2-2-21

4. Algebraic Structures

* Binary Operation :-

Let S be a set, then a mapping $f : S \times S \to S$ is called binary operation on the set S.

In general, a mapping $f : S^n \to S$ is called an n-ary operation on S and n is called the order of operation.

Eg: S = N (set of natural numbers)

$+(8,5) = 8+5 = 13 \in N$;

$+(4,5) = 4+5 = 9 \in N$;

$+ : N \times N \to N$ is a mapping

$\therefore$ + is a binary operation on the set of Natural numbers (N).

→ Example - 1 :

Let S = N, with "*" defined by $a * b = a^b$, $\forall a, b \in N$. Then for any $a, b \in N$ Then for any $a, b \in N$, $a^b \in N$. Hence "*" is a binary operation.

→ Example - 2 :

Let S = Z with "*" defined by $a * b = \frac{a}{b}$, $\forall a, b \in Z$. Then for any $a, 0, \in Z$, $\frac{a}{b} \notin Z$

Hence "*" is not a binary operation

1 9 1 3 1 A 0 5 L 0

* Algebraic Structure :-

Let S be a non-empty set. $f_1, f_2, f_3, \ldots$ are n-ary operations defined on S. Then a system consisting of a set S and one or more n-ary operations on the set is called an algebraic system or algebra or algebraic structure.

Let S be a non empty set and "*" is a binary operation defined on S then the ordered pair $(S, *)$ is called an algebraic structure.

$(N, +)$ is an algebraic structure

$(Z, +)$ is an algebraic structure

→ Example - 1 :

Let $A = Q \times Q$ and let "*" be a binary operation on A defined by $(a,b) * (c,d) = (ac, b + ad)$ for $(a,b), (c,d) \in A$. Then $\langle A, * \rangle$ is an algebraic structure.

→ Example - 2 :

Let $A = Z^+$ and let "*" be a binary operation on A defined by $a * b = \max\{a, b\}$ Then $\langle A, * \rangle$ is an algebraic structure.

→ **Note:**

Two algebraic systems $\langle X, o \rangle$ and $\langle Y, * \rangle$ are said to be of the same type whenever the n-ary operations "o", "*" have the same value of "n".

* **Properties of an algebraic system :-**

Let "o" be an operation on a non-empty set S. Then "o" is said to be

(i) Associative : if $a \circ (b \circ c) = (a \circ b) \circ c$, $\forall a, b, c \in S$

(ii) Commutative : if $a \circ b = b \circ a$, $\forall a, b \in S$

(iii) Identity : if $a \circ e = e \circ a = a$, $\forall a \in S$

(iv) Inverse : if for each $a \in S$, there exist an element $b \in S$ such that $a \circ b = b \circ a = e$

Suppose "*" be another operation on S, then

(v) Distributive : if $a \circ (b * c) = (a \circ b) * (a \circ c)$, $\forall a, b, c \in S$.

1 9 1 3 1 A 0 5 L 0

* **Semi Group :-**

Let S be a non-empty set and "o" is a binary operation defined on S then the algebraic structure $\langle S, o \rangle$ is called a semigroup if the operation "o" satisfies associative property. Or the algebraic structure $\langle S, o \rangle$ is called a semigroup if for any $a, b, c \in S$, $a \circ (b \circ c) = (a \circ b) \circ c$.

→ Example - 1:

Let " * " be defined by $a * b = \max\{a, b\}$, $\forall a, b \in z^+$. Then $\langle z^+, * \rangle$ is a semi group. Because if $a, b \in z^+$ either $\max\{a, b\} = a$ or $\max\{a, b\} = b$. So, $a * b \in z^+$. Hence " * " is a binary operation. Now, we show that it is associative. For this take three elements $a, b, c \in z^+$ then

$a * (b * c) = \max\{a, (b * c)\} = \max\{a, \max\{b, c\}\}$

$= \max\{a, b, c\}$

$\therefore a * (b * c) = (a * b) * c \quad \forall a, b, c \in z^+$.

Hence, " * " is associative

So, $\langle z^+, * \rangle$ is a semi group.

1 9 1 3 1 A 0 5 L 0

11-2-21

→ Semigroup :-

An algebraic structure $(S, \circ)$ is called semigroup if the binary operation '$\circ$' is associative i.e., $a \circ (b \circ c) = (a \circ b) \circ c \quad \forall\ a, b, c \in S$.

Eg - $(N, +)$ is semigroup.

