UNIT-2

Elementry Number Theory:- It is the branch of Number the in which elementry methods (arithmetic, geometry, and high school algebra) are used to solve questions with Integer or rational solutions.

~~Finite~~ Fields:- A field $(F, +, \times)$ is a set of elements with binary operations say addition and multiplicatio such that if a, b, c. are the elements of F, and t following axioms are satisfied.

for addition Operations:- 1. Closer, 2. associative, 3. Additive Identity 4. Commutative 5. Additive inverse.

for Multiplication Operation:- M6. Closer, 7. Associative 8. multiplicative Identity 9. Distributive 10. Commutative. 11. No divisors. 12. Multiple Inverse exist.

If A1 — A6 :
M6 — M7 .
M9 — M10 → Commutative Ring.

M8, M11 → Integral domain

• Multiplective Inverse:- If $a \in F$, e - multiplication identity ordinary multiplication identity is 1 then there must exists an element a^{-1} such that

$$a^{-1} \times a = a \times a^{-1} = e \quad (=1)$$

Finite field: ib the order of the field is finite.
* order = size of the set)

Ring:- Addition and multiplication modulo 8

$Z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$

$(Z_8, +, *)$ - $+, *$, addition and multiplication modulo 8.

a	additive inverse	multiplicative inverse
0	0	—
1	7	1
2	6	—
3	5	3
4	4	—
5	3	5
6	2	—
7	1	7

$(5 \times 5) \text{ modulo } 8 = 25 \bmod 8 = 1$

If a and n relative prime then multiplicative inverse exists to Z_n

Consider n as a prime $n = p$

$Z_p = \{0, 1, 2, 3, \ldots\ldots (p-1)\}$

Since, p is prime so, all the element of Z_p are relatively prime to p.

ib $a \in Z_p$ then a and p relatively prime.

modulo p addition and multiplication. $(Z_p, +, *)$.

+ and * mod p addition and multiplication then it must be a field.

Example:- Z_7 we consider $p=7$ $+, *$, modulo 7 add. mult.

Addition of modulo 7.

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

multiplication:

	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	(1)	2	3	4	5	6
2	0	2	4	6	(1)	3	5
3	0	3	6	2	5	(1)	4
4	0	4	(1)	5	2	6	3
5	0	5	3	(1)	6	4	2
6	0	6	5	4	3	2	(1)

$a * a^{-1} = 1$ for each $a \in Z_7$ other 0.

Under addition and Mul modulo p on Zp is a field.

· Zp is a prime field :-

⇒ GF(p) ✓ Galois field.
GF(2) ✗ GF(2^n)

* Algebric Structure :- The set of elements and the operations on them is called an algebric structure. It includes groups, Ring, fields.

Group :- It is a set of elements with a binary operation that satisfies four properties. A commutative group satisfies an extra property commutativity.

- Closure :- For all a, b ∈ G we have a · b ∈ G.
- Associativity :- For all a, b, c ∈ G we have

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

- Existence of identity :- There exists an element e ∈ G is called identity of the group, such that

$$e \cdot a = a \cdot e = a \quad \text{for all } a \in G$$

- Existence of inverse :- For each a ∈ G, there exists a unique element b ∈ G, called the inverse of a such that a · b, b · a = e.

* A group (G) with the addition of commutative property is known as commutative group or abelian group.

- for all a, b ∈ G we have (a · b) = (b · a)

A group with finite no. of elements is known as finite group i.e |G| < ∞.

Group:-

Let G be a non void set with a binary operation $*$ that assign to each ordered pair (a,b) of elements of G an element of G denoted by $a*b$, we say that G is a group under the binary operation $*$, if the following three properties are satisfied.

① Associative :- The bo $*$ is associative.

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

$\forall a,b,c \in G$.

② Identity:- There an element e, called the identity in G such that

$$a*e = e*a = a$$

$\forall a \in G$.

③ Inverse:- For each element a in G, there is an element b in G, called an inverse of a such that

$$a*b = b*a = e$$

$\forall a,b \in G$.

Note:- If a group has the property that $a*b = b*a$, i.e. Commutative law holds then the group is called an abelian.

* Properties of group:-

The following theorms can understand the elementary features of groups

Theorem 1

① → In a group G there is only identity element

Proof: Let e and e' are two identity in G and let $a \in G$.

$\therefore ae = a$ — ①

$ae' = a$ → ②

R.H.S of ① and ② are equal $\Rightarrow ae = ae'$

Thus by the left cancellation law, we obtain $e = e'$

There are only one identity element in for $a \in G$. Hence theorm is proved.

