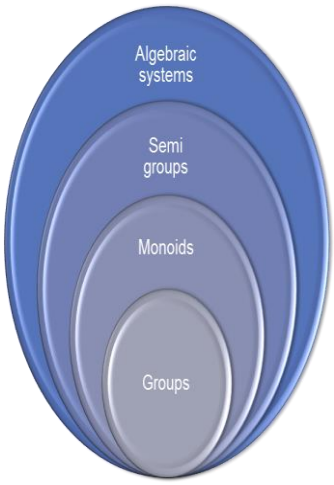
UNIT–I GROUPS AND RINGS

NOTES

Algebraic systems



Algebraic systems: A set 'A' with one or more binary(closed) operations defined on it is called an algebraic system.

Types of Algebraic systems

- Semi groups
- Monoids
- Groups
- Sub groups
- Normal Subgroups

NOTATIONS:

1. N = {1,2,3,4,…. ∞ } = Set of all natural numbers.
2. Z = { 0, ±1, ±2, ± 3, ± 4 , …∞} = Set of all integers.
3. Q = Set of all rational numbers.
4. R = Set of all real numbers.
5. C = Set of all complex numbers.

Binary Operation:

The binary operator * is said to be a binary operation (closed operation) on a non empty set A, if

$a * b \in A$ for all $a, b \in A$ (Closure property).

Semi Group: An algebraic system (A, *) is said to be a semi group if

1. * is closed operation on A.
2. * is an associative operation, for all a, b, c in A.

Ex. (N, +) is a semi group.
Ex. (N, .) is a semi group.
Ex. (N, –) is not a semi group.

Subsemigroup : Let (S, *) be a semigroup and let T be a subset of S. If T is closed under operation * , then (T, *) is called a subsemigroup of (S, *).

Ex: (N, .) is semigroup and T is set of multiples of positive integer m then (T,.) is a sub semigroup.

Monoid: An algebraic system (A, *) is said to be a monoid if the following conditions are satisfied.

1) * is a closed operation in A.
2) * is an associative operation in A.
3) There is an identity in A.

Ex. 'N' is a monoid with respect to multiplication.

Submonoid : Let (S, *) be a monoid with identity e, and let T be a non- empty subset of S. If T is closed under the operation * and e ∈ T, then (T, *) is called a submonoid of (S, *).

Group: An algebraic system (G, *) is said to be a group if the following conditions are satisfied.

1) * is a closed operation.
2) * is an associative operation.
3) There is an identity in G.
4) Every element in G has inverse in G.

Abelian group (Commutative group):

A group (G, *) is said to be abelian (or commutative) if a * b = b * a for all a, b in G.

1. Prove that if every element of the group is its own inverse, then G is abelian.

Solution:

If every element of the group is its own inverse, then $a^{-1} = a$ for all $a \in G$

$\Rightarrow (ab)^{-1} = ab \quad \forall a, b \in G$

$\Rightarrow b^{-1}a^{-1} = ab \quad \left(\because (ab)^{-1} = b^{-1}a^{-1} \right)$

$\Rightarrow ba = ab \quad \left(\because b^{-1} = b \text{ and } a^{-1} = a \right)$

Therefore G is abelian.

2. Prove that identity element in a group is unique.

Solution:

Let (G,*) be a group.

Let 'e_1' and 'e_2' be the identity elements in G

Suppose e_1 is the identity, then

$e_1 * e_2 = e_2 * e_1 = e_2$

Suppose e_2 is the identity, then

$e_1 * e_2 = e_2 * e_1 = e_1$

Therefore $e_1 = e_2$.

Hence identity element is unique.

3. Prove that a group is abelian if and only if $(ab)^{-1} = a^{-1}b^{-1} \; \forall a, b \in G$.

Solution:

By closure property $\forall a, b \in G \Rightarrow ab \in G$

$Let \; x = (ab)^{-1}, \; then \; x(ab) = e$

By associative property $\Rightarrow (xa)b = e$

post multiply by $b^{-1} \Rightarrow (xa)bb^{-1} = eb^{-1}$

$$(xa) = b^{-1}$$

post multiply by $a^{-1} \Rightarrow (xa)a^{-1} = b^{-1}a^{-1}$

$$\Rightarrow x = b^{-1}a^{-1}$$

Assume that G is an abelian group

$\therefore (ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}$ (G is Abelian)

Conversely assume that $(ab)^{-1} = a^{-1}b^{-1} \forall a, b \in G$

To Prove : G is abelian

$$ab = \left((ab)^{-1}\right)^{-1} = \left(a^{-1}b^{-1}\right)^{-1} = \left(b^{-1}\right)^{-1}\left(a^{-1}\right)^{-1} = ba.$$

Thus G is abelian.