* Monoid :-

An algebraic structure $(S, \circ)$ is called monoid if binary operation '$\circ$' is associative and S has identity. i.e.,

i) $a \circ (b \circ c) = (a \circ b) \circ c \quad \forall a, b, c \in S$

ii) There exists an element $e \in S$ such that $a \circ e = e \circ a = a \ \forall a \in S$.
Here, 'e' is called identity element in S

Eg - $(Z, \times)$, $(W, +)$ are monoids

1 9 1 3 1 A 0 5 L 0

* Groups :-

An algebraic structure $(S, \circ)$ is called group if binary operation '$\circ$' is associative and S has identity and inverse.

i) $a \circ (b \circ c) = (a \circ b) \circ c \quad \forall a, b, c \in S$ (Associative)

ii) There exist an element $e \in S$ such that for any $a \in S$, $a \circ e = e \circ a = a$ (identity)

iii) For every $a \in S$, there exist an element $b \in S$ such that $a \circ b = b \circ a = e$ (inverse)

* Abelian group :-

An algebraic structure $(S, \circ)$ is called abelian group if the binary operation '$\circ$' is associative, commutative and S has identity and inverse.

Eg - $(Z, +)$, $(R, +)$.

5-2-21

① Let $G = \{x : x \in R - \{0\}\}$ and "$*$" defined as $a * b = \frac{ab}{2}$ $\forall\ a, b \in G$ then show that $\langle G, * \rangle$ is an abelian group.

Sol. $G = \{x \mid x \in R - \{0\}\}$ and '$*$' is defined as $a * b = \frac{ab}{2}$ $\forall\ a, b \in G$

i) Binary :

Let $a, b \in G$

Then $a, b \in R$ and $a \neq 0$, $b \neq 0$

Now, $a * b = \frac{ab}{2} \in R$

Suppose $\frac{ab}{2} = 0$

$\Rightarrow ab = 0$

$\Rightarrow a = 0$ & $b = 0$

It is contradiction

$\therefore \frac{ab}{2} \neq 0$ i.e., $a * b \neq 0$

$\therefore a * b \in G$

Hence, '$*$' is a binary opeation.

ii) Associative :

Let $a, b, c \in G$

$a * (b * c) = a * \left(\frac{bc}{2}\right)$

$= \frac{abc}{4}$

$(a * b) * c = \left(\frac{ab}{2}\right) * c = \frac{abc}{4}$

$\therefore a * (b * c) = (a * b) * c$

$\therefore$ $*$ is associative

iii) Commutative:

Let $a, b \in G$

$(a * b) = \frac{ab}{2}$

$(b * a) = \frac{ba}{2}$

$\therefore (a * b) = (b * a)$

$\therefore$ '*' is commutative

iv) Identity:

$a * e = a$

$\Rightarrow \frac{ae}{2} = a$

$\Rightarrow e = 2$

Here, $2 \in G$ and

$a * 2 = \frac{2a}{2} = a$

$2 * a = \frac{2a}{2} = a$

$\therefore$ 'S' has identity

v) Inverse:

Let $a, b \in G$

$a * b = 2$

$\Rightarrow \frac{ab}{2} = 2$

$\Rightarrow ab = 4$

$\Rightarrow b = 4/a \in G$

Now, $a * b = a * \left[\frac{4}{a}\right]$

$= \frac{4a}{2a} = 2$

$\therefore b = 4/a$ is inverse of a

Hence, $(G, *)$ is an Abelian group

1913105LO

② If $G = \{x : x \in R - \{-1\}\}$ and "$*$" defined as $a * b = a + b + ab \ \forall\ a, b \in G$, then show that $(G, *)$ is a Group.

Sol. i) Binary:

Let $a, b \in G$

Then $a, b \in R$ and $a \neq -1, b \neq -1$

Now, $a * b = a + b + ab \in R$

Suppose $a + b + ab = -1$

then $a + b + ab + 1 = 0$

$\Rightarrow (a+1)(b+1) = 0$

$\Rightarrow a = -1$ or $b = -1$

It is a contradiction

$\therefore a + b + ab \neq -1$ i.e., $a * b \neq -1$

$\therefore a * b \in G$

$\therefore$ '$*$' is a binary operation

ii) Associative:

Let $a, b, c \in G$

$a * (b * c) = a * (b + c + bc)$

$= a + [b + c + bc] + [ab + ac + abc]$

$= a + b + c + ab + bc + ac + abc$

$(a * b) * c = (a + b + ab) * c$

$= [a + b + ab] + c + [ac + bc + abc]$

$= a + b + c + ab + bc + ac + abc$

$\therefore a * (b * c) = (a * b) * c$

$\therefore$ '$*$' is associative

iii) Existence of identity:

Here, $0 \in G$ and

$$a * 0 = a + 0 + (a.0) = a$$

$$0 * a = 0 + a + (0.a) = a$$

$\therefore$ 0 is the identity element

iv) Existence of inverse:

$$a * b = b * a = 0$$

$$\Rightarrow a + b + ab = 0$$

$$\Rightarrow b(1+a) = -a$$

$$\Rightarrow b = \frac{-a}{1+a}$$

Suppose $\frac{-a}{1+a} = -1$

$$\Rightarrow -a = -a - 1$$

$$\Rightarrow 0 \neq -1$$

It is contradiction

$\therefore \frac{-a}{a+1} \neq -1$

$\therefore b \in G$

Now, $a * b = a * \left[\frac{-a}{1+a}\right]$

$$= a - \frac{a}{1+a} - \frac{a^2}{1+a}$$

$$= \frac{a + a^2 - a - a^2}{1+a} = 0$$

$\therefore b = \frac{-a}{1+a}$ is inverse of a

Hence, $(G, *)$ is a group.