② for each element 'a' in a group G. there is a unique element b in G such that.

$ab = ba = e$ (uniqueness of inverse).

Proof:- Let b and c are both inverses of $a \in G$.

Then $ab = e$ and $ac = e$

$\therefore c = ce$ (existence of identity element)

$\rightarrow c = e(ab)$ $\{\because ab = e\}$

$c = (ca)b$

$\therefore c = (ac)b$ $\{\because ac = ca\}$

$c = eb$

$c = b$ $\{\because b = eb\}$

Hence inverse of a is unique

Theorem-2:-

① In a group G $(a^{-1})^{-1} = a$. $\forall a \in G$.

Proof:- We have $= aa^{-1} = a^{-1}a = e$

where e is the identity element of G.
Thus a is inverse of $a^{-1} \in G$.

$= (a^{-1})^{-1} = a$. $\forall a \in G$.

② In a Group G $(a \cdot b^{-1}) = b^{-1}a^{-1}$
$\forall a, b \in G$.

Proof:- By associatively we have.

$(b^{-1}a^{-1})ab = b^{-1}(a^{-1}a)b$
$\rightarrow (b^{-1}a^{-1})ab = b^{-1}(e)b$ $\{a^{-1}a = e\}$
$\rightarrow (b^{-1}a^{-1})ab = b^{-1}b$ $\{eb = b\}$
$\rightarrow (b^{-1}a^{-1})ab = e$ $\{b^{-1}b = e\}$

Similarly:-

$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1}$
$(ab)(b^{-1}a^{-1}) = a(e)a^{-1}$
$(ab)(b^{-1}a^{-1}) = aa^{-1}$
$(ab)(b^{-1}a^{-1}) = e$

Thus $(b^{-1}a^{-1})ab = ab(b^{-1}a^{-1}) = e$

$\therefore b^{-1}a^{-1}$ is the inverse of ab
i.e $b^{-1}a^{-1} = ab^{-1}$

Theorem - 3.

On a group G, the left and right cancellation laws hold i.e

(i) $ab = ac$ implies $b = c$

(ii) $ba = ca$ implies $b = c$

Proof:- (i) Let $ab = ac$

Premultiplying a^{-1} on both side we get

$$a^{-1}(ab) = a^{-1}(ac)$$
$$(a^{-1}a)b = (a^{-1}a)c$$
$$eb = ec$$
$$b = c$$

Hence proved.

(ii) $ba = ca$ implies $b = c$

Post multiplying a^{-1} on both sides.

$$(ba)a^{-1} = (ca)a^{-1}$$
$$b(aa^{-1}) = c(aa^{-1})$$
$$be = ce$$
$$b = c$$

Hence proved.

* Finite and infinite groups:

A group $(G, *)$ is called a finite group if G is a finite set.

A group $(G, *)$ is called infinite group if G is an infinite set.

Example-1 The group $(I, +)$ is an infinite group as the set I of integers. is an infinite set.

Example-2 → The group $G = \{1, 2, 3, 4, 5, 6, 7, 8\}$ under multiplication modulo 8 is a finite group as the set G is a finite set.

* Order of group :-

The order of group G is the number of elements in the group G. It is denoted by $|G|$. A group of order 1 has only the identity element i.e. $(\{e\}, *)$.

A group of order 2 has two elements i.e one identity element one one some other element.

Example :- Let $(\{e, x\}, *)$ be a group of order 2. The table operation is shown is

*	e	x
e	e	x
x	x	e

The group of order 3 has three elements i.e one identity element and two other elements.

* Subgroup:-

If a non void subset H of a group G is itself a group under the operation of G we say H is a subgroup of G.

Theorm :- A subset H of a group G is a subgroup of G iff

- The identity element $a \in H$.
- H is closed under the operation G i.e. if $a, b \in H$. then $a, b \in H$.
- H is closed under inverse, that is if $a \in H$ then $a^{-1} \in H$.

* Cyclic Subgroup:-

A subgroup K of a group G is said to be cyclic subgroup if there exists an element $x \in G$ such that every element of K can be written in the form of x^n for some $n \in Z$.

The element x is called generator of K and we write $K = \langle x \rangle$.