4. Prove that if every element of the group is its own inverse, then G is abelian.

If every element of the group is its own inverse, then $a^{-1} = a$ for all $a \in G$

$\Rightarrow (ab)^{-1} = ab \quad \forall \; a, b \in G$

$\Rightarrow b^{-1}a^{-1} = ab \quad (\because (ab)^{-1} = b^{-1}a^{-1})$

$\Rightarrow ba = ab \quad (\because b^{-1} = b \text{ and } a^{-1} = a)$

Therefore G is abelian.

5. Give an example of semi group but not a Monoid.

Solution:

The set of all positive integers over addition form a semi-group but it is not a Monoid.

6. Let Z be the group of integers with the binary operation * defined by $a * b = a + b - 2$ for all $a, b \in Z$. Find the identity element of the group $\langle Z, * \rangle$

Solution:

$a = a * e = a + e - 2$

$a = a + e - 2 \Rightarrow e = 2$

7. Prove that $G = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\}$ forms an abelian group under matrix multiplication.

Solution:

Let $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $A = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$, $B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ and $C = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$

The matrix multiplication table is,

$\times$	I	A	B	C
I	I	A	B	C
A	A	I	C	B
B	B	C	I	A

C	C	B	A	I

Claim 1: Closure property

Since all the elements inside the table are the elements of G.

Hence G is closed under multiplication.

Claim 2: Associative property

We know that matrix multiplication is always associative

Claim 3: Identity property

From the above table we observe that the matrix $I \in G$ is the Identity matrix.

Claim 4: Inverse property

From the above table we observe that all the matrices are inverse to each other.

Hence Inverse element exists.

Claim 5: Commutative property

From the table we have

$$A \times B = C = B \times A,\ A \times C = B = C \times A,\ B \times C = A = C \times B$$

Therefore commutative property exists.

DISCRETE MATHEMATICS

Addition modulo m ($+_m$)

let m is a positive integer. For any two positive integers a and b

$a +_m b = a + b$, if $a + b < m$

$a +_m b = r$, if $a + b \geq m$ where r is the remainder obtained by dividing (a+b) with m

Multiplication modulo p ($\times_p$)

let p is a positive integer. For any two positive integers a and b

$a \times_p b = a\,b$, if $a\,b < p$

$a \times_p b = r$, if $a\,b \geq p$ where r is the remainder obtained by dividing (ab) with p.

Ex. $3 \times_5 4 = 2$, $5 \times_5 4 = 0$, $2 \times_5 2 = 4$.

1. Show that set G = {0,1,2,3,4,5} is a group with respect to addition modulo 6.

Solution:

The composition table of G is

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3

5	5	0	1	2	3	4

Closure property: Since all the entries of the composition table are the elements of the given set, the set G is closed under $+_6$.

Associativity: The binary operation $+_6$ is associative in G.

for ex. $(2 +_6 3) +_6 4 = 5 +_6 4 = 3$ and

$2 +_6 (3 +_6 4) = 2 +_6 1 = 3$

Identity : Here, The first row of the table coincides with the top row. The element heading that row , i.e., 0 is the identity element.

Inverse: From the composition table, we see that the inverse elements of 0, 1, 2, 3, 4. 5 are 0, 5, 4, 3, 2, 1 respectively.

Commutativity: The corresponding rows and columns of the table are identical. Therefore the binary operation $+_6$ is commutative.

Hence, $(G, +_6)$ is an abelian group.

Symmetry Group:

Let **F** be a set of points in $\mathbf{R}^n$. The symmetry group of **F** in $\mathbf{R}^n$ is the set of all isometries of that $\mathbf{R}^n$ carry **F** onto itself. The group operation is function composition.

Isometry:

An *isometry* of *n*-dimensional space $\mathbf{R}^n$ is a function from $\mathbf{R}^n$ onto $\mathbf{R}^n$ that preserves distance.

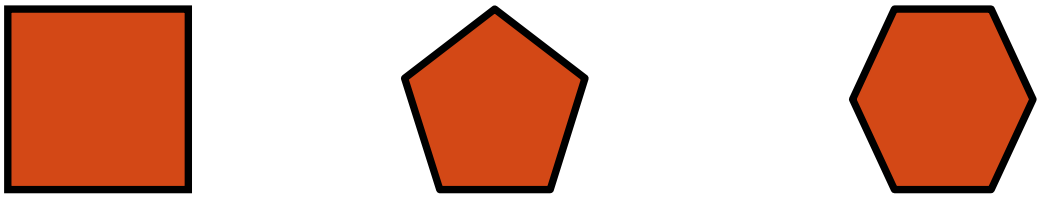
Note: More precisely, π is an isometry from $\mathbb{R}^n$ to $\mathbb{R}^n$ if for all $x, y \in \mathbb{R}^n$ we have

$$d(x,y) = d(\pi(x), \pi(y))$$

where d is a metric on $\mathbb{R}^n$.

Dihedral Groups

The symmetries of a regular n-gon form the dihedral group, $\langle D_n, \circ \rangle$, which consists of 2n permutations.



