CHAPTER 2

At the end of the chapter, students should be able to:
1. Perform basic operations of addition, subtraction, multiplication and division involving modular arithmetic.
2. Apply modular arithmetic in daily life.
3. Solve linear equations involving modular arithmetic.

I. Revision of Addition, Subtraction, Multiplication and Division of Integers

To each number $n \in Z$, we associate two directed numbers known as 'positive n' $(+n)$ and 'negative n' $(-n)$. The number zero with the property that for all 'n', the sum of n and $-n$ is 0, is also defined. We simply refer to $+n$ as n and $-n$ as $-n$. The numbers ..., $-n$, ..., –3, –2, –1, 0, 1,2, 3, ..., n, ... are called the integers (set of positive numbers, zero and negative numbers).
Rules for adding and multiplying integers are as follows. Integer is denoted by Z.
For example $(+7) + (+5) = +12$ and $(+7)(+5) = +35$.
We have the following definitions:

(i) $(+a) + (+b) = +(a + b)$
(ii) $(+a)(+b) = +(ab)$
(iii) $(+a)(-b) = -(ab)$
(iv) $(-a)(-b) = +(ab)$
(v) $(-a) + (-b) = -(a + b)$

It follows that if a and b are integers, then $a + b$ and ab are also integers. An even integer is an integer of the form $2m$ for some integers m, and an odd integer is an integer of the form $2m + 1$ for some integers m.
Examples: –6, –4, –2, 0, 2, 4, 6, 8, ... (even integers). ..., –5, –3, –1, 1, 3, 5, ... (odd integers).

Even integers are integers divisible by 2 and odd integers are those

that are not divisible by two. Integers can be either odd or even, but not both. If p is an integer then $p \cdot p = p_2$. If p_2 is even, then p is even.

Numbers to the left of zero are negative and always less than zero, while
numbers to the right of zero are positive and always greater than zero. The negative or opposite of a positive number +2 is called negative 2 or minus 2, and
is written as –2. We call 2 the absolute value of the number +2 and –2. Integers can be represented on a number line (see Fig. 2.1).

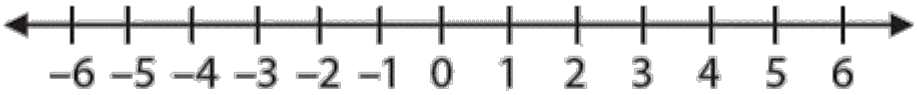


Fig. 2.1

(i) Revision of addition of integers

When two integers are added, we take one integer as the reference point and move to the right, if the other integer is positive or to the left, if the other integer is negative.
Positive integers are counted by moving to the right-hand side or upwards, while we count negative integers by moving to the left-hand side or downwards, depending on whether we use the horizontal or vertical number line. Arrow signs are used to show the direction of movements because positive and negative integers are in opposite directions. They are called directed numbers.

Worked Example 1

Add 3 and 4.

Solution

When neither – nor + is affixed to a number, it is positive.
Note: (+3) + (+4) = +7 = 7.

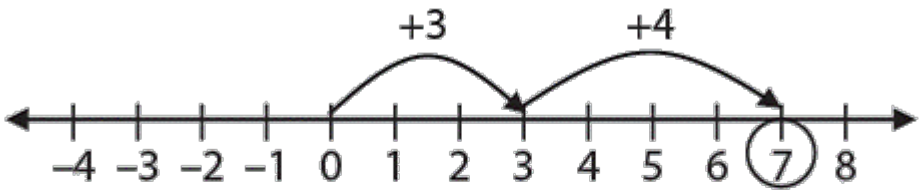


Fig. 2.2

$$\therefore 3 + 4 = 7$$

Worked Example 2

What is the sum of –6 and +2?

Solution

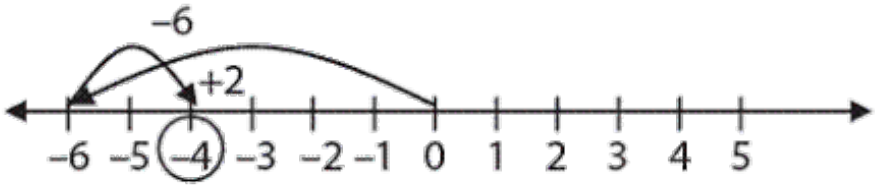


Fig. 2.3

$\therefore (-6) + (+2) = -4$

Worked Example 3

What is the sum of –5 and –3?

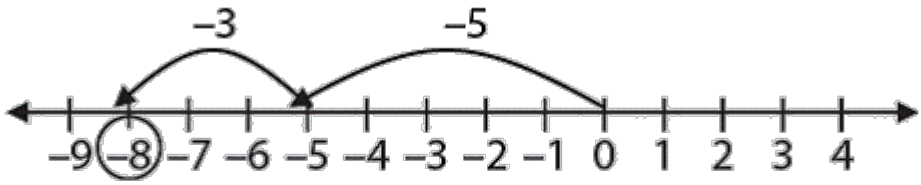


Fig. 2.4

$\therefore (-5) + (-3) = -8$

Note:

1. The addition of two positive whole numbers is always a positive whole number.
2. If a positive whole number is greater than the absolute value of a negative whole number, then their addition is a positive whole number.
3. If a positive whole number is less than the absolute value of a negative number then their addition is a negative whole number.
4. The addition of two negative whole numbers is always a negative whole number. The absolute values of the two numbers are considered.