* Cyclic group:-

In case when $G = X$, we say G is cyclic and X is a generator of G. that is a group G is said to be cyclic if there is an element $x \in G$ such that every element of G can be written in the form x^n for some $n \in Z$

Example:-

The group $G = (1, -1, i, -i)$ under usual multiplication is a finite cyclic group with i as generator, since.

$$i^1 = i,\ i^2 = -1,\ i^3 = -i,\ i^4 = 1$$

Abelian group:-

Let us consider an algebraic system $(G, *)$, where $*$ is a binary operation of G. Then the system $(G, *)$ is said to be an abelian group if it satisfies all the properties of the group plus a additional following property.

(1) The operation $*$ is commutative i.e.

$$a * b = b * a,$$
$$\forall\ a, b \in G.$$

Example:- Consider an algebraic system $(G, *)$ where G is the set of all non-zero real numbers and $*$ is a binary operation defined by

$$a * b = \frac{ab}{4}$$

show that $(G, *)$ is an abelian group.

Solution:-

Closure property:-

- The set G is closed

under the operation * since $a*b = \frac{ab}{2}$ is a real number. Hence it belongs to G.

(ii) Associative property:

The operation * is associative

Let $a, b, c \in G$ then we have,

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

$$= \frac{(ab)c}{16} = \frac{abc}{16}$$

Similarly:

$$a*(b*c) = a*\left(\frac{bc}{4}\right)$$

$$\frac{a(bc)}{16} = \frac{abc}{16}$$

(iii) Identity =

Let assume that e is a +ve real numbers - Then $e*a = a$ where $a \in G$.

$$\frac{ea}{4} = a \quad \text{or} \quad ea = 4$$

Similarly, $a*e = a$

$$\frac{ae}{4} = a \quad \text{or} \quad e = 4$$

Thus the identity element in G is 4.

(iv) Inverse: Let assume that $a \in G$, if $a^{-1} \in Q$ is an inverse of a.

then $a * a^{-1} = 4$

Therefore $\frac{a a^{-1}}{4} = 4$

or $a^{-1} = \frac{16}{a}$

Similarly:

$a^{-1} * a = 4$

therefore:-

$\frac{a^{-1} a}{4} = 4$ or $a^{-1} = \frac{16}{a}$

The inverse of element a in $G = \frac{16}{a}$

(3) Commutative:- The operation * on G is commutative

Since $a * b = \frac{ab}{4} = b * a$.

Thus the algebraic system $(G, *)$ is closed associative, identity, inverse and commutative.

Hence the system $(G, *)$ is an abelian group.

* Product of groups:-

Theorem:-

Prove that if $(G_1, *_1)$ and $(G_2, *_2)$ are groups, then $G = G_1 \times G_2$ i.e. $(G, *)$ is a group with operation defined by $(a_1, b_1) * (a_2, b_2) = (a_1 *_1 a_2, b_1 *_2 b_2)$

Proof:-

To prove that $G_1 \times G_2$ is a group, we have to show that $G_1 \times G_2$ has the associativity operator, has one identity and also exist inverse of every element.

Associativity:

Let $a, b, c \in G_1 \times G_2$ then.

$$a*(b*c) = (a_1, a_2) * ((b_1, b_2) * (c_1, c_2))$$

$$(a_1, a_2) * (b_1 *_1 c_1, b_2 *_2 c_2)$$

$$(a_1 *_1 (b_1 *_1 c_1), a_2 *_2 (b_2 *_2 c_2))$$

$$((a_1 *_1 b_1) *_1 c_1), (a_2 *_2 b_2) *_2 c_2))$$

$$(a_1 *_1 b_1, a_2 *_2 b_2) * (c_1, c_2)$$

$$((a_1, a_2) * (b_1, b_2)) * (c_1, c_2)$$

$$(a*b)*c.$$

Identity:-

Let e_1 and e_2 are identities for G_1 and G_2 respectively. Then the identity for $G_1 \times G_2$ is $e = (e_1, e_2)$. Assume same $a \in G_1 \times G_2$

Then:- $a*e = (a_1, a_2) * (e_1, e_2)$

$$(a_1 *_1 e_1, a_2 *_2 e_2)$$

$$= (a_1, a_2) = a.$$

similarly, we have

$$e*a = a.$$

Inverse!- To determine the inverse of an element in $G_1 \times G_2$ we will determine it component wise i.e.

$$a^{-1} = (a_1, a_2)^{-1} = (a_1^{-1}, a_2^{-1})$$

Now to verify that this is the exact inverse we will compute $a * a^{-1}$ and $a^{-1} * a$.

$$a * a^{-1} = (a_1, a_2) * (a^{-1}, a_2^{-1})$$
$$= (a_1 *_1 a_1^{-1}, a_2 *_2 a_2^{-1})$$
$$= (e_1, e_2) = e.$$

Similarly we have

$$a^{-1} * a = e.$$

Thus $(G_1 \times G_2 *)$ is a group.