These groups are generated by the two fundamental permutations: rotations and reflections.

1. Let G be the set of all rigid motions of a equilateral triangle. Identify the elements of G. Show that it is a non-abelian group of order six.

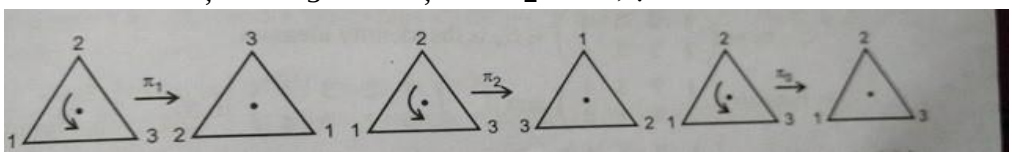
Proof:

Consider an equilateral triangle with vertices named as 1, 2, 3.

Let π_0, π_1 , π_2 denote the rotations of the triangle in the counter clockwise direction about an axis through the centre of the triangle and perpendicular to the plane of the triangle for an angle of 120°, 240°, 360° respectively.

These rotations are called rigid motions of the triangle and are given by

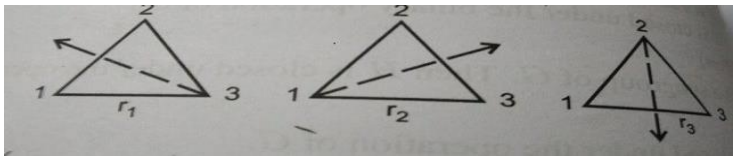
$$\pi_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \pi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$



Let r_1, r_2 , r_3 denote the reflections of the equilateral triangle along the lines joining vertices 3,1,2 and the mid-points of the opposite sides.

Each reflection is a 3-dimensional rigid motion.

$$r_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad r_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad r_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$



Let G = $\{\pi_0, \pi_1 , \pi_2, r_1, r_2 , r_3\}$.

Define binary operations on G as follows

$$\pi_1 r_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = r_3 \in G$$

Cayley's table for G is given by

	π_0	π_1	π_2	r_1	r_2	r_3
π_0	π_0	π_1	π_2	r_1	r_2	r_3
π_1	π_1	π_2	π_0	r_3	r_1	r_2
π_2	π_2	π_0	π_1	r_2	r_3	r_1
r_1	r_1	r_2	r_3	π_0	π_1	π_2
r_2	r_2	r_3	r_1	π_2	π_0	π_1
r_3	r_3	r_1	r_2	π_1	π_2	π_0

From the table it is clear that G is a group.

Note that $\pi_2 r_1 = r_2$ and $r_1 \pi_2 = r_3$

$\therefore \pi_2 r_1 \neq r_1 \pi_2$, G is not an abelian group of order six.

Subgroup :

Let G be a group and $\phi \neq H \subseteq G$. If H is a group under the same binary operation of G then H is a binary subgroup of G.

Example:

$H = \{0,2,4\}$ *or* $K = \{0,3\}$ are the proper subgroups of $(Z_6, +)$.

1. Prove that the necessary and sufficient condition for a non-empty subset H of a group (G, *) to be a subgroup is $a, b \in H \Rightarrow a * b^{-1} \in H$.

Solution:

Necessary Condition:

Let us assume that H is a subgroup of G. Since H itself a group, we have if $a, b \in H$ implies $a * b \in H$

Since $b \in H$ then $b^{-1} \in H$ which implies $a * b^{-1} \in H$

Sufficient Condition:

Let $a * b^{-1} \in H$, for $a * b \in H$

Claim 1: Identity property

If $a \in H$, which implies $a * a^{-1} = e \in H$

Hence the identity element $e \in H$.

Claim 2: Inverse property

Let $a, e \in H$, then $e * a^{-1} = a^{-1} \in H$

Hence a^{-1} is the inverse of a.

Claim 3: Closure property

Let $a, b^{-1} \in H$, then $a * \left(b^{-1}\right)^{-1} = a * b \in H$

Therefore H is closed.

Claim 4: Associative property

Clearly * is associative.

Hence H is a subgroup of G.

2. Prove that intersection of two subgroups of a group G is again a subgroup of G, but their union need not be a subgroup of G.

Solution:

Claim 1: Intersection of two subgroups is again a subgroup.

Let A and B be two subgroups of a group G. We need to prove that $A \cap B$ is a subgroup.

(i.e.) It is enough to prove that $A \cap B \neq \phi$ and $a, b \in A \cap B \Rightarrow a * b^{-1} \in A \cap B$.

Since A and B are subgroups of G, the identity element $e \in A$ and B.

$\therefore A \cap B \neq \phi$

Let

$a,b \in A \cap B \Rightarrow a,b \in A$ and $a,b \in B$

$\Rightarrow a * b^{-1} \in A$ and $a * b^{-1} \in B$

$\Rightarrow a * b^{-1} \in A \cap B$

Hence $A \cap B$ is a subgroup of G.