(ii) Revision of subtraction of integers

When two integers are subtracted from each other on the number line, one of them is taken as the reference point and the other is counted to the left, if it is positive and to the right if it is negative. Subtraction is, therefore, opposite of addition.

Worked Example 4

Subtract −4 from 6.

Solution

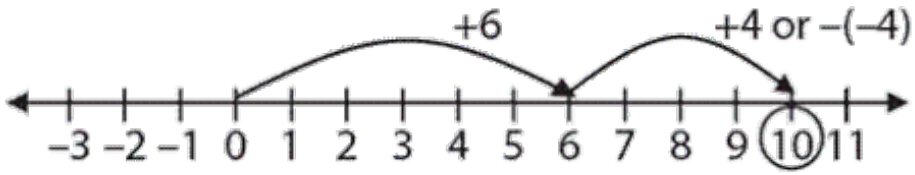


Fig. 2.5

$$\therefore 6-(-4) = 6+4 = 10$$

Worked Example 5

Find −6 − (−2).

Solution

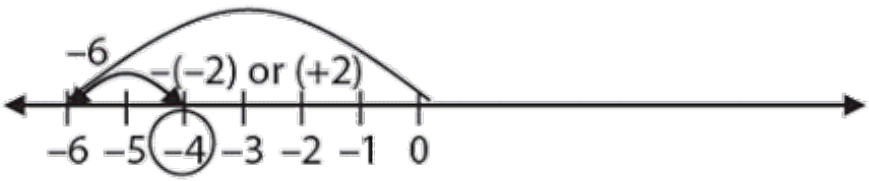


Fig. 2.6

$$\therefore -6-(-2) = -6+2 = -4$$

Note: If we subtract or take away a positive integer from a negative integer, the result is always a negative integer having an absolute value equal to the sum of the absolute values of the given integers.

(iii) Revision of multiplication of integers

Multiplication of integers is obtained through repeated addition. Note the following:

(1) (+) × (+) = +
(2) (+) × (–) = –
(3) (–) × (+) = –
(4) (–) × (–) = +

Worked Example 6

What is the product of −4 and 6?

Solution

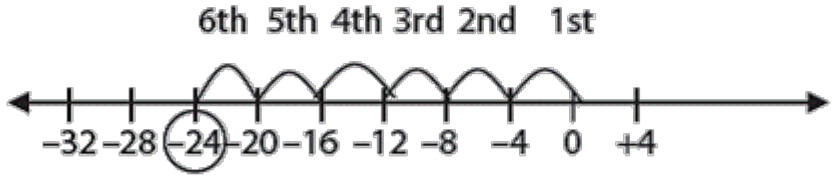


Fig. 2.7

$$\therefore -4 \times 6 = -24$$

Worked Example 7

Multiply the following:

(i) 3 by 4

(ii) –6 by –2

Solution

$$\text{(i)}\quad 3 \times 4 = (3) + (3) + (3) + (3)$$
$$= 3(4) = 12$$

$$\text{(ii)}\quad -6 \times -2 = -2 \times -6$$
$$= -[(-2) + (-2) + (-2) + (-2) + (-2) + (-2)]$$
$$= -(-2)6$$
$$= (2)6 = 12$$

(iv) Revision of division of integers

Division of integers is a successive subtraction of a number from a given number until zero is left. After the successive subtraction, the number of times you subtract the number gives the result. Note the following when dividing integers:

1. (+) ÷ (+) = +
2. (–) ÷ (+) = –
3. (+) ÷ (–) = –

4. (–) ÷ (–) = +

Worked Example 8

Divide 10 by 2.

Solution

$10-2=8, 8-2=6, 6-2=4, 4-2=2, 2-2=0$

2 is subtracted five times

$\therefore 10 \div 2 = 5$

Worked Example 9

Divide (–35) by (–7).

Solution

$-35-(-7)=-28, -28-(-7)=-21, -21-(-7)=-14, -14-(-7)=-7, -7-(-7)=0$

−7 is subtracted five times

$\therefore -35 \div -7 = 5$

Exercise 1

1. What is the sum of 2 and (−6)?
2. Find −8 − (−12).
3. What is −4 − (−9)?
4. What is +8 − (+6)?
5. Subtract −9 from 4.
6. Find −9 − (+4).
7. What is −5 − (−11)?
8. Find 4 − (+4).
9. What is the sum of −6 and −14?
10. Find the sum of 9 and −2.
11. Simplify the following:
    (a) 6 + (−6) + 2
    (b) −4 + 3 + (+3)
    (c) −4 + (−3) + 7
12. Evaluate the following:
    (a) −5 − (−4) − (3) − (−2)
    (b) 4 − 3 − 2 − (−5)

(c) $-2-(-9)-(+9)$

(d) $5-(-8)-(-3)$

13. Simplify:

(a) $-6+(-2)-(-4)$

(b) $8+(-8)-(-8)$

(c) $-7-(-7)$

(d) $0-(-4)$

(e) $89-56+4$

14. Evaluate the following:

(a) $-4-(-7)$

(b) $-11-(+2)$

(c) $+1-(+18)$

(d) $+8-(-6)$

(e) $-3-(-15)$

15. Find the values of the following products:

(a) $5 \times (-8)$

(b) $14 \times (-16)$

(c) 4×9

(d) $-6 \times (-19)$

(e) -4×18

16. Simplify the following:

(a) $36 \div (-9)$

(b) $-45 \div (+15)$

17. A negative number divided by a positive number gives a _____ number.

18. When the signs of the two numbers are different, the answer/result of the division is a _____ number.

Divide:

19. -48 by -6

20. 18 by -2

21. 56 by 4

Evaluate the following:

22. $-144 \div (-36)$

23. $24 \div (-3)$

24. $-183 \div (-61)$

Simplify the following:

25. $\dfrac{(-16) \times (-3) \times (+2)}{2 \times (-4) \times 5}$

26. $\dfrac{-3}{4} \times \dfrac{7}{12} \times \dfrac{6}{7}$

27. $\dfrac{2 \times 3 \times (-5) \times (+4)}{2 \times (-4) \times 5}$

28. $\dfrac{-25}{(-4) \times (-3)}$

Evaluate the following:

29. $(+8) \times (-2) \times (+2)$

30. $(-3) \times (-4) \times (-2)$

II. Concept of Modular Arithmetic

Any arithmetic operation in which the multiples involved are ignored and attention is given mostly to remainders is called modular arithmetic. We then call such arithmetic process under such modulus as modulus of that multiple. Modulus or simply module is represented as '$Z_{\text{mod } n}$', meaning integer modulo n where n = 2, 3, 4, 5, 6, …. Recall, that under number base system, we have

discussed number of digits in a particular number base, for example, base 8 (octal system) has eight digits with the exclusion of eight itself. They are 0, 1, 2, 3, 4, 5, 6 and 7. In the language of modulus, any number greater than 8 can be converted such that its remainder will be our concern.

Examples:

$$\frac{8}{8} = 1R0; \frac{9}{8} = 1R1;$$

$$\frac{10}{8} = 1R2; \frac{11}{8} = 1R3;$$

$$\frac{12}{8} = 1R4; \frac{13}{8} = 1R5;$$

$$\frac{14}{8} = 1R6; \frac{15}{8} = 1R7;$$

$$\frac{16}{8} = 2R0; \frac{17}{8} = 2R1.$$

The results in the above are in base 8. The concept of modular arithmetic is better understood by another concept called *congruency*. In giving the time of day, it is customary to count only up to 12 and then begin over again. Likewise, in a woman's menstrual cycle, after counting to 28 or 30 depending on individual cycles, the cycle begins again. This simple idea of throwing away the multiples of a fixed number 12 is the basis of the arithmetic notion of congruency. We call two integers congruent 'modulus 12' if they differ only by an integral multiple of 12. For example, 2 and 14 are congruent and we write $2 \equiv 14 \pmod{12}$ where mod 12 means with modulus 12 or modulo 12 and ≡ means congruent or equivalent.

Note:

1. $a \equiv b \pmod{m}$, if and only if $m/(a - b)$ means m divides $a - b$.
2. Two integers a and b are congruent modulo m, if and only if they have the same remainder when divided by m.

For example, $17 \div 8 = 2$ remainder 1 and $25 \div 8 = 3$ remainder 1. Hence, $17 \equiv 25 \pmod{8}$ that is; $17 \equiv 25 \equiv 1 \pmod{8}$.

Worked Example 10

Reduce 89 to its simplest form in

(a) modulo 3
(b) modulo 4
(c) modulo 5

Solution

(a) $89 \div 3 = 29$ remainder 2

Notes

$\therefore 89 \equiv 2 \pmod 3 \Rightarrow 3/(89-2) = 3/87$

$= 29$

(b) $89 \div 4 = 22$ remainder 1

$\therefore 89 \equiv 1 \pmod 4 \Rightarrow 4/(89-1) = 4/88$

$= 22$

(c) $89 \div 5 = 17$ remainder 4

$\therefore 89 \equiv 4 \pmod 5 \Rightarrow 6/(89-5) = 6/84$

$= 14$

Exercise 2

Reduce 25 to its simplest form in

1. modulo 3
2. modulo 4
3. modulo 5
4. modulo 6
5. modulo 7

Reduce 153 to its simplest form in

6. modulo 10
7. module 11
8. modulo 4

Perform the following addition under (i) modulo 4 (ii) modulo 5 (iii) modulo 6

9. $14 + 7$
10. $6 + 1$
11. $8 + 17$
12. $13 + 4$
13. $17 + 3$
14. $21 + 5$

Find the quotients of the following:

15. $55 \equiv 1 \pmod 3$
16. $153 \equiv -7 \pmod{10}$
17. $178 \equiv 50 \pmod 4$

Convert the following to congruent and modular arithmetic statements.

18. $7/24 - 3$
19. $26/53 - 1$
20. $5/19 - 4$

III. Addition and Subtraction of Modular Arithmetic

As addition and subtraction is possible in number bases, it is also possible in modular arithmetic.

For example:

Modulo 4 = {0, 1, 2, 3}

Modulo 5 = {0, 1, 2, 3, 4}
Modulo 6 = {0, 1, 2, 3, 4, 5} etc.
The easiest way of doing subtraction in arithmetic modular basis is through rotational basis in an anticlockwise manner while that of addition in arithmetic modular basis is through rotation in a clockwise manner. For example, 4 • 3 = 7 = 1 (mod 6) and 3 • 3 = 6 = 0 (mod 6). The addition is done in modulo 6. You will discover that multiples of 6 are ignored and remainders are written down. Table 2.1 shows an addition table (mod 6) in which digits 0, 1, 2, 3, 4 and 5 are added to themselves.

Table 2.1: Addition table (mod 6)

Second number

First numbers ⊕	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

From the table, we can see that $4 \oplus 3 = 1$ and $3 \oplus 3 = 0$.