In general if $G_1, G_2, \ldots G_n$ are groups then $G = G_1 \times G_2 \times \ldots \times G_n$ is also a group.

* Cosets!- Let H be a subgroup of a group G.

A left coset of H in G is a subset of G whose element may be expressed as $xH = \{x * h / h \in H\}$ for any $x \in G$.

$\{xh / h \in H\}$

The element x is called a representation of the coset. Similarly a right coset of H in G is a subset that may be expressed as $Hx = \{hx / h \in H\}$ for any $x \in G$.

Thus complexes xH and Hx are called respectively a left and right coset.

If the group operation is additive (+) then a left coset is denoted as

$$x+H = \{x+h \mid h \in H\}$$

and a right coset is denoted by

$$H+x = \{h+x \mid h \in H\}.$$

* Normal subgroup:-

Let G be a group. A subgroup H of G is said to be a normal subgroup of G if for all $h \in H$ and $x \in G$

$$xhx^{-1} \in H.$$

If $xHx^{-1} = \{xhx^{-1} \mid h \in H\}$ then H is normal in G if and only if

$$xHx^{-1} \subseteq H, \quad \forall x \in G.$$

Statement:- If G is an abelian group then every subgroup H of G is normal in G.

Proof:- Let any $h \in H$, $x \in G$. Then,

$$xhx^{-1} = x(hx^{-1})$$
$$xhx^{-1} = (xx^{-1})h$$
$$xhx^{-1} = eh$$
$$xhx^{-1} = h \in H$$

Hence H is normal subgroup of G.

Subgroups:-

If $(G,\cdot)$ is a group $G' \subset G$, and $\cdot G'$ is also a group, then $(G',\cdot)$ is a subgroup of $(G,\cdot)$

If a non-void subset H of a group G is itself a group under the the operation of G we can say H is a subgroup of G.

Theorm:- A subset of H of a group G is a subgroup of G if:

- The identity element $a \in H$
- H is closed under the operation G i.e if $a, b \in H$, then $a, b \in G$.
- H is closed under inverse that is if $a \in H$ then $a^{-1} \in H$

Cyclic subgroup:- A subgroup K of a group G is said to be cyclic subgroup if there exists an element $X \in G$ such that every element of K can be written in the form of X^n for some $n \in Z$. The element X is called generator of K and we write $K = \langle X \rangle$

Matrix Representation:- It is the method to used by a computer language to store matrices of more than one dimension in memory.

An $m \times n$ order matrix is a set of numbers arranged in m (rows) and n (columns). Matrices of the same order can be added by the corresponding elements. Two matrices can be multiplied, the condition being that the number of columns of first matrix is equal to the no. of row of the second matrix

operation like row operation can be performed on a matrix using which we can obtain the inverse of a matrix. The inverse may be obtained by determining the adjoint as well. Now rows and columns are the different classes of matrices.

Symmetric Matrices: If the transpose of a matrix is equal to itself that matrix is said to be symmetric

$$A = A' = \begin{bmatrix} 1 & 2 \\ 2 & 3 \end{bmatrix}, \quad B = B' = \begin{bmatrix} 5 & 6 & 7 \\ 6 & 3 & 2 \\ 7 & 2 & 1 \end{bmatrix}$$

* each of these matrix satisfy the defining requirement of a symmetric matrix $A = A'$ and $B = B'$. ✓

Diagonalization of Matrices: If a square $n \times n$ matrix with non zero entries only along the diagonal from the under left to the lower right (the main diagonal)

Diagonal matrices are particularly convenient for eigenvalue* problems since the eigenvalues of a diagonal matrix.

$$A = \begin{bmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & a_{22} & & 1 \\ \vdots & \cdots & \ddots & 0 \\ 0 & \cdots & 0 & a_{nn} \end{bmatrix}$$

Coincide with the diagonal entries $\{a_{ii}\}$ and the eigenvectors corresponding the eigenvalue a_{ii} of just the i^{th} co-ordinate vector

* Special set of scales associated with the linear system of equations.

