1 Modular Arithmetic

M11CH1

1.1. VALUE OF NUMBERS FOR A GIVEN MODULO

Modular arithmetic is a system of arithmetic for integers, where numbers (*i.e.*, integers) wrap around when reaching a fix/certain value, called the *modulo*. It is sometimes called *modulo arithmetic* or *clock arithmetic*. The modern approach to modular arithmetic was developed by Carl Friedrich Gauss in his book 'Disquisitiones Arithmeticae', publish in 1801.

A familiar use of modular arithmetic is in the *12-hour clock* system, in which day is divided into 12-hour period.

Consider a clock. It has an hour hand and a minute hand. The hour hand completes one revolution in 12 hours. At 15 hour from mid-night, i.e., at 3 p.m. the clock shows only 3. What is the relation between these three numbers? Clearly, 3 is the remainder when 15 is divided by 12.

$$\begin{aligned} 15 \text{ hours} &= 12 \text{ hours} + 3 \text{ hours} \\ &= 1 \text{ revolution} + 3 \text{ hours} \end{aligned}$$

At 3 a.m. also, the clock shows 3, because 3 divided by 12 gives 0 quotient and 3 remainder.

Thus, at any time of the day, the hour hand shows only the remainder when the number of hours after mid-night is divided by 12. If n is the number of hours after mid-night and r is the remainder when n is divided by 12, we write

$$n = r \bmod 12$$

It is read as 'n is congruent to r modulo 12.' The minute hand completes 1 revolution in 60 minutes.

Now 80 minutes after 4 p.m. what does the minute hand show?

Obviously, not 80, rather 20 which is the remainder when 80 is divided by 60.

$$\begin{aligned} 80 \text{ minutes} &= 60 \text{ minutes} + 20 \text{ minutes} \\ &= 1 \text{ revolution} + 20 \text{ minutes} \end{aligned}$$

We write 80 = 20 mod 60

In general, if a is a positive integer, 'a' leaves a remainder 'b' when divided by a positive integer 'm', we say 'a is congruent to b modulo m'.

In symbols, we write $a = b \bmod m$ (gives remainder; divided by) ... (1)

It is read as 'a is congruent to b modulo m'.

The relation (1) gives

$$a - b = km \qquad \text{... (2)}$$

where k is an integer.

It can also be written as

$$a = km + b$$

In equation (1), 'mod m' (without parentheses) applies to the entire equation, not just to the right hand side (here, b). This notation is not to be confused with the notation 'b (mod m)' (with parentheses), which refers to the *modulo operation*. Indeep, 'b (mod m)' denotes the unique integer 'p' such that b (mod m) = p or p = b (mod m), that is, the remainder of b' when divided by m.

Example 1: *Calculate the value of*

(i) *39 for mod 6* (ii) *54 for mod 7* (iii) *217 for mod 9*

(iv) *300 for mod 12* (v) *13 for mod 15*

Solution:

(i) 39 divided by 6 leaves a remainder 3

$\Rightarrow$ Value of 39 for mod 6 is 3

$\Rightarrow$ 39 = 3 mod 6

(ii) 54 divided by 7 leaves a remainder 5

$\Rightarrow$ Value of 54 for mod 7 is 5

$\Rightarrow$ 54 = 5 mod 7

(iii) 217 divided by 9 leaves a remainder 1

$\Rightarrow$ Value of 217 for mod 9 is 1

$\Rightarrow$ 217 = 1 mod 9.

(iv) 300 divided by 12 leaves a remainder 0

$\Rightarrow$ Value of 300 for mod 12 is 0

$\Rightarrow$ 300 = 0 mod 12.

(v) 13 divided by 15 leaves a remainder 13

$\Rightarrow$ Value of 13 for mod 15 is 13

$\Rightarrow$ 13 = 13 mod 15.

Note: If the number is less than the modulo (or mod), we leave it as it is, because it is the remainder after dividing it by the modulo.

