A set is a collection of unique elements. The definition of a specific set determines which elements are members of the set.

(1). Z → set of integers (positive or negative including zero).

$[-inf, \ldots -1, 0, 1, \ldots inf]$.

(2) N → set of natural numbers (starting number is 1)

$[1, 2, 3 \ldots inf]$

(3). Q → set of rational numbers (Written like p/q, p & q are integers)

(4) R → set of real numbers (rational, Irrational numbers).

$[-inf, \ldots + inf]$.

Ex (1). $(Z, +)$ is a group or not? {set of integers with standard addition}

(axioms)

(i) Closure property → satisfies.

$a, b \in Z$ then $a+b \in Z$.

(ii) Associative property → satisfies.

$a+(b+c) = (a+b)+c$; $a, b, c \in Z$.

(iii) Identity Property → Satisfies.

$a+0 = 0+a = a$. ; $\underline{e=0} \in Z$.

(iv) Inverse property → Satisfies.

Inverse exists $= -a$.

$a+(-a) = (-a)+a = e = 0 \in Z$. So $(Z, +)$ is a Group.

Ex (2). $(N, +)$? ⇒ No Identity ⇒ No Group.

Ex (3) $(Z, *)$? ⇒ No inverse ⇒ No Group.

Ex (4). $(Q, *)$? ⇒ All satisfies ⇒ Group. [without 0](zero) $(Q_{\neq 0}, \times)$

Ex (5) $(Z, +)$ is an <u>abelian group</u>. becoz $\{a+b = b+a \in Z\}$

RING :- $(R, +, *)$ → $(R, +)$ is an abelian group
$(R, *)$ is a semigroup.

Semigroup → Satisfies closure & associative property both

Ex [$(Z, +, *)$ → Ring → Satisfies]
It is a commutative Ring with unity $e = 1$.

Ex $(2Z, +, *)$ → Ring → Satisfies.

[$(Q, +, *)$ is a field] $2, \frac{1}{2}$ both exists

MODULAR ARITHMETIC:-

→ Given any positive integer n and any nonnegative integer a, if we divide a by n, we get an integer quotient q and an integer remainder r that obey the following relationship:-

$$\boxed{a = qn + r \; ; \; 0 \leq r < n}$$

[The remainder r is often referred to as a residue.]

Example:-
(i). $a = 11$; $n = 7$; $11 = 1 \times 7 + 4$; $r = 4$ $q = 1$.
(ii). $a = -11$; $n = 7$; $-11 = (-2) \times 7 + 3$; $r = 3$ $q = -2$.

→ If a is an integer and n is a positive integer, we define $a \bmod n$ to be the remainder when a is divided by n. The integer n is called the modulus.

$$\boxed{a = \lfloor a/n \rfloor \times n + (a \bmod n)}$$

{$\lfloor x \rfloor$ → Largest integer less than or equal to x}

Example:-
(i). $11 \bmod 7 = 4$. (ii) $-11 \bmod 7 = 3$.

→ Two integers a and b are said to be congruent modulo n, if $(a \bmod n) = (b \bmod n)$. This is written as $\boxed{a \equiv b \pmod{n}}$

Example:- (i). $73 \equiv 4 \pmod{23}$
(ii) $21 \equiv -9 \pmod{10}$.

→ Modular Arithmetic Operation:-

The $(\bmod n)$ operator maps all integers into the set of integers $\{0, 1, \ldots (n-1)\}$.

properties:-
(i) $[(a \bmod n) + (b \bmod n)] \bmod n = (a+b) \bmod n$.
(ii) $[(a \bmod n) - (b \bmod n)] \bmod n = (a-b) \bmod n$.
(iii) $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$.

Example:- 1
(i). $11 \bmod 8 = 3$; $15 \bmod 8 = 7$.
$[(11 \bmod 8) + (15 \bmod 8)] \bmod 8 = [3+7] \bmod 8 = 10 \bmod 8 = 2$.
$(11 + 15) \bmod 8 = 26 \bmod 8 = 2$.
(ii) $[(11 \bmod 8) - (15 \bmod 8)] \bmod 8 = -4 \bmod 8 = 4$
$(11 - 15) \bmod 8 = -4 \bmod 8 = 4$.
(iii) $[(11 \bmod 8) \times (15 \bmod 8)] \bmod 8 = 21 \bmod 8 = 5$
$(11 \times 15) \bmod 8 = 165 \bmod 8 = 5$.