Number Theory :- It is a branch of pure mathmatics devoted to the study of the natural numbers and the integers. It is the study of the set of positive no. whole numbers which are usually called a set of positive numbers. As it holds the foundational place in the discipline. Numb or theory is also called "The Queen of Mathematics."

Divisibility :- suppose $a, b \in Z$ then we say that a divides b if b is the multiple of a

Theorm :-① show that $a/0$

proof → As $0 = a \times 0$

$0 = a+0$

$\Rightarrow a/0$ Hence proved.

Theorm ②: show that $1/a$ and $-1/a$.

proof :- $a = 1 \times a$ by defination

$\Rightarrow 1/a$

$a = -1 \times a$

$a = (-1) \times (a)$ by defination

$-1/a$

Theorm ③ :- If a/b, then show that a/bc

proof :- As $a/b \Rightarrow b = aC_1$ (by defination) —①

$C_1 \in Z$.

multiplying 'c' on both side of ①

$bc = a \times C_1 C$. $\because C_1 \in Z$

$C_1 C \in Z$

$bc = a \times aC_3$ —② $C_1 C = C_3 \in Z$

$\Rightarrow a/bc$ Hence proved.

Theorm-(4) → If $a|b$ and $b|a$ then show that $a = \pm b$

Proof:- $a|b \Rightarrow b = a \times c_1$ —(1) $c_1 \in Z$

Also $b|a \Rightarrow a = b \times c_2$ —(2) $c_2 \in Z$

using (1) in (2)

$a = ac_1 \times c_2$

$a = a c_1 c_2$

$1 = c_1 c_2$

$c_1 c_2 = 1$

This holds only if

$c_1 = \pm 1$ or $c_2 = \pm 1$

Put in (2) value of c

$a = b \times (\pm 1)$

$\boxed{a = \pm b}$ Hence proved.

∴ (1)(1) = 1
(-1)(-1) = 1

Theorm-(5) If $a|b$ and $b|c$ then show that $a|c$

As $a|b \Rightarrow b = a \times c_1$ —(1) $c_1 \in Z$

Also $b|c \Rightarrow c = b \times c_2$ —(2) $c_2 \in Z$

using (1) in (2)

$c_2 = ac_1 \times c_2$

$c_2 = a c_1 c_2$

$c_2 = a \times c_1 c_2$

$c_2 = a \times c_3$ —(3)

$\Rightarrow a|c$ proved.

∵ $c_1, c_2 \in Z$

$c_3 = c_1 c_2 \in Z$

Theorem:- If a/b and a/c then $a/bx+cy$ for any integer x and y.

If $a/b \Rightarrow b = aC_1 \rightarrow (1)$ $C_1 \in Z$

$a/c \Rightarrow c = aC_2 \rightarrow (2)$ $C_2 \in Z$

Now $bx+cy = (aC_1)x + (aC_2)y$

$= aC_1x + aC_2y \Rightarrow a(C_1x + C_2y)$

Since $C_1, C_2, x, y \in Z$

$\therefore C_1x + C_2y \in Z$

$bx+cy = aC_3$ → Hence proved. let $C_3 \in Z$

$\therefore a/bx+cy$

GCD:- Greatest Common Division:-

The largest positive integer that divides both a and b is called GCD of a and b. It is denoted by (a,b)

Example: $a = 24 = \{1, 2, 3, 4, 6, 8, 12, 24\}$ divisors

$b = 16 = \{1, 2, 4, 8, 16\}$

Common $= \{1, 2, 4, 8\}$

$a, (24, 16) = 8$

Prime number:- It is natural number $\{1, 2, 3 \ldots\}$ which are completely divisible by exactly 2 natural numbers (1, itself)

Example:- 1 is not prime number.

4 → Not

1 2 4

Eg 2, 3, 5, 7

Primality Testing:- It means the given positive integer, check is the number is prime or not. A prime ~~no~~ is a natural number greater than 1 that has no positive divisors other than 1 and itself.

It has three methods.

① Fermat little theorm :-

$(x^{p-1} \equiv 1 \pmod p)$

Example:- $x = 2, \; p = 19$

$x^{p-1} \bmod p \rightarrow (1) \rightarrow$ prime

$\neq 1 \rightarrow$ not prime.