Example 2: *Simplify the following:*

(i) *59 (mod 7)* (ii) *66 (mod 4)* (iii) *98 (mod 9)*

(iv) *126 (mod 11)*

Solution:

(i) 59 (mod 7) means the remainder of 57 when divided by 7

$\therefore$ 59 divided by 7 leaves a remainder 3

$\Rightarrow$ 59 (mod 7) = 3

(ii) 66 (mod 4) means the remainder of 66 when divided by 4

$\therefore$ 66 divided by 4 leaves a remainder 2

$\Rightarrow$ 66 (mod 4) = 2

(iii) 98 (mod 9) means the remainder of 98 when divided by 9

$\therefore$ 98 divided by 9 leaves a remainder 8

$\Rightarrow$ 98 (mod 9) = 8

(iv) 126 (mod 11) means the remainder of 126 when divided by 11

$\therefore$ 126 divided by 11 leaves a remainder 5

$\Rightarrow$ 126 (mod 11) = 5

Example 3: *Find the value(s) of x, if*

(i) *34 = 2 mod x* (ii) *26 = 5 mod x*

Solution:

(i) We have, 34 = 2 mod x ... (1)

$\Rightarrow$ 2 is the remainder when 34 is divided by x

$\Rightarrow$ x is a factor of 34 – 2 = 32

Therefore, we have to find the factors of 32.

The factors of 32 are 1, 2, 4, 8, 16 and 32.

But out of these factors, only 4, 8, 16 and 32 satisfy the equation (1).

$\Rightarrow$ x = 4, 8, 16 or 32.

(ii) We have, 26 = 5 mod x ... (1)

$\Rightarrow$ x is a factor of 26 – 5 = 21

Therefore, we have to find the factors of 21.

The factors of 21 are 1, 3, 7 and 21.

But out of these factors, only 7 and 21 satisfy the equation (1).

$\therefore \quad x = 7$ or 21.

Example 4. *Find the least positive integer x such that 5x + 1 = 3 mod 4.*

Solution. We have, $5x + 1 = 3$ mod 4

$\Rightarrow$ 3 is the remainder when $5x + 1$ is divided by 4

$\Rightarrow$ 4 is a factor of $(5x + 1) - 3 = 5x - 2$

Therefore, the least positive value of x for which 4 is a factor of $5x - 2$ is 2.

$\therefore \quad x = 2.$

EXERCISE 1.1

1. Calculate the value of:

(i) 22 for mod 6 (ii) 36 for mod 5

(iii) 44 for mod 7 (iv) 67 for mod 8

(v) 72 for mod 9 (vi) 117 for mod 12

(vii) 349 for mod 15 (viii) 791 for mod 16

2. Simplify the following:

(i) 51 (mod 8) (ii) 67 (mod 7)

(iii) 83 (mod 3) (iv) 113 (mod 5)

(v) 127 (mod 12) (vi) 233 (mod 16)

(vii) 283 (mod 13) (viii) 385 (mod 17)

3. Find the value(s) of x for the following equations:

(i) $24 = 3$ mod x (ii) $34 = 4$ mod x

4. Find the least positive integers that satisfy the following:

(i) $3x = 2$ mod 4 (ii) $2x + 3 = 4$ mod 7

(iii) $5x + 4 = 3$ mod 8

1.2. MODULO ADDITION, SUBTRACTION AND MULTIPLICATION

The addition, subtraction or multiplication of two or more numbers in a given modulo (of same kind) is found by first adding, subtracting or multiplying the numbers before converting to the given modulo.

For modulo n, modulo **addition** is defined as:

$$a + b \text{ (mod } n) = \text{the remainder when } a + b \text{ is divided by } n$$

For modulo n, modulo **subtraction** is defined as:

$$a - b \text{ (mod } n) = \text{the remainder when } a - b \text{ is divided by } n$$

For modulo n, modulo **multiplication** is defined as:

$$a \times b \text{ (mod } n) = \text{the remainder when } a \times b \text{ is divided by } n$$

We can also define as:

For adding: $[a \text{ (mod } n) + b \text{ (mod } n)] \text{ (mod } n) = (a + b) \text{ (mod } n)$
or $a + b$ (mod n)

For subtracting: $[a \text{ (mod } n) - b \text{ (mod } n)] \text{ (mod } n) = (a - b) \text{ (mod } n)$
or $a - b$ (mod n)

For multiplying: $[a \text{ (mod } n) \times b \text{ (mod } n)] \text{ (mod } n) = (a \times b) \text{ (mod } n)$
or $a \times b$ (mod n)

Note: Here, a (mod n) denotes the remainder when a divided by n.