1 9 1 3 1 A 0 5 L 0

* Order of a group :-

The order of a group $\langle G, * \rangle$ denoted by $|G|$ is the number of elements of G, when G is finite.

* Subgroup :-

Let $\langle G, * \rangle$ be a group and $S \subseteq G$ be such that it satisfies the following conditions

i) For any $a, b \in S$, $a * b \in S$

ii) $e \in S$ where "e" is the identity of $\langle G, * \rangle$

iii) For any $a \in S$, $a^{-1} \in S$

Then $\langle S, * \rangle$ is called a subgroup of $\langle G, * \rangle$

$G = \{1, \omega, \omega^2\}$ where $\omega^3 = 1$

G under multiplication is a group

$S = (1)$ is subgroup the group G (cube roots of unity under multiplication)

→ Note :-

i) If $\langle S, * \rangle$ is a subgroup of $\langle G, * \rangle$, then $\langle S, * \rangle$ is itself a group with the same identity element as that of $\langle G, * \rangle$. Also the operation "$*$" on S is same as the operation "$*$" in G, but restricted to S.

ii) For any group, $\langle G, * \rangle$, naturally $\langle G, * \rangle$ and $\langle G, * \rangle$ are trivial subgroups of $\langle G, * \rangle$. All other subgroups of are called proper subgroups.

* **Theorem :-**

A subset $S = \phi$ of G is a subgroup of $\langle G, * \rangle$ iff for any pair of elements $a, b \in S$, $a * b^{-1} \in S$.

Proof :

Let us assume that subset $S = \phi$ of G is a subgroup of $\langle G, * \rangle$

Now, we show that for any pair of elements $a, b \in S$, $a * b^{-1} \in S$

Let $a, b \in S$. Since, $b \in S$ so by definition of subgroup, we've $b^{-1} \in S$.

Now, we've $a, b^{-1} \in S$. So, by definition of subgroup we've $a * b^{-1} \in S$.

Hence, for any pair of elements $a, b \in S$, $a * b^{-1} \in S$ if a subset $S = \phi$ of G is a subgroup of $\langle G, * \rangle$.

Conversely, suppose that $S \neq \phi$ is a subset of G and for any pair of elements $a, b \in S$, $a * b^{-1} \in S$.

Now, we've to show a non-empty ~~set~~ subset S is a subgroup of $\langle G, * \rangle$

1 9 1 3 1 A 0 5 L 0

Since, $a, a \in S$, so by hypothesis we have $e = a * a^{-1} \in S$ where e is the identity element of G.

Now, for $e, a \in S$, we have $e * a^{-1} \in S$ $\Rightarrow a^{-1} \in S$. Similarly, $b^{-1} \in S$.

Finally because $a, b^{-1} \in S$ so we have $a * (b^{-1})^{-1} \in S \Rightarrow a * b \in S$

$\therefore$ (i) $e \in S$, where "e" is the identity element of $(G, *)$.

(ii) For any $a \in S$, $a^{-1} \in S$

(iii) For any $a, b \in S$, $a * b^{-1} \in S$.

Hence, S is a subgroup of $(G, *)$.

1 9 1 3 1 A 0 5 L 0

9-2-21

* Homomorphism :-

Let $\langle G, * \rangle$ and $\langle H, \circ \rangle$ be two groups. A mapping $f: G \to H$ is called a group homomorphism from $\langle G, * \rangle$ to $\langle H, \circ \rangle$ if for any $a, b \in G$, $f(a * b) = f(a) \circ f(b)$.

→ Example:

Let G be the additive group of integers and G' be the multiplicative group whose elements are 2^m for $m \in Z$. Consider the mapping $f: G \to G'$ by $f(m) = 2^m$ for $m \in Z$.

Let $a, b \in G(N, +)$

$f(a+b) = 2^{a+b} = 2^a \cdot 2^b = f(a) \cdot f(b)$

* Kernel of a Homomorphism :-

Let f be a group homomorphism from $(G, *)$ to $(H, \circ)$. Then the set of all elements of G which are mapped into e_H i.e., $\ker f = \{a \in G / f(a) = e_H\}$

where e_H is the identity element in H.

Ex -

Consider a mapping $f : (R, +) \to (R^+, \cdot)$ defined as $f(x) = a^x$, then $\ker f = \{0\}$, where 'a' is any non zero real number.

→ Note:

(a) If $f : G \to H$ is an homomorphism and G and H are groups, then

$f(a) * f(e_G) = f(a * e_G) = f(a)$ &

$f(e_G) * f(a) = f(e_G * a) = f(a)$

⇒ If e_G is the identity in G, then $f(e_G) = e_H$ is the identity element in H.

