, 2, 2)	(2, 3, 5)	18	(0, 0, 3)	(2, 3, 5)
3	(1, 0, 3)	(2, 3, 5)	19	(1, 1, 4)	(2, 3, 5)
4	(0, 1, 4)	(2, 3, 5)	20	(0, 2, 0)	(2, 3, 5)
5	(1, 2, 0)	(2, 3, 5)	21	(1, 0, 1)	(2, 3, 5)
6	(0, 0, 1)	(2, 3, 5)	22	(0, 1, 2)	(2, 3, 5)

7	(1, 1, 2)	(2, 3, 5)	23	(1, 2, 3)	(2, 3, 5)
8	(0, 2, 3)	(2, 3, 5)	24	(0, 0, 4)	(2, 3, 5)
9	(1, 0, 4)	(2, 3, 5)	25	(1, 1, 0)	(2, 3, 5)
10	(0, 1, 0)	(2, 3, 5)	26	(0, 2, 1)	(2, 3, 5)
11	(1, 2, 1)	(2, 3, 5)	27	(1, 0, 2)	(2, 3, 5)
12	(0, 0, 2)	(2, 3, 5)	28	(0, 1, 3)	(2, 3, 5)
13	(1, 1, 3)	(2, 3, 5)	29	(1, 2, 4)	(2, 3, 5)
14	(0, 2, 4)	(2, 3, 5)	30	(0, 0, 2)	(2, 3, 7)
15	(1, 0, 0)	(2, 3, 5)	31	(1, 1, 3)	(2, 3, 7)

Table (4): Numbers and their Residues with respect to Moduli (1,2,--)

Decimal No u	**Residue (u1,u2,u3)**	**Moduli (m1,m2,m3)**	**Decimal No u**	**Residue (u1,u2,u3)**	**Moduli (m1,m2,m3)**
0	(0, 0, 0)	(1, 2, 3)	11	(0, 1, 4)	(1, 2, 7)
1	(0, 1, 1)	(1, 2, 3)	12	(0, 0, 5)	(1, 2, 7)
2	(0, 0, 2)	(1, 2, 3)	13	(0, 1, 6)	(1, 2, 7)
3	(0, 1, 0)	(1, 2, 3)	14	(0, 0, 5)	(1, 2, 9)
4	(0, 0, 1)	(1, 2, 3)	15	(0, 1, 6)	(1, 2, 9)
5	(0, 1, 2)	(1, 2, 3)	16	(0, 0, 7)	(1, 2, 9)
6	(0, 0, 1)	(1, 2, 5)	17	(0, 1, 8)	(1, 2, 9)
7	(0, 1, 2)	(1, 2, 5)	18	(0, 0, 7)	(1, 2, 11)
8	(0, 0, 3)	(1, 2, 5)	19	(0, 1, 8)	(1, 2, 11)
9	(0, 1, 4)	(1, 2, 5)	20	(0, 0, 9)	(1, 2, 11)
10	(0, 0, 3)	(1, 2, 7)	21	) (0, 1, 10	(1, 2, 11)

Garner's laws 2 , 3 , and 4 will be correct when the numbers to be added , or subtracted , or multiplied with their results are within the same set of numbers with their own moduli , otherwise , the results of the modular operations will be wrong. Consider the following examples:

Example (9): Find the result of adding 5 and 10 in modular rep.

5 = (1 mod 2 , 2 mod 3 , 0 mod 5)

10 = (0 mod 2 , 1 mod 3 , 0 mod 5)

According to Garner's law (2) the result will be :

= ((1 + 0) mod 2 , (2 + 1) mod 3 , (0 + 0) mod 5)

= (1 mod 2 , 3 mod 3 , 0 mod 5)

= (1 mod 2 , 0 mod 3 , 0 mod 5)

Referring to table (1) , since the numbers 5 , 10 , and their result 15 are in the same set of numbers and within the same moduli , and by Introducing the formula **Dynamic Range**: **[0 ,** $\prod_{i=1}^{N} m_i - 1$ **]** [8],

5 , 10 , 15 are within the set from 0 to ($m_1 \times m_2 \times m_3 - 1$)

= ($2 \times 3 \times 5 - 1$) = 30 – 1 = 29. Hence , the result of the addition (1 mod 2 , 0 mod 3 , 0 mod 5) is 15.