Example 5: *Find the sum of the following*:

(i) *12 + 17 (mod 3)* (ii) *46 – 13 (mod 5)*
(iii) *15 × 10 (mod 8)* (iv) *19 – 11 + 15 (mod 4)*

Solution:

(i) 12 + 17 (mod 3) = 29 (mod 3) = 2
(ii) 46 – 13 (mod 5) = 33 (mod 5) = 3
(iii) 15 × 10 (mod 8) = 150 (mod 8) = 6
(iv) 19 – 11 + 15 (mod 4) = 23 (mod 4) = 3

EXERCISE 1.2

Simplify the following:

1. 17 + 39 (mod 6)
2. 88 – 25 (mod 12)
3. 23 × 8 (mod 5)
4. 123 – 77 + 32 (mod 9)
5. 5 × 7 × 9 (mod 13)
6. 81 + 38 – 54 + 16 (mod 11)

1.3. ADDITION AND MULTIPLICATION TABLES IN GIVEN MODULO

Let S be a given finite set of integers and $a, b \in S$. Let m be a positive integer, then

(i) $a \oplus_m b$ is called '**addition modulo *m***' in S and it stands for the remainder when $a + b$ is divided by m.

Mathematically, $a \oplus_m b = a + b \pmod{m}$.

(ii) $a \otimes_m b$ is called '**multiplication modulo *m***' in S and it stands for the remainder when $a \times b$ is divided by m.

Mathematically, $a \otimes_m b = ab \pmod{m}$.

Thus, if $S = \{0, 1, 2, 3\}$, then

$2 \oplus_4 3$ = the remainder when 2 + 3 i.e., 5 is divided by 4.

$\Rightarrow \quad 2 \oplus_4 3 = 1$

$2 \otimes_4 3$ = the remainder when 2 × 3 i.e., 6 is divided by 4.

$\Rightarrow \quad 2 \otimes_4 3 = 2$

Clearly, $\oplus_4$ and $\otimes_4$ are compositions in S. They can be best described by means of a table called **composition table**.

Suppose $S = \{a_1, a_2, a_3\}$. Let us prepare the composition table for 'addition modulo m', i.e., for $\oplus_m$.

We write the composition $\oplus_m$ at the top left hand corner. Against $\oplus_m$, we write the elements of S in a row. Also below $\oplus_m$, we write the elements of S in a column.

Thus, we have a 3 × 3 table, i.e., a table having 3 rows and 3 columns. The unique element $a_i \oplus_m a_j$ i.e., the remainder when $a_i + a_j$ is divided by m, is written at the intersection of the row headed by a_i and the column headed by a_j.

Composition table for $\oplus_m$

$\oplus_m$	a_1	a_2	a_3
a_1	$a_1 \oplus_m a_1$	$a_1 \oplus_m a_2$	$a_1 \oplus_m a_3$
a_2	$a_2 \oplus_m a_1$	$a_2 \oplus_m a_2$	$a_2 \oplus_m a_3$
a_3	$a_3 \oplus_m a_1$	$a_3 \oplus_m a_2$	$a_3 \oplus_m a_3$

Location of an element in the table

$\oplus_m$			a_3
a_2			$a_2 \oplus_m a_3$

We have a similar table for $\otimes_m$ in which unique element $a_i \otimes_m a_j$ i.e., the remainder when $a_i \times a_j$ is divided by m is written at the intersection of the row headed by a_i and the column headed by a_j.