(b) If $f : G \to H$ is an homomorphism and G and H are groups, then

$f(a) * f(a^{-1}) = f(a * a^{-1}) = f(e_G) = e_H$ and

$f(a^{-1}) * f(a) = f(a^{-1} * a) = f(e_G) = e_H$

⇒ If a^{-1} is the inverse of a in G, then $f(a^{-1})$ is the inverse of $f(a)$ in H.

⇒ $f(a^{-1}) = [f(a)]^{-1}$

1 9 1 3 1 A 0 5 L 0

* Left coset of a subgroup :-

Let $\langle H, * \rangle$ be a subgroup of $\langle G, * \rangle$. For any $a \in G$, the set aH defined by $aH = \{a * h / h \in H\}$ is called the left coset of H in G determined by the element $a \in G$.

→ Example :

$G = \{1, \omega, \omega^2\}$ where $\omega^3 = 1$ under multiplication

$H = \{1\}$ is subgroup of G

FOR $\omega \in G$

$\omega H = \{\omega\}$ is called left coset of H in G determined by element $\omega = G$.

→ Example :

Let G be the additive group of integers and H be the subgroup of obtained by multiplying each element of G by 3 then $1+H, 2+H, 0+H$ are all left cosets of H in G.

* Right Coset of a subgroup :-

Let $\langle H, * \rangle$ be a subgroup of $\langle G, * \rangle$. For any $a \in G$, the set Ha defined by $Ha = \{h * a / h \in H\}$ is called the right coset of H in G determined by element $a \in G$.

1 9 1 3 1 A 0 5 L 0

Congruent Modulo m :-

If "a" and "b" are any two nos. then we say that $a \equiv b \pmod m$ or $a - b \equiv 0 \pmod m$ if $m(a-b)$ i.e., $\frac{a-b}{m}$ = integer

→ Example :

$5 \equiv 2 \pmod 3$, $6 \equiv 4 \pmod 2$

Twin Primes :-

A pair of prime numbers is said to be twin primes if they differ by 2.

Eg - 3, 5 are twin primes

Perfect Number :

A number "n" is said to be perfect if the sum of all divisors of n (including n) is equal to 2n.

Eg - 6, 28 are perfect numbers.

Since 1, 2, 3, 6 are divisors of 6 and
sum of divisors = 12 = 2(6).

1, 2, 4, 7, 12, 28 are divisors of 28 and
sum of divisors = 54 = 2(28).

Co-Prime :-

Two numbers "a" and "b" are said to be co-prime (relatively prime) if "1" is the only common divisor of "a" and "b"
i.e., (a, b) = 1 or gcd of a, b = 1

Eg - (4, 5) = 1, (3, 7) = 1.

1 9 1 3 1 A 0 5 L 0

* Properties of Congruence :-

i) If $a \equiv b \pmod m$, then $a+c \equiv b+c \pmod m$ and $ac \equiv bc \pmod m$ for any integer "c"

ii) If $a \equiv b \pmod m$ and if $c \equiv d \pmod m$, then $a+c \equiv b+d \pmod m$ and $a-c \equiv b-d \pmod m$ and $ac \equiv bd \pmod m$.

iii) If $a \equiv b \pmod m$, then if $a^2 \equiv b^2 \pmod m$ for every positive integer "k".

* Polynomial Congruence :-

Let $f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$ be a polynomial with integral coefficients, and if $a_n \not\equiv 0 \pmod m$, then we say that $f(x) \equiv 0 \pmod m$ is polynomial Congruence modulo "m" of degree "n".

* Linear Congruence :-

A polynomial congruence of degree "1" is called a linear congruence. Any linear congruence can be written in the form $ax \equiv b \pmod m$ where $a \not\equiv 0 \pmod m$.

* Solution of Linear Congruence :-

An integer "t" is said to be a solution of linear congruence $ax \equiv b \pmod m$ if $at \equiv b \pmod m$ i.e., $m \mid (at - b)$.

11-2-21

→ Note:

i) If x_1 is a solution of $ax \equiv b \pmod m$, and any integer "x_2" is such that $x_2 \equiv x_1 \pmod m$ then "x_2" is also a solution of $ax \equiv b \pmod m$.

ii) A linear congruence may or may not have a solution.
$2x \equiv 1 \pmod 4$ has no solution

iii) A linear congruence $ax \equiv b \pmod m$ has a solution iff (a, m) divides b.

iv) If $(a, m) = d$ and $d \mid b$, then the congruence $ax \equiv b \pmod m$ has exactly "d" incongruent solutions mod m.

v) If $(a, m) = 1$, then the congruence $ax \equiv b \pmod m$ has a unique solution.