Claim 2: Union of two subgroups need not be a subgroup

Consider the following example,

Consider the group $(Z,+)$, where Z is the set of all integers and the operation + represents usual addition.

Let $A = 2Z = \{0, \pm 2, \pm 4, \pm 6, \ldots\}$ and $B = 3Z = \{0, \pm 3, \pm 6, \pm 9, \ldots\}$.

Here $(2Z,+)$ and $(3Z,+)$ are both subgroups of $(Z,+)$

Let $H = 2Z \cup 3Z = \{0, \pm 2, \pm 3, \pm 4, \pm 6, \ldots\}$

Note that $2, 3 \in H$, but $2+3 = 5 \notin H \Rightarrow 5 \notin 2Z \cup 3Z$

(i.e.) $2Z \cup 3Z$ is not closed under addition.

Therefore $2Z \cup 3Z$ is not a group

Therefore (H, +) is not a subgroup of (Z, +).

Cyclic group:

A group (G,*) is said to be cyclic if there exists an element $a \in G$ such that every element of G can be written as some power of 'a'.

$G = \{1, -1, i, -i\}$ is a cyclic group with generators $\langle i \rangle$ or $\langle -i \rangle$

1. Show that every cyclic group is abelian.

Let (G,*) be a cyclic group with 'a' as generator

$\therefore \forall x, y \in G \Rightarrow x = a^m, y = a^n \cdot x * y = a^m * a^n = a^{m+n} = a^{n+m} = y * x$.

2. Prove that the multiplicative group $Z_7^* = \{1, 2, 3, 4, 5, 6\}$ is cyclic and find its generator.

The element 3 is a cyclic generator since

$3^1 \bmod 7 = 3$

$3^2 \bmod 7 = 9 \bmod 7 = 2$

$3^3 \bmod 7 = (3^2 \cdot 3) \bmod 7 = (2 \cdot 3) \bmod 7 = 6 \bmod 7 = 6$

$3^4 \bmod 7 = (3^3 \cdot 3) \bmod 7 = (6 \cdot 3) \bmod 7 = 18 \bmod 7 = 4$

$3^5 \bmod 7 = (3^4 \cdot 3) \bmod 7 = (4 \cdot 3) \bmod 7 = 12 \bmod 7 = 5$

$3^6 \bmod 7 = (3^5 \cdot 3) \bmod 7 = (5 \cdot 3) \bmod 7 = 15 \bmod 7 = 1$

whereas the element 4 is not a generator but only generates a the cyclic subgroup {1, 2, 4} of Z_7^* since

$4^1 \bmod 7 = 4$

$4^2 \bmod 7 = 16 \bmod 7 = 2$

$4^3 \bmod 7 = (4^2 \cdot 4) \bmod 7 = (2 \cdot 4) \bmod 7 = 1$

Since every element of $Z_7^* = \{1, 2, 3, 4, 5, 6\}$ can be written in powers of 3, $Z_7^* = \{1, 2, 3, 4, 5, 6\}$ is a

cyclic group.

3. Prove that every subgroup of a cyclic group is cyclic.

Proof:

Let (G,*) be the cyclic group generated by an element $a \in G$ and let H be the subgroup of G.

Claim: H is cyclic

If H = G or {e} then trivially H is cyclic.

If not the elements of H are non-zero integral powers of a, Since if $a^r \in H$, its inverse $a^{-r} \in H$.

Let "m" be the smallest positive integer such that $a^m \in H$. **(1)**

Let a^n be any arbitrary element of H. Let q be the quotient and r be the remainder when n is divided by m.

Then $n = qm + r$ where $0 \leq r < m$. **(2)**

Now $a^n = a^{qm+r} = (a^m)^q . a^r$

$a^r = (a^m)^{-q} . a^n = a^{n-mq}$.

Since $a^m \in H$, $(a^m)^q \in H$ by closure property

$a^{mq} \in H$

$(a^{mq})^{-1} \in H$, by existence of inverse, as H is a subgroup

$a^{-mq} \in H$

Since $a^n \in H$ and $a^{-mq} \in H$

$a^{n-mq} \in H$

$\therefore a^r \in H$

By **(1) & (2),** we get r=0, $\therefore n=mq$

$$a^n = a^{mq} = \left(a^m\right)^q .$$

Thus every element of $a^n \in H$ is of the form $\left(a^m\right)^q$

Hence H is a cyclic subgroup generated by a^m.

4. Prove that every group of prime order is cyclic.

Proof:

Let O(G)=p, where p is a prime number.

Let $a(\neq e) \in G$.

Consider a subgroup generated by a.