Note: If the set S is not given for 'addition modulo m' or 'multiplication modulo m', then we use the set $S = \{0, 1, 2, 3, \dots m-1\}$ to for the composition table in modulo m.

Example 6: *Let S = {0, 1, 2, 3}. Construct the table for 'addition modulo 4' in S. Using the table, answer the following:*

(i) $1 \oplus_4 3 = \dots$

(ii) $3 \oplus_4 2 = \dots$

(iii) *Is* $(1 \oplus_4 3) + (3 \oplus_4 2) = 1 \oplus_4 0$?

(iv) $3 \oplus_4 n = 1$

Solution: Here, $S = \{0, 1, 2, 3\}$

For $a, b \in S$, $a \oplus_4 b$ = the remainder when $a + b$ is divided by 4.

Composition Table for $\oplus_4$

$\oplus_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

From the table, we have

(i) $1 \oplus_4 3 = 0$

(ii) $3 \oplus_4 2 = 1$

(iii) $(1 \oplus_4 3) - (3 \oplus_4 2) = 0 + 1 = 1$

Also $1 \oplus_4 0 = 1$

Yes, $(1 \oplus_4 3) + (3 \oplus_4 2) = 1 \oplus_4 0$.

(iv) $3 \oplus_4 n = 1$

Yes, the remainder when $(3 + n)$ divided by $4 = 1$

$\Rightarrow \quad n = 2$

Note: To find the truth set of the given equation, we put $n = 0, 1, 2, 3$ in the given equation and determine which of them satisfies it. The value(s) of n which satisfy the equation gives the truth set.

Example 7: *Let S = {1, 2, 3, 4}. Construct the table for 'multiplication modulo 5' in S.*

Using the table, find (i) $3 \otimes_5 4$ (ii) $4 \otimes_5 2 =$ (iii) $(3 \otimes_5 2) + (1 \otimes_5 4)$ (iv) $2 \otimes_5 n = 3$.

Solution: Here, $S = \{1, 2, 3, 4\}$

For $a, b \in S$, $a \otimes_5 b$ = the remainder when $a \times b$ is divided by 5.

Composition Table for $\otimes_5$

$\otimes_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

From the table,

(i) $3 \otimes_5 4 = 2$

(ii) $4 \otimes_5 2 = 3$

(iii) $(3 \otimes_5 2) + (1 \otimes_5 4) = 1 + 4 = 5$

(iv) $2 \otimes_5 n = 3 \Rightarrow n = 4$.

Example 8: *Construct the tables for 'addition modulo 6' and multiplication modulo 6. Using the tables,*

(a) *Evaluate the following*:

(i) $2 \oplus_6 3$ (ii) $3 \oplus_6 4$

(iii) $(1 \oplus_6 3) \oplus_6 5$ (iv) $3 \otimes_6 5$

(v) $3 \otimes_6 4$ (vi) $5 \otimes_6 (4 \otimes_6 2)$

(b) *Find the truth sets of the following*:

(i) $3 \oplus_6 n = 0$ (ii) $3 \otimes_6 n = 0$

(iii) $n \otimes_6 n = 1$ (iv) $3 \oplus_6 (2 \oplus_6 n) = 1$.

Solution: Here, the set S is not given. Therefore, we use the set $S = \{0, 1, 2, 3, 4, 5\}$ to form the tables in modulo 6.

For $a, b \in S$,

- addition modulo 6 = $a \oplus_6 b$ = the remainder when $a + b$ is divided by 6.
- multiplication modulo 6 = $a \otimes_6 b$ = the remainder when $a \times b$ is divided by 6.