Example:- 2 $n = 8, a = 27, b = 34$. LHS = RHS
$5 = 5$

Addition modulo 8

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Multiplication modulo 8

x	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

→ **Property of Modular Arithmetic :-**

- Define the set Z_n as the set of non negative integers less than n :

$$Z_n = \{0, 1, \ldots\ldots (n-1)\}.$$

- This is referred to as the set of residues or residues classes modulo n.
- We can label the residue classes modulo n as $[0], [1], [2] \ldots [n-1]$, where

$$[r] = \{a : a \text{ is an integer}, a \equiv r \pmod n\}.$$

Example :-

The residue classes modulo 4 are :

$[0] = \{\ldots -16, -12, -8, -4, 0, 4, 8, 12, 16, \ldots\}$

$[1] = \{\ldots -15, -11, -7, -3, 1, 5, 9, 13, 17, \ldots\}$

$[2] = \{\ldots -14, -10, -6, -2, 2, 6, 10, 14, 18, \ldots\}$

$[3] = \{\ldots -13, -9, -5, -1, 3, 7, 11, 15, 19, \ldots\}$

Example:- Prove that Z_n is a commutative ring with a multiplicative identity element.

Application :- Used to solve higher powers.

Ex:- $3^8 \bmod 7$.

→ 1 way: $3^8 = 6561 \bmod 7 = 2$

→ 2 way: $3^4 \cdot 3^4 = 81 \cdot 81 \bmod 7 = 2$.

→ $3^4 \cdot 3^4 = 81 \cdot 81 \equiv 4 \cdot 4 \pmod 7$

$\equiv 16 \pmod 7 = 2$.

Ex:- $11^7 \bmod 13$. → $11^2 = 121 \equiv 4 \pmod{13}$.

$11^4 = (11^2)^2 \equiv 4^2 \equiv 3 \pmod{13}$.

Euclidean Algorithm :-

* It is a simple procedure for determining the greatest common divisor of ~~to~~ two positive integers.

The positive integer c is said to be the greatest common divisor of a and b if:

(i). c is a divisor of a and of b;

(ii). any divisor of a and b is a divisor of c.

$$\boxed{\gcd(a,b) = \max[k, \text{ such that } k|a \text{ and } k|b]}$$

$$\{\gcd(a,b) = \gcd(a,-b) = \gcd(-a,b) = \gcd(-a,-b)\} \quad \gcd(a,b) = \gcd(|a|,|b|)$$

Example:- $\gcd(60,24) = \gcd(60,-24) = 12.$ $\quad \boxed{\gcd(a,0) = |a|}$

$\gcd(55,22) = 11.$

* For any non negative integer a and any positive integer b

$$\boxed{\gcd(a,b) = \gcd(b, a \bmod b)}$$

Example:-

(i) $\gcd(55,22) = \gcd(22, 55 \bmod 22) = \gcd(22,11)$

$= \gcd(11, 22 \bmod 11) = \gcd(11,0) = 11$

(ii) $\gcd(18,12) = \gcd(12, 18 \bmod 12) = \gcd(12,6)$

$= \gcd(6, 12 \bmod 6) = \gcd(6,0) = 6.$

(iii) $\gcd(11,10) = \gcd(10, 11 \bmod 10) = \gcd(10,1)$

$= \gcd(1, 10 \bmod 1) = \gcd(1,0) = 1.$

Example:- (i) $\gcd(24140, 16762)$.

(ii) $\gcd(4655, 12075)$.

```
EUCLID (a,b)
1.  A ← a ; B ← b
2.  IF B = 0
      return A = gcd(a,b)
3.  R = A mod B.
4.  A ← B.
5.  B ← R.
6.  Go to step 2.
```

The algorithm has the following progression:

$$A_1 = B_1 * Q_1 + R_1$$

$$A_2 = B_2 * Q_2 + R_2$$

$$A_3 = B_3 * Q_3 + R_3$$

$$A_4 = B_4 * Q_4 + R_4$$

Example:- To find $\gcd(1970, 1066) = 2.$