Worked Example 11

Find the values of the following in the moduli stated beside them.

(a) $41 \oplus 3 \pmod 4$

(b) $10 \oplus 21 \pmod 7$

Solution

(a) $41 + 3 = 44$

$= (4 \times 10 + 4)$

$\equiv 4 \pmod 4$

(b) $10 + 21 = 31$

$= (7 \times 4 + 3)$

$\equiv 3 \pmod 7$

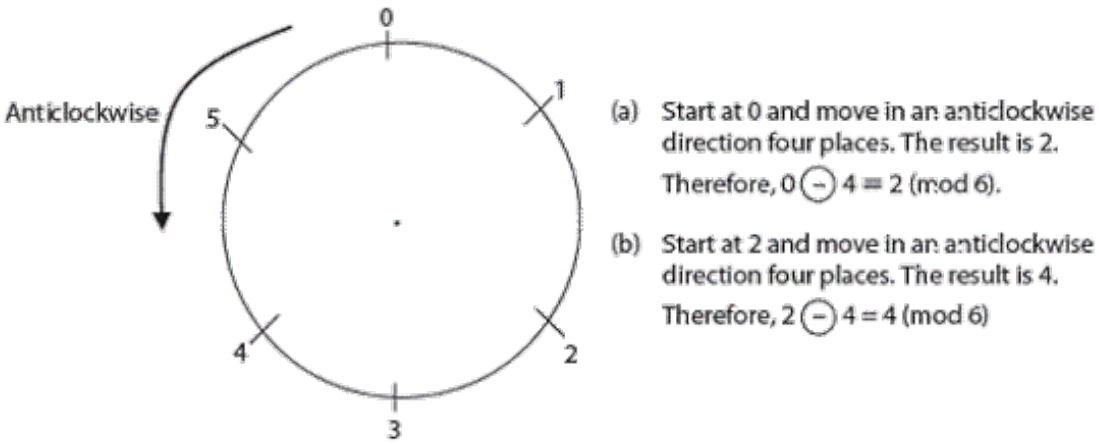
Worked Example 12

Find:

(a) $0 \ominus 4 \pmod 6$

(b) $2 \ominus 4 \pmod 6$

Solution



(a) Start at 0 and move in an anticlockwise direction four places. The result is 2.
Therefore, $0 \ominus 4 \equiv 2 \pmod 6$.

(b) Start at 2 and move in an anticlockwise direction four places. The result is 4.
Therefore, $2 \ominus 4 \equiv 4 \pmod 6$

Fig. 2.8

Worked Example 13

Find the simplest positive form of each of the following:

(a) –16 (mod 3)

(b) –2 (mod 11)

Solution

(a) $-16 = (3 \times -6 + 2)$
$= 2 \pmod 3$

(b) $-2 = (11 \times -1 + 9)$
$= 9 \pmod{11}$

Worked Example 14

Add $41 \oplus 30 \pmod 4$.

Solution

$41 + 30 = 71$
$= (4 \times 17 + 3)$
$= 3 \pmod 4$

or $41 + 30 = (4 \times 10 + 1) + (4 \times 7 + 2)$
$= (1 + 2) \pmod 4$
$= 3 \pmod 4$

Worked Example 15

Calculate the following in the given moduli.

(a) $13 \ominus 7 \pmod 3$

(b) $22 \ominus 26 \pmod 7$

Solution

(a) $13 \ominus 7 = 6 = 3 + 3 = 3 \pmod 3$

(b) $22 \ominus 26 = -4 = -7 + 3 = 3 \pmod 7$

Note:

1. $3 \ominus 1 \neq 1 \ominus 3$ (subtraction is not commutative)
2. $4 \oplus 2 = 2 \oplus 4$ (addition is commutative)
3. Any negative number has an equivalent positive value in modular (see Example 15).
4. Moduli is the plural of modulus.
5. Addition or subtraction is done by writing/listing all the digits in modulus first before counting clockwise or anticlockwise to a given number as specified in the question or instruction, for example, $4 \oplus 7$ under Z_8.

0, 1, 2, 3, 4, 5, 6 and 7

4th 5th 6th 7th 1st 2nd 3rd

Counting clockwise from 5 to and fro 7 times gives 3. Therefore, $4 \oplus 7 = 11 \equiv 3 \pmod 8$. Also, $1 \ominus 2$ under Z_4.

0, 1, 2, and 3

1st 2nd

Counting anticlockwise from 0 to and fro 2 times gives 3. Therefore, $1 \ominus 2 = -1 \equiv 3 \pmod 4$.

Exercise 3

1. Find the following numbers in their simplest form in modulo 5:
   (a) 16 (b) 33 (c) 63
   (d) 48 (e) 83 (f) 18
   (g) 79 (h) 39 (i) 57
   (j) 103 (k) 98 (l) 102

2. Find the following addition in modulo 7:
   (a) $4 \oplus 9$ (b) $9 \oplus 10$
   (c) $5 \oplus 9$ (d) $8 \oplus 18$
   (e) $13 \oplus 8$ (f) $6 \oplus 7$

3. Calculate in the given moduli.
   (a) $4 \oplus 7 \pmod 2$
   (b) $54 \oplus 25 \pmod 5$
   (c) $7 \oplus 5 \pmod 3$
   (d) $82 \oplus 35 \pmod 3$
   (e) $41 \oplus 29 \pmod 8$
   (f) $39 \oplus 22 \pmod{11}$