The addition and multiplication tables for modulo 6 are given by below:

Composition table for $\oplus_6$ in S

$\oplus_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0

2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Composition table for $\otimes_6$ in S

$\otimes_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

(a) From the tables, we have

(i) $2 \oplus_6 3 = 5$

(ii) $3 \oplus_6 4 = 1$

(iii) $(1 \oplus_6 3) \oplus_6 5 = 4 \oplus_6 5 = 3$

(iv) $3 \otimes_6 5 = 3$

(v) $3 \otimes_6 4 = 0$

(vi) $5 \otimes_6 (4 \otimes_6 2) = 5 \otimes_6 2 = 4$

(b) Using the table, we have

(i) $3 \oplus_6 n = 0 \Rightarrow n = 3 \Rightarrow$ Truth set = {3}

(ii) $3 \otimes_6 n = 1 \Rightarrow n = 0, 2, \text{or } 4 \Rightarrow$ Truth set = {0, 2, 4}

(iii) $n \otimes_6 n = 1 \Rightarrow n = 1, \text{or } 5 \Rightarrow$ Truth set = {1, 5}

(iv) $3 \oplus_6 (2 \oplus_6 n) = 1 \Rightarrow n = 2 \Rightarrow$ Truth set = {2}

Note: If there are brackets, perform the expression in the brackets first.

Example 9: *Let S = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10}. (a) Construct the table for 'multiplication modulo 11' in S.*

(b) Using the table, evaluate the following:

(i) $4 \otimes_{11} 7$ (ii) $3 \otimes_{11} (5 \otimes_{11} 8)$

(iii) $(7 \otimes_{11} 9) \otimes_{11} (6 \otimes_{11} 4)$.

(c) Using the table, find the truth set of the following:

(i) $5 \otimes_{11} n = 1$ (ii) $n \otimes_{11} 9 = 2$

(iii) $n \otimes_{11} n = 3$.

Solution: (*a*) For $a, b \in S$, 'multiplication modulo 11' denoted by $a \otimes_{11} b$ is the remainder when $a \times b$ is divided by 11.

Composition Table for $\otimes_{11}$ in S.

$\otimes_{11}$	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	1	3	5	7	9
3	3	6	9	1	4	7	10	2	5	8
4	4	8	1	5	9	2	6	10	3	7
5	5	10	4	9	3	8	2	7	1	6
6	6	1	7	2	8	3	9	4	10	5
7	7	3	10	6	2	9	5	1	8	4
8	8	5	2	10	7	4	1	9	6	3
9	9	7	5	3	1	10	8	6	4	2
10	10	9	8	7	6	5	4	3	2	1

(b) Using the table, we have

(i) $4 \otimes_{11} 7 = 6$

(ii) $3 \otimes_{11} (5 \otimes_{11} 8) = 3 \otimes_{11} 7 = 10$

(iii) $(7 \otimes_{11} 9) \otimes_{11} (6 \otimes_{11} 4) = 8 \otimes_{11} 2 = 5$

(c) Using the table,

(i) $5 \otimes_{11} n = 1 \Rightarrow n = 9 \Rightarrow$ Truth set = {9}

(ii) $n \otimes_{11} 9 = 2 \Rightarrow n = 10 \Rightarrow$ Truth set = {10}

(iii) $n \otimes_{11} n = 3 \Rightarrow n = 5$ or $6 \Rightarrow$ Truth set = {5, 6}

EXERCISE 1.3

1. Find the values of the following:

(i) $2 \oplus_3 1$ (ii) $3 \oplus_4 3$

(iii) $5 \oplus_7 4$ (iv) $3 \otimes_5 4$

(v) $4 \otimes_7 6$ (vi) $7 \otimes_{11} 9$

2. Let $S = \{0, 1, 2\}$. Construct the tables for 'addition modulo 3' and 'multiplication modulo 3'.

3. Let $S = \{0, 1, 2, 3, 4\}$. Construct the tables for 'addition modulo 5' and 'multiplication modulo 5'. From the table, answer the following:

(i) $2 \oplus_5 3$ (ii) $4 \oplus_5 3$

(iii) $3 \oplus_5 1$ (iv) $3 \otimes_5 4$

(v) $4 \otimes_5 4$ (vi) $(2 \otimes_5 3) \otimes_5 4$

4. Let $S = \{1, 2, 3, 4, 5, 6\}$. Construct the table for 'multiplication modulo 7'. From the table, answer the following:

(i) $6 \otimes_7 3$ (ii) $3 \otimes_7 4$

(iii) $5 \otimes_7 6$ (iv) $(2 \otimes_7 5) \otimes_7 6$

(v) $(4 \otimes_7 5) \otimes_7 2$ (vi) $(2 \otimes_7 5) \otimes_7 (4 \otimes_7 3)$.