We can check that it's true by using Garner's laws 6 , 7.

Example (10): find the result of adding 13 and 20 in modular rep.

$13 = (1 \bmod 2 , \quad 1 \bmod 3 , \quad 3 \bmod 5)$

$20 = (0 \bmod 2 , \quad 2 \bmod 3 , \quad 0 \bmod 5)$

According to Garner's law (2), the result will be :

$= ((1 + 0) \bmod 2 , \quad (1 + 2) \bmod 3 , \quad (3 + 0) \bmod 5)$

$= (1 \bmod 2 , 3 \bmod 3 , 3 \bmod 5) = (1 \bmod 2, 0 \bmod 3, 3 \bmod 5)$

This number is 3 , which is not the true answer 33 , we can check that by using Garner's laws 6 , and 7. Referring to table (1) , the numbers 13 , 20 , are in the same set of numbers and within the same moduli : i.e.

13 , 20 are within the set from 0 to $(m_1 \times m_2 \times m_3 - 1)$

$= (2 \times 3 \times 5 - 1) = 30 - 1 = 29$. But the result of the addition 33 is in another set of numbers with other moduli from 0 to

$(m_1 \times m_2 \times m_3 - 1) = (2 \times 3 \times 7 - 1) = 41$ **[8].**

We can check by using Garner's laws 6 , and 7 the modular number 33 is: ($1 \bmod 2 , \quad 0 \bmod 3 , \quad 5 \bmod 7$) .

Example (11): multiply the decimal numbers 7 by 9 in modular rep. :

$7 = (1 \bmod 2 , \quad 1 \bmod 3 , \quad 2 \bmod 5)$

$9 = (1 \bmod 2 , \quad 0 \bmod 3 , \quad 4 \bmod 5)$

According to the multiplication law (4) , the result must be:

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

$= (1 \bmod 2 , \quad 0 \bmod 3 , \quad 8 \bmod 5)$

$= (1 \bmod 2 , \quad 0 \bmod 3 , \quad 3 \bmod 5)$ → the modular result

This modular number is not the decimal number 63 .

To check the above modular number is not 63 , let us use Garner's law (5) , (6) , and (7) , to convert it to a decimal number.

From the above modular result of multiplication, we have :

$u_1 = 1 , \ u_2 = 0 , \ u_3 = 3 ,$ and $m_1 = 2 , \ m_2 = 3 , \ m_3 = 5$

To find C_{12} , C_{13} , C_{23} we us Garner's law (5) , as follows:

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

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

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

Now , finding v_1 , v_2 , v_3 , by using Garner's law (6):

$v_1 = u_1 \bmod m_1$

$= 1 \bmod 2$ → $v_1 = 1$

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

$= (0 - 1) \times 2 \mod 3$

$= -2 \mod 3 = (-2+3) \mod 3 \rightarrow v_2 = 1$

$v_3 = ((u_3 - v_1) C_{13} - v_2) C_{23} \mod 5$

$= ((3 - 1) \times 3 - 1) \times 2 \mod 5$

$= 10 \mod 5 \rightarrow v_3 = 0$

Finding the decimal number u , by using Garner's law (7):

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

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

$u = 3$ in decimal representation , which is error result ($63 \neq 3$).

Referring to table (1) , the numbers 7 , 9 , are in the same set of numbers and within the same moduli : i.e. 7 , 9 are within the set from 0 to ($m_1 \times m_2 \times m_3 - 1$) = ($2 \times 3 \times 5 - 1$) = $30 - 1 = 29$. But the result of the multiplication 63 is in another set of numbers with another moduli from 0 to ($m_1 \times m_2 \times m_3 - 1$) = ($2 \times\times 3 \times 11 - 1$) = 65 **[8].**

That is the reason behind the error result.