4. Copy and complete Table 2.2 for addition (mod 7).

Table 2.2

Second number

First number ⊕	0	1	2	3	4	5	6
0							
1							
2							
3							
4							
5							
6							

5. Find the simplest form of the following in the given moduli:
   (a) −6 (mod 4)
   (b) −103 (mod 7)
   (c) −31 (mod 7)
   (d) −9 (mod 7)
   (e) −53 (mod 3)
   (f) −17 (mod 10)

6. Find the simplest positive form of each of the following numbers in modulo 7:
   (a) −156 (b) − 36
   (c) −75 (d) −56
   (e) −72 (f) −103

7. Copy and complete Table 2.3 for subtraction in modulo 5.

Table 2.3

Second number

$\ominus$	0	1	2	3	4
0					
1					
2					
3					
4					

First number

8. Find the values of the following in the moduli stated beside them:
   (a) $7 \oplus 14 \pmod 4$
   (b) $18 \oplus 7 \pmod 7$
9. Find (a) $0 \ominus 2 \pmod 3$
   (b) $1 \ominus 2 \pmod 3$

10. Find (a) $1 \ominus 6 \pmod 7$
(b) $2 \ominus 5 \pmod 7$.

11. Calculate $13 \ominus 6 \pmod 5$.

12. Calculate $47 \ominus 40 \pmod 3$.

13. Calculate $74 \ominus 79 \pmod 7$.

Express each of the following as a single digit from the set {0, 1, 2, 3, 4}:

14. $-22 \pmod 5$

15. $78 \ominus 19 \pmod 4$

IV. Multiplication and Division of Modular Arithmetic

In solving multiplication and division operations involving modular arithmetic, we note the following: $5 \otimes 3 = 3 \otimes 5$ (multiplication is commutative).

$\frac{2}{5} \neq \frac{5}{2}$ (division is not commutative).

A congruence of degree 1 is called a linear congruence. It is of the form $ax \equiv b \pmod{m}$ with $a \not\equiv 0 \pmod{m}$. A way of solving linear congruence is to use the linear property for the highest common factor (H.C.F). We shall employ the use of the above fact to solve problems involving linear congruence by simply writing their linear combination and finding their H.C.F.

Division in modular arithmetic is sometimes possible and sometimes impossible, thus, we may divide the congruence $4 \equiv 18 \pmod{7}$ by 2 and obtain the $2 \equiv 9 \pmod{7}$ that is, $\frac{7}{2-9} = \frac{7}{-7}$. While $6 \equiv 15 \pmod{9}$ divided by 3 will give invalid congruencies, that is, $2 \equiv 5 \pmod{9}$ which implies 9/2 – 5 = 9/ – 3. Hence, division is not always possible.

Worked Example 16

Evaluate the following, modulo 5:

(a) $4 \otimes 6$
(b) $5 \otimes 5$
(c) $41 \otimes 9$
(d) $25 \otimes 7$

Solution

(a) $4 \otimes 6 = 24 = (5 \times 4 + 4) = 4 \pmod 5$
(b) $5 \otimes 5 = 25 = (5 \times 5 + 0) = 0 \pmod 5$
(c) $41 \otimes 9 = 369 = (5 \times 73 + 4) = 4 \pmod 5$
(d) $25 \otimes 7 = 175 = (5 \times 35 + 0) = 0 \pmod 5$

or

$$\begin{aligned} 25 \otimes 7 &= (5 \times 5 + 0) \times (5 \times 1 + 2) \\ &= 0 \pmod 5 \times 2 \pmod 5 \\ &= 0 \times 2 \pmod 5 \\ &= 0 \pmod 5 \end{aligned}$$

Worked Example 17

Evaluate the following in modulo 5:

(a) $18 \otimes 25$
(b) $93 \otimes 64$
(c) $14 \otimes 57$

Solution

(a) $$\begin{aligned} 18 \otimes 25 &\equiv 5 \times 3 + 3 \pmod 5 \times 5 \times 5 \\ &\quad + 0 \pmod 5 \\ &\equiv 3 \pmod 5 \times 0 \pmod 5 \end{aligned}$$

$\equiv 3 \times 0 \pmod 5$

$\equiv 0 \pmod 5$

(b) $93 \otimes 64 \equiv 5 \times 18 + 3 \pmod 5 \times 5 \times 12 + 4 \pmod 5$

$\equiv 3 \pmod 5 \times 4 \pmod 5$

$\equiv 3 \times 4 \pmod 5$

$\equiv 12 \pmod 5$

$\equiv 12 - 5(2) \pmod 5$

$\equiv 12 - 10 \pmod 5$

$\equiv 2 \pmod 5$

(c) $14 \otimes 57 \equiv 5 \times 2 + 4 \pmod 5 \times 5 \times 11 + 2 \pmod 5$

$\equiv 4 \pmod 5 \times 2 \pmod 5$

$\equiv 4 \times 2 \pmod 5$

$\equiv 8 \pmod 5$

$\equiv 8 - 5 \pmod 5$

$\equiv 3 \pmod 5$

Worked Example 18

Evaluate the following in the moduli written beside them:

(a) $14 \otimes 9 \pmod 6$

(b) $19 \otimes 18 \pmod 3$

Solution

(a) $14 \otimes 9 = 126$

$= 6 \times 21 + 0$

$\equiv 0 \pmod 6$

or by expressing 14 and 9 in linear combination.