1 9 1 3 1 A 0 5 L 0

→ Examples:

i) $135x \equiv 6 \pmod{10}$ has no solution
When comparing the above congruence with $ax \equiv b \pmod m$ we've $a=135$, $b=6$, $m=10$ and $(135, 10) = 5 = d$ and $d \mid b$. Hence, $135x \equiv 6 \pmod{10}$ has no solution

ii) $3x \equiv 5 \pmod 7$ has unique solution
When comparing the above congruence with $ax \equiv b \pmod m$ we've $a=3$, $b=5$, $m=7$ and $(3, 7) = 1$. Hence $3x \equiv 5 \pmod 7$ has unique solution.

iii) $4x \equiv 5 \pmod 6$ has no solution

When comparing the above congruence with $ax \equiv b \pmod m$ we've $a=4, b=5, m=6$ and $(4,6)=2=d$ and $d \mid b$. Hence, $4x \equiv 5 \pmod 6$ has no solution

iv) $10x \equiv 15 \pmod{35}$ posses 5 solutions

When comparing the above congruence with $ax \equiv b \pmod m$, we've $a=10, b=15$, $m=35$ and $(10,35)=5=d$ and $d \mid b$. Hence, $10x \equiv 15 \pmod{35}$ posses 5 solutions

v) $3x+2 \equiv 0 \pmod 7$ has unique solution

Given congruence is $3x+2 \equiv 0 \pmod 7 \Rightarrow$
$3x \equiv -2 \pmod 7$

When comparing the above congruence with $ax \equiv b \pmod m$, we've $a=3, b=-2, m=7$ and $(3,7)=1$. Hence $3x+2 \equiv 0 \pmod 7$ has unique solution.

1913105LO

* Multiplicative inverse of "a" :

For $0<a<m$, if there exists an element "b" such that $ab \pmod m = 1$ or $ab \equiv 1 \pmod m$ then b is said to be multiplicative inverse of a.

* Euler's function :-

The number of integers less than or equal to "n" and which are co-prime to "n" is called Euler's function of "n" and is denoted by $\phi(n)$.

Eg: $\phi(1) = 1$, $\phi(2) = 1$,

$\phi(8) = 4 = \#\{1,3,5,7\}$

$\phi(10) = 4 = \#\{1,3,7,9\}$, $\phi(7) = 6$

→ Note:

i) If "p" is prime number, then
$\phi(p) = p-1$.

ii) If "p" is prime number, then
$\phi(p^k) = p^k\left(1 - \frac{1}{p}\right) = p^k - p^{k-1}$

iii) If "a" and "b" are co-prime to each other then $\phi(ab) = \phi(a).\phi(b)$

1 9 1 3 1 A 0 5 L 0

* Euler's Theorem :-

Let "a" and "m" be relatively prime. then for any a,

$a^{\phi(m)} \pmod m = 1$ or $a^{\phi(m)} \equiv 1 \pmod m$.

→ Note:

If $a^{\phi(m)} \equiv 1 \pmod m$ then $a.a^{\phi(m)-1} \equiv 1 \pmod m$

$\Rightarrow a.b \equiv 1 \pmod m$ where $b = a^{\phi(m)-1} \pmod m$. is the inverse of a which is obtained by using Euler's theorem, where $\phi(m)$ is Euler's function of m.

* Chinese Remainder Theorem :-

Let $n_1, n_2, n_3, \ldots, n_s$ be positive integers such that the gcd $(n_i, n_j) = 1$ for $i \neq j$.
Then the system of linear congruences

$$x \equiv a_1 \pmod{n_1},$$
$$x \equiv a_2 \pmod{n_2},$$
$$x \equiv a_3 \pmod{n_3},$$
$$\vdots$$
$$x \equiv a_s \pmod{n_s}$$

has a simultaneous solution, which is unique modulo the integer N.

i.e., $x \equiv [a_1 N_1 x_1 + a_2 N_2 x_2 + \ldots + a_s N_s x_s] \pmod{N}$ is the solution,

where $N = n_1 \cdot n_2 \cdot n_3 \ldots n_s$,

$N_1 = \frac{N}{n_1}$, $N_2 = \frac{N}{n_2}$, $\ldots$ $N_s = \frac{N}{n_s}$ and

$N_1 x_1 \equiv 1 \pmod{n_1}$, $N_2 x_2 \equiv 1 \pmod{n_2}$, $\ldots$, $N_s x_s \equiv 1 \pmod{n_s}$

(3) Using Chinese Remainder theorem, find a solution of $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$.

Sol. Given system of congruences are

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

By comparing the above system with $x \equiv a_1 \pmod{n_1}$, $x \equiv a_2 \pmod{n_2}$, $x \equiv a_3 \pmod{n_3}$

We've $a_1 = 2$, $a_2 = 3$, $a_3 = 2$.
$n_1 = 3$, $n_2 = 5$, $n_3 = 7$.