$\therefore 2^{10} > 1$

$= 2^{18} \bmod 19$

$= \dfrac{2^5 \cdot 2^5 \cdot 2^5 \cdot 2^3}{\bmod 19}$

$= \dfrac{32 \cdot 32 \cdot 32 \cdot 8}{\bmod 19} = \dfrac{13 \cdot 13 \cdot 13 \cdot 8}{\bmod 19} = \dfrac{169 \cdot 10}{\bmod}$

$= \dfrac{17 \cdot 9}{\bmod 19} = \dfrac{153}{\bmod 19} = 1$

② Squar root test:- $x^2 \bmod n = ?$ Example $n = 8$?

$x =$ set of residules:-

$x = 1, 2, \ldots n-1$

$1, 2, 3, 4, 5, 6, 7$

$1^2 \bmod 8 = (1)$

$2^2 \bmod 8 = 4$

$3^2 \bmod 8 = (1)$

$4^2 \bmod 8 = 0$

$5^2 \bmod 8 = (1)$

$6^2 \bmod 8 = 4$

$7^2 \bmod 8 = (1)$

4 times ones but the no. of 1's is 2 times then number is prime.

1's $\rightarrow$ 2 times $\rightarrow$ not prime.

8 is not prime.

② $n = 6 \quad x = n-1$ ——

$1^2 \bmod 6 = 1$

$2^2 \bmod 6 = 4$

$3^2 \bmod 6 = 3$

$4^2 \bmod 6 = 0$

$5^2 \bmod 6 = 1$

$=$

from this formula this is fail

$6 =$ prime but we know this not prime.

Miller - Rabin Test :-

To find prime no. or not. ① Perform $n-1$ such that $n-1 = m \times 2^k$

* If $k \le 1$,
  Calculate T such that $T = a^m \bmod n$.
  If $(T = \pm 1)$, no. is prime, else composite

* If $k > 1$,
  Calculate T such that $T = T^2 \bmod n$
  If $(T = 1)$, no. is composite
  If $(T = -1)$, no. is prime.
  else, no. is composite.

Example :- $n = 27$, $a = 2$ prime or not
Find if $n = 27$ is a prime or not

Step-1 $n-1 = s.t. \ (n-1) = m \times 2^k$
$26 = 13 * 2^1 =$ $m = 13$, $k = 1$

Step-2 is following if $k \le 1$

$T = a^m \bmod n$
$= 2^{13} \bmod 27$
$= \frac{2^5 \cdot 2^5 \cdot 2^3}{\bmod 27} = \frac{5 \cdot 5 \cdot 8}{\bmod 27} = \frac{200}{\bmod 27}$
$= \frac{200}{\bmod 27} = 11$

$T \neq 11$, ± 1 $n = 27$ is composite. ✓

Congruence :- If is very useful tool for the study of divisibility

Definition :- If a and b are integers and $n > 0$, we write
$a \equiv b \bmod n$.
to mean $n \mid (b-a)$ we read this as "a is congruent to b modulo n"

For example:

$$29 \equiv 8 \bmod 7$$

$$60 \equiv 0 \bmod 15$$

The notation is used because the properties of the congruence are very similar to the property of equality "=".

Find out the values of a, b, n — follow these steps

① Find gcd(a, n) = d (let)

② b/d → if possible → sol. exist

③ Find d mod n → These no. of sol are possible.

④ Divide both the sides by d.

⑤ Multiply both the sides by multiplicative inverse of a

i.e. $(a \cdot a^{-1})x \equiv b \cdot a^{-1} \pmod n$

⑥ General solution equation is :-

$$\boxed{x_k = x_0 + k\left(\frac{n}{d}\right)}$$ where $k = \{0, 1, 2, \ldots (d-1)\}$

Example:- $14x \equiv 12 \pmod{18}$

$ax \equiv b \pmod n$ $\quad a = 14, b = 12, n = 18$

Step-1 = GCD(14, 18) → ② = ④

② b/d = $\frac{12}{2} = 6$ → Solution does exist

③ d mod n ⇒ 2 mod 18 = 2 → solution exists

④ to divide both side by d ⇒

$$\frac{14x}{2} \equiv \frac{12}{2} \pmod{\frac{18}{2}}$$

$$7x \equiv 6 \pmod 9$$

⑤ $7x \equiv 6 \bmod 9 \Rightarrow 7 \cdot 7^{-1}x \equiv 6 \cdot 7^{-1} \bmod 9$

$x \equiv 6 \cdot 7^{-1} \bmod 9$

$7^{-1} = 4$

$x \equiv 6 \cdot 4 \bmod 9$

$(7 \times 1) \bmod n = 1$
$(7 \times 1) \bmod 9 = 1$
$(k=1) \quad 7 \bmod 9 \neq 1$
$k=2 \quad 14 \bmod 9 \neq 1$

$= 24 \bmod 9$,

$\boxed{x_0 = 6}$,

(b) $x_k = x_0 + k\left(\frac{n}{d}\right)$

$x_1 \Rightarrow 6 + 1\left(\frac{18}{2}\right) \Rightarrow 6+9 = \boxed{15 = x_1}$ Ans

Chinese Remainder Theorem:-

It states that there always exists an "x" that satisfies the given congruence.