Let $H = \langle a \rangle$

$\Rightarrow O(H) > 1$ [$\because H$ contains $a \Rightarrow H$ & also $e \Rightarrow H$ $O(H) > 1$]

Since H is a subgroup of G, then by Lagrange's theorem,

O(H)/O(G) $\Rightarrow$ O(H)/p

$\Rightarrow O(H) = 1 \text{ or } p$ [$\because$ *p is prime*]

But $O(H) > 1, \therefore O(H) \neq 1.$

Thus $O(H) = p = O(G)$

$\therefore G = H$

But H is a cyclic group, $\therefore$ G is a cyclic group.

COSETS:

If H is a sub group of(G, *) and a $\in$ G then the set

Ha = { h * a | h $\in$ H}is called a right coset of H in G.

Similarly aH = {a * h | h $\in$ H}is called a left coset of H is G.

Note: 1) Any two left (right) cosets of H in G are either identical or disjoint.

2) Let H be a sub group of G. Then the right cosets of H form a partition of G. i.e., the union of all right cosets of a sub group H is equal to G.

1. Let G = $(Z_{12}, +_{12})$, Find the left cosets of $H = \{[0],[4],[8]\}$ and show that the distinct left cosets of H forms a partition of G.

$Z_{12} = \{[0],[1],[2],[3],[4],[5],[6],[7],[8],[9],[10],[11]\}$; $H = \{[0],[4],[8]\}$

$[0]+H = \{[0],[4],[8]\} = H = [4]+H = [8]+H$

$[1]+H = \{[1],[5],[9]\} = [5]+H = [9]+H$

$[2]+H = \{[2],[6],[10]\} = [6]+H = [10]+H$

$[3]+H = \{[3],[7],[11]\} = [7]+H = [11]+H$

$\therefore G = H \cup ([1]+H) \cup ([2]+H) \cup ([3]+H)$

2. State and Prove Lagrange's theorem on finite groups *(or)* Prove that in a finite group, order of any subgroup divides the order of the group.
The order of each subgroup of a finite group is divides the order of the group.
Proof:

Let *G* be a finite group and $O(G) = n$ and let *H* be a subgroup of G and $O(H) = m$

Let $h_1, h_2, h_3, ..., h_m$ are the m distinct elements of *H*

For $x \in G$, the right coset of *H* is defined by $Hx = \{h_1 x, h_2 x, h_3 x, ... h_m x\}$.

Since there is a one to one correspondence between *H* and *Hx* , the members of *Hx* are distinct.

Hence, each right coset of *H* in *G* has *m* distinct members.

We know that any two right cosets of *H* in *G* are either identical or disjoint.

The number of distinct right cosets of H in G is finite (say k)

The union of these k distinct cosets of *H* in *G* is equal to *G*.

(i.e.) $G = Hx_1 \cup Hx_2 \cup Hx_3 \cup ... \cup Hx_k$

$O(G) = O(Hx_1) + O(Hx_2) + O(Hx_3) + ... + O(Hx_k)$

$n = m + m + m + ... + m$ (*k* times)

$$\frac{O(G)}{O(H)} = k$$

Hence $O(H)$ divides $O(G)$

3. **Let G be a group subgroups H and K. If |G|=660, |K|=66 and K⊂H⊂G, what are the possible values of |H| ?**

O(K) < O(H) < O(G) and O(K) divides O(H) and O(H) divides O(G).

O(K) = |K| = 66 = 2·3·11.

O(G) = |G| = 660 = 2^2·3·5·11.

|K| divides |H| and |K| < |H|

⇒|H| = x |K| = x (2·3·11), with $x > 1$

|H| divides |G| and |H| < |G|

⇒|G| = y |H| = $y\,x$ (2.3.11), with $y > 1$

⇒660 = $y\,x$ (2.3.11)

2^2.3.5.11 = $y\,x$ (2.3.11)

2.5= $y\,x$,with $x > 1$, $y > 1$

⇒ x = 2 or x = 5

When $x = 2$ ⇒|H| = 2 (2.3.11) =132

When $x = 5$ ⇒|H| =5 (2.3.11) =330.

Normal Subgroup :

A subgroup (N, *) of a group (G, *) is said to be a normal subgroup of G, If for every g∈G and n∈N, $g * n * g^{-1} \in N$.

1. **Prove that intersection of any two normal subgroups of a group (G, *) is a normal subgroup of a group (G, *).**

Solution:

Let G be the group and H and K are the normal subgroups of G.

Since H and K are normal subgroups of

⇒ H and K are subgroups of G

⇒ $H \cap K$ is a subgroup of G.

Now we have to prove $H \cap K$ is normal

Since $e \in H$ and $e \in K \Rightarrow e \in H \cap K$.

Thus H∩K is nonempty.

Let $x \in G$ and $h \in H \cap K$

$x \in G$ and $h \in H$, $h \in K$

$x \in G$, $h \in H$ and $x \in G$, $h \in K$

So, $x * h * x^{-1} \in H$ and $x * h * x^{-1} \in K$

$\therefore x * h * x^{-1} \in H \cap K$

Thus $H \cap K$ is a Normal subgroup of G.