J 9 1 3 1 A 0 5 L 0

So, $N = n_1 . n_2 . n_3 = 3.5.7 = 105$

$N_1 = \frac{N}{n_1} = \frac{105}{3} = 35$

$N_2 = \frac{N}{n_2} = \frac{105}{5} = 21$ $\quad N_3 = \frac{N}{n_3} = \frac{105}{7} = 15$

$N_1 x_1 \equiv 1 \pmod{n_1}$

$35 x_1 \equiv 1 \pmod 3$

$2 x_1 = 1 \pmod 3$

$x_1 = 2$

$N_2 x_2 \equiv 1 \pmod{n_2}$

$21 x_2 \equiv 1 \pmod 5$

$1 x_2 \equiv 1 \pmod 5$

$x_2 = 1$

$N_3 x_3 \equiv 1 \pmod{n_3}$

$15 x_3 = 1 \pmod 7$

$1 x_3 = 1 \pmod 7$

$x_3 = 1$

$\therefore x \equiv [a_1 N_1 x_1 + a_2 N_2 x_2 + \dots + a_3 N_3 x_3] \pmod N$

$= [2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1] \pmod{105}$

$= [140 + 63 + 30] \pmod{105}$

$= 233 \pmod{105}$

$= 23 \pmod{105}$

$\therefore x \equiv 23 \pmod{105}$ is the solution of given system

1913105L0

④ Solve the following linear congruences by using Chinese Remainder Theorem.

HW

i) $x \equiv 1 \pmod 2$

$x \equiv 2 \pmod 3$

$x \equiv 4 \pmod 5$

Sol. By comparing the above system with $x \equiv a_1 \pmod{n_1}$, $x \equiv a_2 \pmod{n_2}$, $x \equiv a_3 \pmod{n_3}$.

$a_1 = 1 \quad a_2 = 2 \quad a_3 = 4 \quad n_1 = 2 \quad n_2 = 3 \quad n_3 = 5$

$\therefore N = n_1 . n_2 . n_3 = 2 \times 3 \times 5 = 30$

$N_1 = \frac{N}{n_1} = \frac{30}{2} = 15$

$N_2 = \frac{N}{n_2} = \frac{30}{3} = 10$

$N_3 = \frac{N}{n_3} = \frac{30}{5} = 6$

$N_1 x_1 \equiv 1 \pmod{n_1}$ $N_2 x_2 \equiv 1 \pmod{n_2}$ $N_3 x_3 \equiv 1 \pmod{n_3}$

$15 x_1 \equiv 1 \pmod 2$ $10 x_2 \equiv 1 \pmod 3$ $6 x_3 \equiv 1 \pmod 5$

$x_1 = 1$ $x_2 = 1$ $x_3 = 1$

$\therefore x = [a_1 N_1 x_1 + a_2 N_2 x_2 + \dots a_3 N_3 x_3] \pmod N$

$= [1.15.1 + 2.10.1 + 4.6.1] \pmod{30}$

$= 59 \pmod{30}$

$x = 29 \pmod{30}$ is the solution of given system

ii) Sol.

$x_1 \equiv 1 \pmod 2$ $x \equiv 1 \pmod 3$ $x \equiv 1 \pmod 5$

Comparing with $x \equiv a_1 \pmod{n_1}$, $x \equiv a_2 \pmod{n_2}$, $x \equiv a_3 \pmod{n_3}$

$a_1 = 1$ $a_2 = 1$ $a_3 = 1$

$n_1 = 2$ $n_2 = 3$ $n_3 = 5$

$N = n_1 . n_2 . n_3 = 30$

$N_1 = \frac{30}{2} = 15$ $N_2 = \frac{30}{3} = 10$ $N_3 = \frac{30}{5} = 6$

$N_1 x_1 \equiv 1 \pmod{n_1}$ $N_2 x_2 \equiv 1 \pmod{n_2}$ $N_3 x_3 \equiv 1 \pmod{n_3}$

$15 x_1 \equiv 1 \pmod 2$ $10 x_2 \equiv 1 \pmod{n_3}$ $6 x_3 \equiv 1 \pmod 5$

$x_1 = 1$ $x_2 = 1$ $x_3 = 1$

$x = [1.15.1 + 1.10.1 + 1.6.1] \pmod{30}$

$= 31 \pmod{30}$

$x = 1 \pmod{30}$ is the solution of given system

1 9 1 3 1 A 0 5 L 0

12-2-21

* Fermat's Theorem :-

If "p" is a prime, and (a.p) = 1 then $a^{m-1} \equiv 1 \pmod{p}$.

⑤ Find all integers "x" which satisfy the condition $x \equiv 1 \pmod 7$, $x \equiv 6 \pmod 9$, $x \equiv 5 \pmod{11}$

Sol. Comparing the above system with $x \equiv a_1 \pmod{n_1}$, $x \equiv a_2 \pmod{n_2}$, $x \equiv a_3 \pmod{n_3}$

we get $a_1 = 1$ $a_2 = 6$ $a_3 = 5$

$n_1 = 7$ $n_2 = 9$ $n_3 = 11$

So, $N = n_1 \cdot n_2 \cdot n_3 = 7.9.11 = 693$

$N_1 = \frac{693}{7} = 99$ $N_2 = \frac{693}{9} = 77$ $N_3 = \frac{693}{11} = 63$

$N_1 x_1 \equiv 1 \pmod{n_1}$ $N_2 x_2 \equiv 1 \pmod{n_2}$ $N_3 x_3 \equiv 1 \pmod{n_3}$

$99 x_1 \equiv 1 \pmod 7$ $77 x_2 \equiv 1 \pmod 9$ $63 x_3 \equiv 1 \pmod{11}$

$x_1 = 1$ $x_2 = 5$ $x_3 = 8$

$\therefore x \equiv [a_1 N_1 x_1 + a_2 N_2 x_2 + \ldots + a_3 N_3 x_3] \pmod N$

$= [1.99.1 + 6.77.5 + 5.63.8] \pmod{693}$

$= [99 + 2310 + 2520] \pmod{693}$

$= 4929 \pmod{693}$

$= 78 \pmod{693}$

$\therefore x \equiv 78 \pmod{693}$ is the solution of given system.