We can check by using Garner's laws 6 , and 7 , that the modular number 63 is: (1 mod 2 , 0 mod 3 , 8 mod 11) .

2.2 Proposing a Method To Perform Modular Arithmetic Operations For Numbers With Different Types Of Moduli.

To apply Garner's laws 2 , 3 , and 4 , the numbers to be added or subtracted or multiplied in modular representation , with their results must be in the same moduli , otherwise , the results will not be correct.

Now, if we want to perform modular operations on numbers , with their results are in different types of moduli, In this case , the laws of Garner 2 , 3 , and 4 cannot be applicable , consider the following :

Example (12): find the product and the sum of the numbers 3 and 6 in modular representation.

Referring to table (2) , the modular representation of 3 , 6 , and their multiplication 18 , and their sum 9 , are in the following moduli:

3 = (0 mod 1 , 1 mod 2 , 0 mod 3)

6 = (0 mod 1 , 0 mod 2 , 1 mod 5)

18 = (0 mod 1 , 0 mod 2 , 7 mod 11)

9 = (0 mod 1 , 1 mod 2 , 4 mod 5)

Here , 3 is in moduli (1 , 2 , 3) ,
6 is in moduli (1 , 2 , 5) ,
18 is in moduli (1 , 2 , 11) ,
9 is in moduli (1 , 2 , 5).

It's clear that 3 , 6 , 18 , and 9 are in different types of moduli.
In this case , we cannot apply Garner's laws 2 , 3 , and 4.
To make Garner's laws applicable, and to produce correct results, this paper suggests the following **rule**:

Change the moduli types of the numbers to be added or subtracted or multiplied to the moduli type of the result.

Now , to find the product of 3 by 6 , we must change the moduli of 3 from (1 , 2 , 3) to moduli type of the product 18 (1 , 2 , 11).
By using Garner's law (1) , the modular of the number 3 will be:
3 = (0 mod 1 , 1 mod 2 , 3 mod 11).
Changing the moduli type of 6 from (1 , 2 , 5) to moduli type 18 (1,2,11)
6 = (0 mod 1 , 0 mod 2 , 6 mod 11).
Now , we can use Garner's multiplication law safely, as follows:
= ($(0 \times 0) \ mod 1, \ (1 \times 0) \ mod 2, \ (3 \times 6) \ mod 11$)
= (0 mod 1 , 0 mod 2 , 18 mod 11)
= (0 mod 1 , 0 mod 2 , 7 mod 11)
This modular number is 18. We can check this result is true by applying Garner's laws (2) , (3) , and (4).
In the same way we can use the suggested rule to find the addition of 3 and 6, and the result will be 9, the true answer.

2.3 Subtraction in Modular Arithmetic.

Consider the following notations:
First , Referring to table (1) , and example (7) , the numbers to be added 8 , 10 , and 15 , are within the range of numbers from :
0 to ($m_1 \times m_2 \times m_3$ - 1) = ($2 \times 3 \times 5 - 1$) = 29 **[8].**
While the result of the addition, which is 33 is in another range (set) of numbers, i.e. the number 33 is within the range of numbers from:
0 to ($m_1 \times m_2 \times m_3 - 1$) = ($2 \times 3 \times 7 - 1$) = 41 **[8]**.

That is the reason behind the wrong addition result (i.e. $33 \neq 3$).

Second , Referring to table (1) , and example (8) , the numbers to be multiplied 7 , and 8 , are within the range of numbers from :

0 to ($m_1 \times m_2 \times m_3$ - 1) = ($2 \times 3 \times 5 - 1$) = 29 **[8].**

While the result of the multiplication , which is 56 is in another range (set) of numbers , i.e. the number 56 is within the range of numbers from: 0 to ($m_1 \times m_2 \times m_3 - 1$) = ($2 \times 3 \times 11 - 1$) = 65 [**8**].