Quotient group or Factor group:

If (N, *) is a normal subgroup of (G, *) then the group (G/N,⊕) is called the quotient group or factor group of G by N or quotient group modulo N.

Group Homomorphism:

Let (G,*) and $(S, \square)$ be two groups. A mapping f: G → S is said to be a group homomorphism if for any a, b ∈G,

$$f(a*b) = f(a) \square f(b).$$

Example: Consider $f : (R^+, .) \to (R, \quad)$ where $f(x) = \log_{10}(x)$

for any a, b $\in R^+$, $f(a \cdot b) = \log_{10}(ab) = \log_{10}(a) + \log_{10}(b) = f(a) + f(b)$.

Therefore f(x) is a group homomorphism.

Group Isomorphism:

A group homomorphism 'f' is called group isomorphism, if 'f' is one-to-one and onto.

Kernel of homomorphism:

Let $(G, *) \to (G', \quad)$ be groups with e′ as the identity element of G′. Let f: G → G′ be a homomorphism. The kernel of f is the set of all elements of G which are mapped onto e′ and is denoted by **ker *f*.**

$Ker\, f = \{x \in G \mid f(x) = e'\}$

1. **Consider two groups G and G′ where G={Z, +} and G′={z^m/m=0,± 1,± 2 ,± 3,..., □ }. Let □ : $Z \to \{z^m / \text{m isaninteger}\}$ defined by□ □ m □ $= 2^m$ where m∈Z. Prove that □ is homomorphism.**

   □ $(m) = 2^m$ where $m \in Z$

   $\therefore$ □ $(m + r) = 2^{m+r} = 2^m \square 2^r =$ □ (m)□ □ (r)

   Hence □ is homomorphism.

2. **Let $f : (G, *) \to (G', \quad)$ be an isomorphism. If G is an abelian group then prove that G' is also an abelian group.**

   Let $a', b' \in G'$.

   Then there exists $a, b \in G$, such that $f(a) = a'$ & $f(b) = b'$

   $a' + b' = f(a) + f(b) = f(a * b) = f(b * a) = f(b) + f(a) = b' + a'$

   Hence G' is an abelian group.

3. Let f : G → H be a homomorphism from the group (G,∗) to the group (H, Δ). Prove that the kernel of f is a normal subgroup of G.

Proof:

Let K be the Kernel of the homomorphism g. That is $K = \{x \in G \mid g(x) = e'\}$ where e' the identity element of H. is

Let x, y ∈ K. Now

$$g(x * y^{-1}) = g(x)\,\Delta\, g(y^{-1}) = g(x)\,\Delta\left[g(y)\right]^{-1} = e'\,\Delta\,(e')^{-1} = e'\Delta\, e' = e'$$

$$x * y^{-1} \in K$$

Therefore K is a subgroup of G. Let

$x \in K, f \in G$

$$g(f * x * f^{-1}) = g(f) * g(x) * g(f^{-1}) = g(f)\, e' \left[\, g(f)\right]^{-1} = g(f)\left[g(f)\right]^{-1} = e'$$

$$\therefore \quad f * x * f^{-1} \in K$$

Thus K is a normal subgroup of G.

4. Let $(G, \square)$, (H,*) be groups with respective identities e_G , e_H .If f :G→H is a homomorphism, then show that

(a) $f(e_G) = e_H$

(b) $f(a^{-1}) = \left[\, f(a)\right]^{-1} \ \forall a \in G$

(c) $f(a^n) = \left[\, f(a)\right]^n \ \forall a \in G \text{ and all } n \in Z$

(d) f (S) is a subgroup of H for each subgroup S of G.

Proof:

(a) $e_H * f(e_G) = f(e_G) = f(e_G \square e_G) = f(e_G) * f(e_G)$

$\therefore e_H = f(e_G)$, by right cancellation law

(b) Let $a \in G$, since G is a group, $a^{-1} \in G$

Since G is a group, $a * a^{-1} = e_G$

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

$$f(a) \square f(a^{-1}) = e_H$$

Hence $f\left(a^{-1}\right)$ is the inverse of $f(a)$

i.e., $f(a^{-1}) = \left[\, f(a)\right]^{-1} \ \forall a \in G$

(c) $\forall a \in G \text{ and all } n \in Z$

Case(i): if n=0 then $a^n = a^0 = e$

$$f(a^0) = f(e_G) = e_H = \left[\, f(a)\right]^0$$

$$\Rightarrow f(a^n) = \left[\, f(a)\right]^n$$

Case(ii): if n is a positive integer then

$$a^n = a \square a \square a \square \qquad a \ (n \text{ times})$$

$$f(a^n) = f(a * a * a * \ldots \text{ (n times)} \ldots * a)$$
$$= f(a) * f(a) * f(a) * \ldots * f(a)$$
$$= [f(a)]^n$$

Case(iii): if n is a negative integer , then n=-r, r>0.

$$f(a^n) = f(a^{-r}) = f\left[(a^{-1})^r\right] = \left[f(a^{-1})\right]^r = [f(a)]^{-r} = [f(a)]^n$$

$\therefore f(a^n) = [f(a)]^n \ \forall a \in G \text{ and all } n \in Z$

(d) If S is a subgroup of G , then S $\neq \phi$, so f $(S) \neq \phi$. Let x,y $\in$ f(S).