$14 = 12 + 2 \equiv 2 \pmod 6$

$9 = 6 + 3 \equiv 3 \pmod 6$

$14 \times 9 \equiv 2 \times 3 \pmod 6$

$\equiv 6 \pmod 6$

$\equiv 6 - 6 \pmod 6$

$14 \otimes 9 \equiv 0 \pmod 6$

(b) $19 \otimes 18 \pmod 3$

$19 = 15 + 4 \equiv 4 \pmod 3$

$= 4 - 3 \pmod 3$

$= 1 \pmod 3$

$18 = 18 + 0 \equiv 0 \pmod 3$

$\equiv 0 \times 1 \pmod 3$

$19 \otimes 18 \equiv 0 \pmod 3$

Worked Example 19

Where possible, find the values of the following in modulo 4:

(a) $2 \div 3$

(b) $2 \div 2$

(c) $3 \div 2$

Solution

(a) If $2 \div 3 = x$, then $3x \equiv 2 \pmod 4$.
Solve by using inspection method.

Table 2.4: Z_4

x	0	1	2	3
3	0	3	2	1

Locate the remainder which is 2, hence, the solution of the linear congruence $3x \equiv 2 \pmod 4$ is $x \equiv 2 \pmod 4$.

$\therefore x \equiv 2 \pmod 4$

(b) If $2 \div 2 = x$, then $2x \equiv 2 \pmod 4$

Table 2.5

x	0	1	2	3
2	0	2	0	2

Locate the remainder which is 2, hence, the solution of the linear congruence $2x \equiv 2 \pmod 4$ has integral solutions. It has two values. They are $x \equiv 1 \pmod 4$ and $x \equiv 3 \pmod 4$.
Therefore, $2 \div 2 \pmod 4$ has two values: 1 and 3.

(c) If $3 \div 2 = x$, then $2x \equiv 3 \pmod 4$.

Table 2.6

x	0	1	2	3
2	0	2	0	2

Locate the remainder which is 3, hence $2x \equiv 3 \pmod 4$ has no solution since no multiple of 4 can be added to 3 to make it exactly divisible by 2.

Worked Example 20

Find the solutions or truth sets of the following linear congruences:
(a) $6x \equiv 2 \pmod 4$
(b) $x + 1 \equiv 3 \pmod 7$

Solution

(a) Z_4 of $6x \equiv 2 \pmod 4$

Table 2.7

x	0	1	2	3
6	0	2	0	2

Locate the remainder in the given linear congruence that is 2, hence, the solutions of the linear congruence are 1 and 3. That is, it has two values.
$\therefore x \equiv 1 \pmod 4$
and $x \equiv 3 \pmod 4$

(b) Z_7 of $x + 1 \equiv 3 \pmod 7$

Table 2.8

$x+1$	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0

The solution of the linear congruence is
$x \equiv 2 \pmod 7$

or $x + 1 \equiv 3 \pmod 7$
$x + 1 = 3 + 7$
$x + 1 = 10$
$x + 1 - 1 = 10 - 1$
$x \equiv 9 \pmod 7$
$x \equiv 9 - 7 \pmod 7$
$x \equiv 2 \pmod 7$

Remark:
1. Division in modular arithmetic may give more than one value or even no value at all.

2. Given numbers can first be converted to their simplest form before calculation.
3. Trial and inspection methods are used in division to obtain solution(s) as shown in Worked Examples 19 and 20.

Exercise 4

1. Find the values of the following in modulo 5:
   (a) $6 \otimes 7$ (b) $5 \otimes 17$
   (c) $17 \otimes 9$ (d) $21 \otimes 19$
   (e) $3 \otimes 73$ (f) $21 \otimes 64$
2. Find the values of the moduli written beside the following.
   (a) $15 \otimes 9 \pmod 4$
   (b) $41 \otimes 16 \pmod 7$

(c) $31 \otimes 19 \pmod 9$

(d) $7 \otimes 25 \pmod 5$

(e) $80 \otimes 29 \pmod 7$

(f) $6 \otimes 73 \pmod 3$

3. Complete the multiplication in modulo 6 in Table 2.9.

Table 2.9

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

4. Find the values of the moduli written beside the following.

(a) $8 \div 4 \pmod 3$

(b) $18 \div 9 \pmod 2$

(c) $16 \div 4 \pmod 5$

(d) $15 \div 5 \pmod 4$

(e) $60 \div 5 \pmod 7$

(f) $90 \div 10 \pmod 6$

(g) $28 \div 4 \pmod{11}$

(h) $44 \div 11 \pmod 2$

(i) $3 \div 5 \pmod 2$

(j) $30 \div 5 \pmod 7$

(k) $24 \div 6 \pmod 3$

(l) $36 \div 4 \pmod 7$

5. Calculate the following in modulo 7:

(a) $18 \div 6$ (b) $30 \div 5$

(c) $27 \div 3$ (d) $20 \div 5$

(e) $90 \div 10$ (f) $14 \div 7$

(g) $77 \div 11$ (h) $70 \div 7$

6. Use the multiplication table completed in question modulo 6 divisions.

(a) $3 \div 5$ (b) $1 \div 4$

(c) $2 \div 5$ (d) $3 \div 4$

(e) $0 \div 5$ (f) $2 \div 4$

(g) $1 \div 5$ (h) $2 \div 3$

7. Solve the following linear congruences in modulo 4:

(a) $3x \equiv 1$ (b) $3x \equiv 3$

(c) $5x \equiv 3$ (d) $2x \equiv 3$

(e) $4x \equiv 1$ (f) $2x \equiv 2$

8. Solve the linear congruences in the given moduli.

(a) $6 + x \equiv 0 \pmod 7$

(b) $x + 4 \equiv 0 \pmod 5$

(c) $3 - y \equiv 0 \pmod 3$

(d) $n - 5 \equiv 0 \pmod 6$

(e) $a + 3 \equiv 0 \pmod 9$

(f) $r + 7 \equiv 0 \pmod{11}$

9. Solve the following linear congruences:

(a) $9x \equiv 11 \pmod{26}$

(b) $3x + 1 \equiv 4 \pmod 5$

(c) $7x \equiv 4 \pmod{10}$

(d) $6x \equiv 4 \pmod{11}$

(e) $3x \equiv 2 \pmod{11}$

(f) $6x \equiv 3 \pmod 9$

Solve the following linear congruences:

10. $32x \equiv 1 \pmod{17}$

11. $3x \equiv 23 \pmod{26}$

12. $5x \equiv 6 \pmod{7}$

13. Express each of the following as a single digit from the set $\{0, 1, 2, 3, 4\}$:

    (a) $17 \otimes 6 \pmod{5}$

    (b) $18 \div 3 \pmod{3}$

14. Find the solutions or truth sets of the following:

    (a) $3x \equiv 1 \pmod{4}$

    (b) $8x \equiv 2 \pmod{3}$

    (c) $8 + n = 4 \pmod{9}$

15. Evaluate the following in modulo 5:

    (a) $15 \otimes 26$ (b) $7 \otimes 13$

    (c) $14 \div 7$

V. Application of Modular Arithmetic to Daily Life

Modular arithmetic is widely used in determining the following: (1) market day, (2) menstrual period or cycle in women, (3) 12-hour clock, (4) compass in an aeroplane, etc. For example, markets are held on rotational basis in Nigeria. Some markets are held every 3rd day, others are held every 7th day and so on. Wind vane of a particular region/location rotates every 5th second. Table 2.10 shows some days of the week in a month when the wind vane was rotates.

Table 2.10 shows that the wind vane rotates in a cycle as also shown in Fig. 2.9.

Note that this is not the four cardinal points. It is just a hypothetical position of the wind vanes location.

Table 2.10

Week/day	Sun	Mon	Tues	Wed	Thu	Fri	Sat
1st week							
2nd week							
3rd week	S	W	N	E	S	W	N
4th week	E	S	W	N	E	S	W

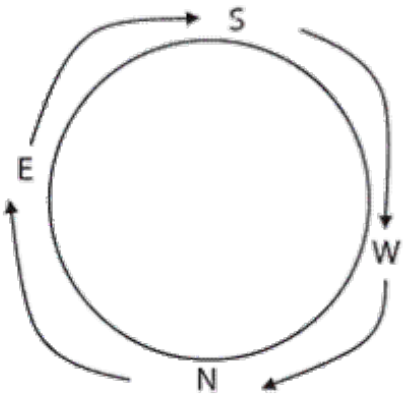


Fig. 2.9

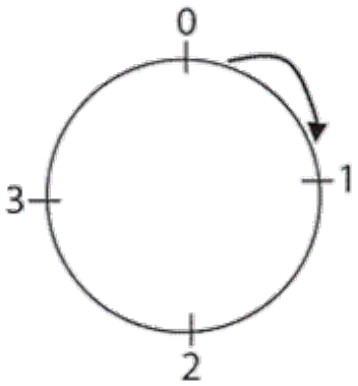


Fig. 2.10

The numbers 0, 1, 2, 3 may be used as codes for the wind vanes S, W, N and E as in Table 2.11.

The wind vanes number codes are shown as a number cycle in Fig. 2.10.

Table 2.11

Wind vane	Number code
S	0
W	1
N	2
E	3

Worked Example 21

By completing Table 2.10, find which wind vane is held on:
(a) Sunday of the 1st week.
(b) Sunday of the 2nd week.

Solution

Table 2.12 shows the complete Table 2.10.

Table 2.12

Week/day	Sun	Mon	Tue	Wed	Thu	Fri	Sat
1st week	N	E	S	W	N	E	S
2nd week	W	N	E	S	W	N	E
3rd week	S	W	N	E	S	W	N
4th week	E	S	W	N	E	S	W

(a) Wind vane N is held on Sunday of the 1st week.
(b) Wind vane W is held on Sunday of the 2nd week.

Worked Example 22

By using Table 2.12, find the days in which
(a) Wind vane E is held in the 3rd week.
(b) Wind vane N is held in the 2nd week.

Solution

(a) E occurs on Wednesday only in the 3rd week in Table 2.20. Therefore, wind vane E is held on Wednesday of the 3rd week.
(b) N occurs on Monday and Friday in the 2nd week. Therefore, wind vane N is held on Monday and Friday of the 2nd week.

Exercise 5

Using the number cycle in Fig. 2.10, find:

1. Which wind vane was held 5 days after wind vane S?
2. Which wind vane was held 12 days after wind vane N?

Find the number which results from the following addition on the number cycle in Fig. 2.10.