⑥ Give the residue representation of all integers in Z_{60} for moduli $m_1 = 4$, $m_2 = 3$ and $m_3 = 5$.

1913105LO

Sol. Given that $Z_{60} = \{0, 1, 2, \ldots, 59\}$

i) $m_1 = 4$, the remainder after divisible by 4 are $\{0, 1, 2, 3\}$

$\overline{0} = [0]_R = \{0, 4, 8, \ldots, 56\}$ i.e.,

For $x \in \overline{0} \Rightarrow x \equiv 0 \pmod 4$

$\overline{1} = [1]_R = \{1, 5, 9, \ldots, 57\}$ i.e.,

For $x \in \overline{1} \Rightarrow x \equiv 1 \pmod 4$

$\overline{2} = [2]_R = \{2, 6, 10, \ldots, 58\}$ i.e.,

For $x \in \overline{2} \Rightarrow x \equiv 2 \pmod 4$

$\overline{3} = [3]_R = \{3, 7, 11, \ldots, 59\}$ i.e.,

For $x \in \overline{3} \Rightarrow x \equiv 3 \pmod 4$

ii) $m_2 = 3$, the remainder after divisibly by 3 are $\{0, 1, 2\}$

$[0]_R = \{0, 3, 6, \ldots, 57\}$ i.e.,

For $x \in \overline{0} \Rightarrow x \equiv 0 \pmod 3$

$[1]_R = \{1, 4, 7, \ldots, 58\}$ ie.,

For $x \in \overline{1} \Rightarrow x \equiv 1 \pmod 3$

$[2]_R = \{2, 5, 8, \ldots, 59\}$ i.e.,

For $x \in \overline{2} \Rightarrow x \equiv 2 \pmod 3$

iii) $m_3 = 5$, the remainder after divisible by 5 are $\{0, 1, 2, 3, 4\}$

$[0]_R = \{0, 5, 10, \ldots 55\}$ i.e.,

For $x \in \overline{0} \Rightarrow x \equiv 0 \pmod 5$

$[1]_R = \{1, 6, 11, \ldots 56\}$ i.e,

For $x \in \overline{1} \Rightarrow x \equiv 1 \pmod 5$

$[2]_R = \{2, 7, 12, \ldots, 57\}$ i.e.,

For $x \in \overline{2} \Rightarrow x \equiv 2 \pmod 5$

$[3]_R = \{3, 8, 13, \ldots, 58\}$ i.e.,

For $x \in \overline{3} \Rightarrow x \equiv 3 \pmod 5$

$[4]_R = \{4, 9, 14, \ldots, 59\}$ i.e.,

For $x \in \overline{4} \Rightarrow x \equiv 4 \pmod 5$

Q. Compute the inverse of each element in Z_7 using Fermat's theorem.

Sol.

Fermat's theorem:

If "p" is a prime, and $(a, p) = 1$ then $a^{p-1} \equiv 1 \pmod p$

Given that $Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$

"0" has no inverse, since inverse exist for non zero elements.

1 9 1 3 1 A 0 5 L 0

Inverse of remaining:

$1^{7-1} \equiv 1 \pmod 7 \Rightarrow 1^6 \equiv 1 \pmod 7 \Rightarrow 1.1^5 \equiv 1 \pmod 7$

$\Rightarrow 1^5 = 1$ is the inverse of 1.

$2^{7-1} \equiv 1 \pmod 7 \Rightarrow 2^6 \equiv 1 \pmod 7 \Rightarrow 2.2^5 \equiv 1 \pmod 7$

$\Rightarrow 2^5 = 2.2^3.2^2 \equiv 1 \pmod 7 \Rightarrow 1.2^2 = 4$ is inverse of 2

$3^{7-1} \equiv 1 \pmod 7 \Rightarrow 3^6 \equiv 1 \pmod 7 \Rightarrow 3.3^5 \equiv 1 \pmod 7$

$\Rightarrow 3^5 = 3.3.3^2.3^2 \equiv 1 \pmod 7 \Rightarrow 3.2.2 = 12$

$= 5$ is inverse of 3

$4^{7-1} \equiv 1 \pmod 7 \Rightarrow 4^6 \equiv 1 \pmod 7 \Rightarrow 4.4^5 \equiv 1 \pmod 7$