Then x = f(a), y = f(b) for some a,b$\in$S. Since S is a subgroup of G, it follows that

$\therefore a * b \in S,$

$f(a) * f(b) = f(a * b) \in f(S)$

$\Rightarrow x * y \in f(S), \text{ so } f(S) \text{ is closed}$

Finally, $x^{-1} = [f(a)]^{-1} = f[a^{-1}]$

$a \in S \Rightarrow a^{-1} \in S \ \& \ f[a^{-1}] \in f(S)$

$x^{-1} \in f(S)$

$\therefore f$(S) is a subgroup of H for each subgroup S of G.

5. State and prove Fundamental Theorem of Group Homomorphism.

Statement :

Let (G, *) and (H, Δ) be two groups. Let $g : G \to H$ be a homomorphism with kernel K . Then G/K is isomorphic to H(g(G) $\subseteq$ H).

Proof:

Let $g : G \to H$ be a homomorphism from the group $(G,*)$ to the group (H,Δ)

Then K= ker(g) = $\{x \in G / g(x) = e^1\}$ is a normal sub-group of $(G,*)$

Also we know that the quotient set $\left(G/K, \otimes\right)$ is a group.

Define $\phi : G/K \to H$ is mapping from the group $\left(G/K, \otimes\right)$ to the group (H,Δ) given by

$\phi(Ka) = g(a), \quad \text{for any } a \in G.$

Type your text

Since if $Ka = Kb$

$\Rightarrow a * b^{-1} \in K$

$\Rightarrow g(a * b^{-1}) = e'$

$\Rightarrow g(a) \Delta g(b^{-1}) = e'$

$\Rightarrow g(a) \Delta g(b^{-1}) \Delta g(b) = e' \Delta g(b)$

$\Rightarrow g(a) \Delta e' = e' \Delta g(b)$

$\Rightarrow g(a) = g(b)$

$\Rightarrow \phi(Ka) = \phi(Kb)$

ϕ is well defined.

Claim: ϕ is homomorphism

Let $Ka, kb \in G$.

Now,

$$\begin{aligned}\phi(Ka \otimes Kb) &= \phi[K(a * b)] \\ &= g(a * b) \\ &= g(a) \Delta g(b) \\ &= \phi(Ka) \Delta \phi(Kb)\end{aligned}$$

$\therefore$ ϕ is a homomorphism

Claim: ϕ is one-to-one.

If $\phi(Ka) = \phi(Kb)$

then $g(a) = g(b)$

$\Rightarrow g(a) \Delta g(b^{-1}) = g(b) \Delta g(b^{-1})$

$g(a * b^{-1}) = g(b * b^{-1}) = g(e) = e'$

$\therefore a * b^{-1} \in k \Rightarrow Ka = Kb$

$\therefore \phi$ is one-to-one.

Claim: ϕ is onto.

Let y be any element of H.

Since $g : G \to H$ is homomorphism from G to H.

Therefore there exists an element $a \in G$ such that $g(a) = y$

$\therefore$ For every $a \in G$, $Ka \in G/K$

we get $\phi(Ka) = g(a)$ for all $g(a) = y \in H$

$\therefore \phi$ is onto.

$\therefore \phi : G/K \to H$ is an isomorphism $\quad G/K \cong H$

6. State and prove Cayley's theorem.

Statement :

Every finite group G of order n is isomorphic to a permutation group of degree n.

Proof:

Let O(G) be finite say n and $a \in$ G. Define f_a: G $\to$G as $f_a(x) = ax \ \forall x \in G$

To prove f_a is bijection

Consider $f_a(x) = f_a(y)$

$\Rightarrow ax = ay \Rightarrow x = y \Rightarrow f_a$ is one to one

For any $g \in G$, there exists an element a, $x \in G$ such that $g = ax = f_a(x)$

Thus for every image in G , there is a pre-image in G $\Rightarrow f_a$ is onto

Since G has n elements, f_a is just the permutation of n-symbols

Define G′ = $\{f_a / a \in G\}$

To prove G′ is a group under composition

(i) Closure property

$(f_a \circ f_b)(x) = f_a[f_b(x)]$

$= f_a(bx)$

$= abx = f_{ab}(x)$

Since $a, b \in G$, $ab \in G \Rightarrow f_{ab} \in G'$

Therefore it has the closure property.