5. (a) Construct the table for 'multiplication modulo 12' on the set $S = \{1, 4, 9, 11\}$.

(b) Using the table, answer the following:

(i) $4 \otimes_{12} 9$ (ii) $11 \otimes_{12} 4$

(c) Using table, find the truth set of

(i) $9 \otimes_6 n = 0$ (ii) $n \otimes_6 n = 1$

6. (a) Construct the tables for 'addition modulo 6' and 'multiplication modulo 6'.

(b) Using the tables, evaluate the following:

(i) $4 \oplus_6 3$ (ii) $(2 \oplus_6 3) \oplus_6 4$

(iii) $3 \otimes_6 4$ (iv) $(3 \otimes_6 4) \otimes_6 5$

(c) Using the tables, find the truth set of the following:

(i) $5 \otimes_6 n = 1$ (ii) $2 \oplus_6 n = 0$

(iii) $n \oplus_6 4 = 1$ (iv) $n \otimes_6 n = 1$

7. (a) Construct the table for 'multiplication modulo 13' on the set $S = \{1, 5, 8, 12\}$.

(b) Using the table, find the truth set of the following:

(i) $5 \otimes_{13} n = 1$ (ii) $12 \otimes_{13} n = 5$

(iii) $n \otimes_{13} n = 12$

MULTIPLE CHOICE QUESTIONS

1. Given figure of a clock shows that it is 4 o'clock. After 78 hours, it will show

(a) 7 o'clock (b) 8 o'clock
(c) 9 o' clock (d) 10 o'clock

2. The value of 57 (mod 7) is
(a) 0 (b) 1
(c) 2 (d) 3

3. The value of (23 × 4) (mod 5) is
(a) 2 (b) 3
(c) 4 (d) None of these

4. The value of 'a' in the modulo $25 \equiv a \pmod{4}$ is
(a) 0 (b) 1
(c) 5 (d) 3

5. If n is a natural number such that 15 (mod n) = 3, the value of n is
(a) 4 (b) 3
(c) 2 (d) None of these

6. If n is a natural number such that 56 (mod n) = 2, the value of n is
(a) 8 (b) 7
(c) 6 (d) 5

7. If 26 = 2 mod x, the value of x is
(a) 5 (b) 7
(c) 8 (d) 9

8. If $2x$ = 1 mod 3, the value of least positive integer that satisfies this equation is
(a) 2 (b) 3
(c) 4 (d) 5

9. $7 \oplus_5 10$ is equal to
(a) 0 (b) 1
(c) 2 (d) 3

10. $25 \otimes_6 10$ is equal to
(a) 2 (b) 3
(c) 4 (d) 5

11. If today is Friday, the day that will come after 100 days is

(a) Monday (b) Friday

(c) Saturday (d) Sunday

12. If today is Sunday, the day that will come after 1000 days is

(a) Monday (b) Friday

(c) Saturday (d) Sunday

13. Four security persons Hassan, William, Michael and Albert take turns to secure a bank in Monrovia. Hassan is on duty on Tuesday of the first week. After how many weeks, he will be on his duty on Tuesday?

(a) 4 weeks (b) 6 weeks

(c) 7 weeks (d) 8 weeks

14. There are four persons on duty roster. Sunday is the most popular day to be on duty. Felix, one of them, delivered his first duty on Friday. After how many weeks, he will be on Sunday again for his duty?

(a) 4 weeks (b) 6 weeks

(c) 7 weeks (d) 8 weeks

15. Daniel travels from Monrovia to Kakata once every seven months. His first visit was in August 2017. The month in which he will have his ninth visit is

(a) September 2022 (b) January 2022

(c) November 2022 (d) March 2022