$\Rightarrow 4^5 = 4.4.4^2.4^2 \equiv 1 \pmod 7 \Rightarrow 4.2.2 = 16$

$= 2$ is inverse of 4

$5^{7-1} \equiv 1 \pmod 7 \Rightarrow 5^6 \equiv 1 \pmod 7 \Rightarrow 5.5^5 \equiv 1 \pmod 7$

$\Rightarrow 5^5 = 5.5.5^2.5^2 \equiv 1 \pmod 7 \Rightarrow 5.4.4 = 80$

$= 3$ is inverse of 5

$6^{7-1} \equiv 1 \pmod 7 \Rightarrow 6^6 \equiv 1 \pmod 7 \Rightarrow 6.6^5 \equiv 1 \pmod 7$

$\Rightarrow 6^5 = 6.6.6^2.6^2 \equiv 1 \pmod 7 \Rightarrow 6.1.1 = 6$ is

its inverse of 6

(8) Compute the inverse of each element in Z_{12}, if exists using Euler's theorem.

Sol.

$Z_{12} = \{0, 1, 2, 3, \ldots, 11\}$

"0" has no inverse, since inverse exist for non-zero elements.

Inverse of remaining:

W.K.T. $\phi(p) = p-1$, $\phi(p^k) = p^k - p^{k-1}$ and

$\phi(ab) = \phi(a).\phi(b) \Rightarrow \phi(12) = \phi(3.4) = \phi(3).\phi(4)$

$= (3-1)\phi(2^2)$

$= (3-1)(2^2-2)$

$= 2.2 = 4$

∴ The numbers which are relatively prime to 12 are $\{1, 5, 7, 11\}$

$1^4 \equiv 1 \pmod{12} \Rightarrow 1.1^3 \equiv 1 \pmod{12} \Rightarrow 1^3 = 1$ is inverse of 1

$5^4 \equiv 1 \pmod{12} \Rightarrow 5.5^3 \equiv 1 \pmod{12} \Rightarrow 5^3 \equiv 5.5^2 \equiv 1 \pmod{12}$

$\Rightarrow 5.1 = 5$ is inverse of 5

$7^4 \equiv 1 \pmod{12} \Rightarrow 7.7^3 \equiv 1 \pmod{12} \Rightarrow 7^3 = 7.7^2 = 1 \pmod{12}$

$\Rightarrow 7.1 = 7$ is inverse of 7

1 9 1 3 1 A 0 5 L 0

$11^4 \equiv 1 \pmod{12} \Rightarrow 11.11^3 \equiv 1 \pmod{12} \Rightarrow 11^3 \equiv 11.11^2 \equiv 1 \pmod{12}$

$\Rightarrow 11.1 = 11$ is inverse of 11.

⑨ Using Chinese Remainder theorem, find a solution of linear congruence $17x \equiv 9 \pmod{276}$

Sol. Given linear congruence is $17x \equiv 9 \pmod{276}$

Since, $276 = 3.4.23$

So, the given linear congruence is equivalent to the system of congruences

$17x \equiv 9 \pmod 3, \; 17x \equiv 9 \pmod 4, \; 17x \equiv 9 \pmod{23}$

$2x \equiv 9 \pmod 3, \; 1x \equiv 9 \pmod 4, \; 17x \equiv 9 \pmod{23}$

$2x \equiv 0 \pmod 3, \; x \equiv 1 \pmod 4, \; 17x \equiv 9 \pmod{23}$

$x \equiv 0 \pmod 3, \; x \equiv 1 \pmod 4, \; 17.19x \equiv 9.19 \pmod{23}$

$[\because 17.19 = 1 \pmod{23}]$

$x \equiv 0 \pmod 3, \; x \equiv 1 \pmod 4, \; x \equiv 171 \pmod{23}$

$x \equiv 0 \pmod 3, \; x \equiv 1 \pmod 4, \; x \equiv 10 \pmod{23}$

$[\because \frac{171-10}{23}$ is integer$]$

By comparing, $a_1 = 0 \quad a_2 = 1 \quad a_3 = 10$

$n_1 = 3 \quad n_2 = 4 \quad n_3 = 23$

So, $N = n_1.n_2.n_3 = 276$

$N_1 = \frac{276}{3} = 92 \qquad N_2 = \frac{276}{4} = 69 \qquad N_3 = \frac{276}{23} = 12$

$N_1x_1 \equiv 1 \pmod{n_1} \qquad N_2x_2 \equiv 1 \pmod{n_2} \qquad N_3x_3 \equiv 1 \pmod{n_3}$

$92x_1 \equiv 1 \pmod 3 \qquad 69x_2 \equiv 1 \pmod 4 \qquad 12x_3 \equiv 1 \pmod{23}$

$x_1 = 2 \qquad x_2 = 1 \qquad x_3 = 2$

$\therefore x = [0.92.2 + 1.69.1 + 10.12.2] \pmod{276}$

$= [0 + 69 + 240] \pmod{276}$

$= 309 \pmod{276}$

$\therefore x = 33 \pmod{276}$ is solution of given system