That is the reason behind the wrong addition result (i.e. $56 \neq 26$).

Third, The Modular Subtraction is an exception , since the result of subtraction will be always within the same range (set) of the numbers to be subtracted. Consider the following example:

Example (13): subtract 10 from 13 in modular representation:

Referring to Garner's law (2) , and table (2) ,

The modular representation of the numbers 13 , and 10 are:

13 = (0 mod 1 , 1 mod 2 , 6 mod 7)

10 = (0 mod 1 , 0 mod 2 , 3 mod 7).

According to the subtraction law (3) , the modular result will be:

= (0 mod 1 , 1 mod 2 , 3 mod 7).

This number is 3 , which is the right answer. To check it's 3, we use Garner's laws 5 , 6 , and 7 , and as follows:

$C_{12} \times 1 \equiv 1 \ mod \ 2$ → C_{12} = 1

$C_{13} \times 1 \equiv 1 \ mod \ 7$ → C_{13} = 1

$C_{23} \times 2 \equiv 1 \ mod \ 7$ → C_{23} = 4

v_1 = 0 mod 1 = 0

v_2 = $(1 - 0) \times 1 \ mod \ 2$ → v_2 = 1

v_3 = $((3 - 0) \times 1 - 1) \times 4$ mod 7 = 8 mod 7 → v_3 = 1

Hence , u = $1 \times 2 \times 1 + 1 \times 1 + 0$ = 3.

The reason behind this correct result is that, the numbers to be subtracted with their result are in the same range of numbers from:

0 to ($m_1 \times m_2 \times m_3$ - 1) = ($1 \times 2 \times 7 - 1$) = 13, as in table (2).

Note: In this case the numbers to be subtracted must have the same moduli, otherwise, we must change the moduli of one number to another one, as suggested by the rule mentioned earlier.

2.4 C++ Program to Convert from Decimal to Modular representation.

The following program written in c++ language illustrates how to convert a decimal number to its modular representation. We convert the decimals 12, 5, 30, 9, and 13 to their modular and we checked the results with table(3), and table(4). The following are the results:

Enter **1** for moduli (2, 3, --)
Enter **2** for moduli (1, 2, --)
1
Enter any decimal number:
12
The moduli of the number 12 is: **(2**, **3**, **5**)
The modular rep. of 12 is:

12 ≡ 0 mod 2
12 ≡ 0 mod 3
12 ≡ 2 mod 5

Another run for the program:
Enter **1** for moduli (2, 3, --)
Enter **2** for moduli (1, 2, --)
2
Enter any decimal number:
5
The moduli of the number 5 is: **(1**, **2**, **3**)
The modular rep. of the number is:

5 ≡ 0 mod 1
5 ≡ 1 mod 2
5 ≡ 2 mod 3

Another run of the program:
Enter **1** for moduli (2, 3, --)
Enter **2** for moduli (1, 2, --)
1
Enter any decimal number:

30

The moduli of the number 30 is: **(2**, **3**, **7**)

The modular rep. of 30 is:

30 ≡ 0 mod 2

30 ≡ 0 mod 3

30 ≡ 2 mod 7

Another run of the program:

Enter **1** for moduli (2, 3, --)

Enter **2** for moduli (1, 2, --)

2

Enter any decimal number:

9

The moduli of the number 9 is: **(1**, **2**, **5**)

The modular rep. of the number is:

9 ≡ 0 mod 1

9 ≡ 1 mod 2

9 ≡ 4 mod 5

Another run of the program:

Enter **1** for moduli (2, 3, --)

Enter **2** for moduli (1, 2, --)

2

Enter any decimal number:

13

The moduli of the number 13 is: **(1**, **2**, **7**)

The modular rep. of 13 is:

13 ≡ 0 mod 1

13 ≡ 1 mod 2

13 ≡ 6 mod 7

```
#include<iostream.h>
#include<conio.h>
int type2()
{
```

```
int x, u1, u2, u3, m3;
cout<<"inter any decimal number\n";
cin>>x;
for( m3=5;m3<100;m3+=2)
if((2*3*m3-1)>=x) break;

{
u1=x%2;
u2=x%3;
u3=x%m3;
}
cout<<"the moduli of "<< x<<" is: (2, 3, "<<m3<<")\n";
cout<<"the modular rep. of "<<x<<" is: \n";
cout<<"     "<<x<<" ≡ "<<u1<<" mod "<<2<<"\n";
cout<<"     "<<x<<" ≡ "<<u2<<" mod "<<3<<"\n";
cout<<"     "<<x<<" ≡ "<<u3<<" mod "<<m3<<"\n";
getch();
return 0;
}
int type1()
{
int y, v1, v2, v3, m3;
cout<<"enter any decimal number\n";
cin>>y;
for( m3=3;m3<100;m3+=2)
if((1*2*m3-1)>=y) break;
{
v1=y%1;
v2=y%2;
v3=y%m3;
}
cout<<"the moduli of "<<y<<" is:(1, 2, "<<m3<<")\n";
cout<<"the modular rep. of the number is:\n";
cout<<"     "<<y<<" ≡ "<<v1<<" mod "<<1<<"\n";
cout<<"     "<<y<<" ≡ "<<v2<<" mod "<<2<<"\n";
cout<<"     "<<y<<" ≡ "<<v3<<" mod "<<m3<<"\n";
getch();
return 0;
}
main(){
clrscr();
int t;
cout<<"enter 1 for moduli (2, 3, -)\n";
cout<<"enter 2 for moduli (1, 2, -)\n";
cin>>t;
switch(t){
case 1 :type2();getch();break;
case 2 :type1();break;
defult:cout<<"error:try again\n";
getch();
}return 0;}
```

C++ Program to Convert Decimal Number to its Modular Rep.

4. Conclusion

(1) this paper is concern with three kinds of modulo , m1 , m2 , and m3 , and studied two types of moduli, namely, from (1 , 2 , 3) to (1 , 2 , 21), and from (2 , 3 , 5) to (2 , 3 , 25), as in table(1), and table(2), while the Modular context extend to a large numbers of moduli, as stated by Garner's law(1).

(2) Referring to the program written, which convert decimal number to its modular representation, it's not difficult to write a computer program to convert any modular representation of a number to its decimal, and according to Garner's laws 5, 6, and 7, so its recommended.

(3) It is recommended to write general Algorithms for converting from decimal to modular representation, and vice versa, when these operations are required.

(4) It is recommended to proceed to list another tables concerning other types of moduli, if it is required, and to write Algorithms concerning these tables and moduli, for decimal numbers.

(5) There are several different set of moduli, therefore the choice of moduli should satisfy the following properties:

a. The moduli should be as small as possible; so that the modulo operations requires less computational time.

b. The moduli should be relative prime, i.e. no two moduli should have a greatest common divisor greater than 1.

REFERENCES

[1] Modular Arithmetic Operations, www.yahoo.com, Wikipedia, The Free, Encyclopaedia.
[2] Residue Number System, www.yahoo.com , Wikipedia, The Free Encyclopaedia.
[3] Alfred J. Menezes, Paul C. Van Oorschet, Scott A. Vanstone, "Hand book of Applied Cryptography", CRC PRESS, India, 1997.
[4] Donald Knuth, “The Art of Computer Programming”, volume 2: Semi Numerical Algorithms. Third Edition, Addison-Wesley, 1997.
[5] H.L. Garner, “The Residue Number System”, IRE Trans. Electro Comp. vole EC8, 1959.
[6] History of Residue Number System – University of Jordan-A www.yahoo.com.
[7] Introduction Modular Arithmetic, www.yahoo.com.
[8] Residue Number System 2, www.yahoo.com.