General form:-

$$x = a_1 \pmod{m_1}$$
$$x = a_2 \pmod{m_2}$$
$$\vdots$$
$$x = a_n \pmod{m_n}$$

Step-1 = Find out common modulus M.

$M = m_1 \times m_2 \times m_3 \times \cdots m_n$

Step-2 = Find : $M_1 = \frac{M}{m_1}$, $M_2 = \frac{M}{m_2}$ ---

Step-3 = Find out the inverse, m_1^{-1}, m_2^{-1}, -- m_n^{-1} with respect to $m_1, m_2, m_3 \cdots m_n$

Step-4 = $x = \left((a_1 * m_1 * m_1^{-1}) + (a_2 * m_2 * m_2^{-1}) + \cdots + (a_n * m_n * m_n^{-1})\right) \bmod M$.

Example:- $x \equiv 4 \pmod{11}$, $x \equiv 5 \pmod{7}$, $x \equiv 6 \pmod{13}$

$m_1 = 11$, $m_2 = 7$, $m_3 = 13$

$a_1 = 4$, $a_2 = 5$, $a_3 = 6$

Step-1 = $M = m_1 * m_2 * m_3$

$= 11 * 7 * 13 = 1001$

Step-2 = $M_1 = \frac{M}{m_1} = \frac{1001}{11} = 91$

$m_2 = \frac{1001}{7} = 143$, $m_3 = \frac{1001}{13} = 77$

Step-3 ⇒ $M_1^{-1} = 91^{-1} \pmod{11}$

$M_1^{-1} = \boxed{4}$

$M_2^{-1} = 143^{-1} \pmod 7 = \boxed{5}$

$M_3^{-1} = 77^{-1} \pmod{13} = \boxed{12}$

$(x * 91) \bmod 11 =$

$(4 * 91) \bmod 11 =$

Step-4 ⇒ $x = ((4 \cdot 91 \cdot 4) + (5 \cdot 143 \cdot 5) + (77 \cdot 6 \cdot 12)) \bmod$

$\boxed{x = 565}$ Ans

Verification = $565 \bmod 11 = 4$

$565 \bmod 7 = 5$

$565 \bmod 13 = 6$.

Fermat's theorem:- If n is prime and 'x' is a positive integer not divisible by n then

$\boxed{x^{n-1} \equiv 1 \bmod n}$

$\boxed{\phi(n) = n-1}$

Also -
x, n → coprime

n = prime no.
x = not divisible by n

eg:- $x = 3$, $n = 5$

$3^{5-1} = 3^4 = 81$

$\boxed{81 \equiv 1 \bmod 5}$ Solved

another form of fermat theorm:-

$$x^n \equiv x \bmod n$$

$x = 3$, $n = 5$ $\Rightarrow$ $x^n = 3^5$

$\Rightarrow 243 \equiv 3 \bmod 5$

Toitient function:-

Euler's ϕ

It is represented by $\phi(n)$ and may also be called Euler's phi function.

→ It defined as the no of +ve integers less than n that are coprime to n

$n \geq 1$

$\phi(5) = \{1, 2, 3, 4\}$

$\phi(6) = \{1, 5\}$

no. of elements in these sets is the toitient function

*Note:- Two integers a, b are said to be relatively prime, mutually prime or coprime if the only +ve integer factor that divided both of them is 1

Now when n → prime $\phi(n) = n-1$

eg = $\phi(5) = 4$

$\phi(23) = 23 - 1 = 22$

Also. $\phi(a*b) = \phi(a) * \phi(b)$ // a and b should be coprime ($GCD = 1$)

eg = $\phi(35) = \phi(7) * \phi(5)$

$6 * 4 = 24$

Euler's theorem:- It states that if x and n are coprime positive ## integers, then

gcd(a,n) = 1

$a^{\phi(n)} \equiv 1 \pmod n$

$x^{\phi(n)} \equiv 1 \bmod n$

$\phi(n)$ → toitient of n

Note:- It is generalized version of fermats theorem.

eg:- let $x = 11$, $n = 10$ both are coprime.