3. $0 \oplus 11$
4. $1 \oplus 19$

5. $2 \oplus 21$

6. $3 \oplus 24$

Use the number cycle in Fig. 2.11 to simplify the following:

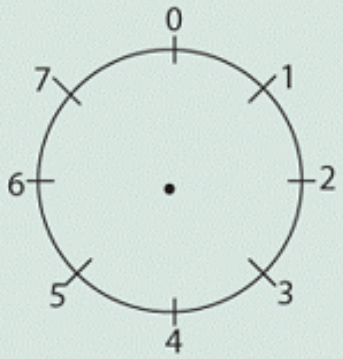


Fig. 2.11

7. $4 \oplus 12 =$

8. $6 \oplus 19 =$

9. $0 \oplus 20 =$

10. $5 \oplus 39 =$

11. $7 \oplus 12 =$

12. $2 \oplus 34 =$

13. Write down the names of five markets in your locality which are held in rotation over 5 days.

14. State the days of the week when the markets are held over a period of 5 weeks. Then prepare a table similar to Table 2.12.

15. Represent each market by a code number beginning with 0 (as in Table 2.11) up to the number 4 and use this to prepare a table similar to Table 2.12.

SUMMARY

In this chapter, we learnt that

- That modulus means modulo and it is thus represented as Zm, that is, set of integers modulo m.
- That arithmetic modulo m of the set of integers can be reduced to residue class system modulo m of a set of whole numbers 0, 1, 2, 3, 4, …, $n-1$, for example, in arithmetic (mod 6), all integers can be reduced to 0, 1, 2, 3, 4 and 5.
- That two integers a and b can have the same remainder when divided by m, we then say that $a = b$ with modulo m which is mathematically written as $a \equiv b \pmod{m}$. For example, $17 \div 8 = 2$ remainder 1 and $25 \div 8 = 3$ remainder 1. We then say that 17 and 25 are equal modulo 8, that is, $17 = 25 = 1 \pmod{8}$.
- Addition, subtraction and multiplication are possible under arithmetic modulo. Symbols such as $\oplus$, $\ominus$ and $\otimes$ are used in modular arithmetic to differentiate it from ordinary arithmetic of $+, -$ and $\times$.
- Division is at times not possible in modular arithmetic. It sometimes gives more than one value or no value at all.
- That addition and multiplication under modular arithmetic are commutative, while subtraction and division are not.

GRADUATED EXERCISES

Simplify the following:

1. $\dfrac{(-18) \times (-4) \times (+6)}{4 \times (-6)}$
2. $\dfrac{-4}{7} \times \dfrac{6}{-21} \times \dfrac{-6}{12}$
3. $\dfrac{4 \times 6 \times (-6) \times (+5)}{3 \times (-6) \times 7}$
4. $\dfrac{(+6) \times (-12)}{(-5) \times (-3)}$
5. $\dfrac{(18) \times (-8) \times (+6)}{(8) \times (+2) \times (-4)}$
6. $\dfrac{-66}{(+3) \times (-11)}$

Reduce 36 to its simplest form in

7. Modulo 8
8. Modulo 4
9. Modulo 5

Perform the following additions under modulo 7:

10. $8 + 21$
11. $36 + 49$
12. $33 + 37$

Find the quotients of the following:

13. $81 \equiv 4 \pmod 7$
14. $167 \equiv -9 \pmod{11}$
15. $138 \equiv 5 \pmod 7$
16. $18 \equiv -3 \pmod 7$

Convert the following to congruent and modular mathematical statements:

17. $6/27 - 9$
18. $3/47 - 5$
19. $10/86 - 6$
20. Find the following addition in modulo 9
    $89 \oplus 47$.
21. Find the following numbers in thei simplest form in modulo 7:
    (a) 47
    (b) 147
    (c) 302
22. Calculate in the given modulo:
    $55 \oplus 28 \pmod 8$.
23. Find the simplest form $-63 \pmod 7$.
24. Find the simplest positive form of -153 modulo 5.
25. Find $13 \ominus 17 \pmod 8$.
26. Calculate $16 \ominus 7 \pmod 9$
27. Find the values of the following:
    (a) $9 \otimes 21 \pmod{11}$
    (b) $94 \otimes 46 \pmod{13}$
28. Find the values of the following:
    (a) $32 \oslash 4 \pmod 8$
    (b) $84 \oslash 7 \pmod 5$

29. Where possible, find the values of the following in modulo 5:
    (a) $3 \circledast 4$
    (b) $4 \circledast 4$
    (c) $4 \circledast 2$

30. Find the solution or truth sets of the following:
    (a) $3y \equiv 3 \pmod 4$
    (b) $8r \equiv 1 \pmod 3$
    (c) $n + 8 \equiv 4 \pmod 9$
    (d) $2x \equiv 3 \pmod 7$

31. Solve the following linear congruences:
    (a) $5n + 2 \equiv 3 \pmod{11}$
    (b) $3x \equiv 5 \pmod 7$
    (c) $m - 4 \equiv 0 \pmod 6$
    (d) $k \equiv 8 \pmod{11}$
    (e) $5 - r \equiv 0 \pmod 7$

32. Solve the following linear congruences in mod 11:
    (a) $3x \equiv 1$
    (b) $5x \equiv 2$
    (c) $4x \equiv 1$

33. Arrange the first seven months of the year: Jan, Feb, Mar, Apr, May, June and July on a circular using the number code 0 to 6 respectively and accordingly. If this month is May, which month will it be in:
    (a) 5 months' time
    (b) 10 months' time
    (c) 7 months' time
    (d) 39 months' time

(e) 2 years' time

(f) 52 months' time

34. Reduce 45 to its simplest form.

(a) modulo 3

(b) modulo 4

(c) modulo 5

(d) modulo 6

35. Write down the addition $47 + 35 = 82$.

(a) Under each number, write its simplest form in module 6.

(b) What do you notice?

(c) Repeat the above step for mod 4 and mod 3.