∴ we can represent them as.

$$11^{\phi(10)} \equiv 1 \bmod 10$$

$$11^4 \equiv 1 \bmod 10$$

$$\boxed{14641 \equiv 1 \bmod 10}$$ which is true

$$\phi(10) = \phi(2) * \phi(5)$$
$$= 1 * 4$$
$$= 4$$

*Note:- $x^{\phi(n) \cdot a} \equiv 1 \bmod n$

Like $11^{4*2} \equiv 1 \bmod 10$

$11^{40} \equiv 1 \bmod 10$.

i.e. any multiple of ϕ will give the same result.

Modular Arithmetic:- It is a system of arithmetic for integ where numbers "wrap around" when reaching a certain val called the modulus.

$\text{mod} = 7 \bmod 4 = 3.$

$-11 \bmod 7 = 3$

$7 - (11 \% 7) = 7 - 4$

$= 3.$

Congruent modulo:- Two integers a and b are said to be congruent modulo n.

if $(a \bmod n) = (b \bmod n)$

This is written as $= a \equiv (b \bmod n)$ or $b \equiv (a \bmod n)$

eg:- $73 \equiv 4 \pmod{23}$ means $73 \bmod 23 = 4 \bmod 23$.

Properties of Congruence:

(i) $a \equiv b \pmod{n}$ if $n \mid (a-b)$

(ii) $a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$

(iii) if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ then, $a \equiv c \pmod{n}$

* Modular arithmetic operations/properties.

① $(a+b) \bmod n \Rightarrow [(a \bmod n) + (b \bmod n)] \bmod n$

② $(a-b) \bmod n \Rightarrow [(a \bmod n) - (b \bmod n)] \bmod n$.

③ $(a*b) \bmod n \Rightarrow [(a \bmod n) * (b \bmod n)] \bmod n$.

OR

$x = (y*z) \bmod n$ then,

$x = (y \bmod n * z \bmod n) \bmod n$

① eg:- $(6+8) \bmod 2 = (6 \bmod 2 + 8 \bmod 2) \bmod 2$

$14 \bmod 2 = (0+0) \bmod 2$

$0 = 0$.

③ eg:- Let a=11, b=15, n=8

$(a*b) \bmod n = (11 \times 15) \bmod n$

$= 165 \bmod 8 = 5$.

④ if $x \equiv y \bmod n$, $a \equiv b \bmod n$ then

$(x+a) \equiv (y+b) \bmod n$

eg:- $17 \equiv 4 \bmod 13$, $42 \equiv 3 \bmod 13$

$59 \equiv 7 \bmod 17$. which is true

⑤ if $x \equiv y \pmod n$ and $a \equiv b \bmod n$. then

$(x-a) \equiv (y-b) \bmod n$

$42 \equiv 3 \bmod 13$

$14 \equiv 1 \bmod 13$

$28 \equiv 2 \bmod 13$ true

Modular Exponentiation:-

It means calculating the remain when dividing by a positive number m (called modulus a positive ~~number~~ integer b (called the base) raised to e-th power (e is called exponent)

$x^a \pmod n$

Eg:-

$11^7 \bmod 13 = ?$

$11^1 = 11 \bmod 13 = 11$ or -2

$11^2 = 11^1 \times 11^1 = -2 \cdot -2 = 4 \bmod 11 = 4$

$11^3 = 11^2 \times 11^2 = 4 \times 4 = 16 \bmod 11 = 5$

$11^7 = 11^4 \times 11^2 \times 11^1 = 5 \cdot 4 \cdot -2 = -40 \bmod 11$

$= -7 \bmod 11$

$= 4$

② $7^{256} \bmod 13 =$

$7^1 \bmod 13 = 7 \bmod 13 = 7$ or -6

$7^2 = 7^1 \cdot 7^1 = -6 \cdot -6 = 36 \bmod 13 = 10 \bmod 13 = 10$ or -3

$7^4 = 7^2 \cdot 7^2 = -3 \cdot -3 = 9 \bmod 13 = 9$ or -4

$7^8 = 7^4 \cdot 7^4 = -4 \cdot -4 = 16 \bmod 13 = 3 \bmod 13 = 3$

$7^{16} = 7^8 \cdot 7^8 = 3 \cdot 3 = 9 \bmod 13 = 9$ or -4.