(ii) Associative property:

$f_a \circ (f_b \circ f_c))(x) = f_a[(f_b \circ f_c)(x)]$

$= f_a[f_b(f_c(x))]$

$= f_a[f_b(cx)]$

$= f_a(bcx)$

= abcx

Thus $(f_a \circ f_b) \circ f_c = f_a \circ (f_b \circ f_c)$

Therefore it has the associative property.

(iii) Identity element:

Consider $(f_a \circ f_e)(x) = f_a[f_e(x)]$

$= f_a(ex) = f_a(x)$

$\Rightarrow f_e$ is the identity element

(iv) Inverse element:

$$(f_a \circ f_{a^{-1}})(x) = f_a[f_{a^{-1}}(x)]$$
$$= f_a(a^{-1}x)$$
$$= aa^{-1}x = ex = f_e(x)$$

$f_{a^{-1}}$ is the inverse of f_a

Thus (G′, °) is a group

Define $\varphi: G \to G'$ by $\varphi(a) = f_a$ for all $a \in G$.

(i) φ **is one to one**

Consider $\varphi(a) = \varphi(b)$

$\Rightarrow f_a = f_b$

$\Rightarrow f_a(x) = f_b(x)$

$\Rightarrow ax = bx$

$\Rightarrow a = b$

Thus φ is one to one

ii) φ **is onto**

For every $f_a \in G'$,

since f is onto, there exists $a \in G$

such that $\varphi(a) = f_a$

Thus φ is onto

(iii) φ **is a homomorphism**

$\varphi(a*b) = f_{a*b} = f_a \circ f_b$

$(f_a \circ f_b)(x) = f_a[f_b(x)]$

$= f_a(bx)$

$= abx = f_{a*b}(x)$

$= \varphi(a) \circ \varphi(b)$

Thus φ is a homomorphism

$\varphi \Rightarrow$ is a isomorphism between G and G′

$\Rightarrow G \cong G'$.

7. Show that $(M, \square)$ is an abelian group where $M = \{A, A^2, A^3, A^4\}$ with $A = \begin{bmatrix} 0 & 1 \\ - & \end{bmatrix}$ and $\square$ is the ordinary matrix multiplication. Further prove that $(M, \square)$ is isomorphic to the abelian group $(G, \square)$ where G={1, -1, *i*, -*i*} and $\square$ is the ordinary multiplication.

Solution:

$$A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix};\ A^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix};\ A^3 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix};\ A^4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

For all $1 \le m, n \le 4$, $A^m \cdot A^n = A^{m+n} = A^r$ where $1 < r < 4$ and $m + n \cong r \pmod 4$.

Thus **.** is a closure. Thus **.** is a closure operation. Since matrix multiplication is associative so is '.'.

$A^4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$ is the identity.

$$A^{-1} = \frac{1}{1}\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = A^3$$

$$\left(A^2\right)^{-1} = \frac{1}{1}\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = A^2$$

$$\left(A^3\right)^{-1} = \frac{1}{1}\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = A$$

$$\left(A^4\right)^{-1} = \frac{1}{1}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I = A^4$$

For all $1 \le m, n \le 4$, $A^m \cdot A^n = A^{m+n} = A^{n+m} = A^n \cdot A^m$, so '.' is commutative.

$\therefore (M, \square)$ is an abelian group **.**

Define f: M → G such that $f(A) = i,\ f(A^2) = -1 = i^2,\ f(A^3) = -i = i^3,\ f(A^4) = 1 = i^4$

$\therefore$ f is 1-1 and onto

Since $i^3 = -i = f(A^3) = f(A \cdot A^2) = f(A) f(A^2) = i \cdot i^2 = i^3 = -i$

Hence f is isomorphic from M to G.

RING:

An algebraic system $< R, +, \cdot >$ is called a ring if it satisfies the following properties

(i) $< R, + >$ is an abelian group

(ii) $< R, \cdot >$ is a semi group

(iii) R satisfies distributive law

Example: (Z,+, .), (R,+, .) and (C,+, .) are all rings.

Commutative ring:

A commutative ring is a ring R that satisfies $ab = ba$ for all $a, b \in R$ (it is commutative under multiplication). Note that rings are always commutative under addition.

Subring:

Let (R, +, ·) be a ring. A non – empty subset S of R is called a subring of R , if (S, +, ·) is a ring.

Example: The ring of rational numbers is a subring of the ring of real numbers.

1. Prove that the set R of numbers of the form $a + b\sqrt{2}$, where a and b are integers, is a ring with respect to ordinary addition and multiplication.

Proof:

1. Closure : Let $x_1 = a_1 + b_1\sqrt{2}$, $x_2 = a_2 + b_2\sqrt{2} \in R$ where $a_1, a_2, b_1, b_2 \in Z$

$$x_1 + x_2 = \left(a_1 + b_1\sqrt{2}\right) + \left(a_2 + b_2\sqrt{2}\right) = \left(a_1 + a_2\right) + \left(b_1 + b_2\right)\sqrt{2} \in R$$

$$\text{where} \left(a_1 + a_2\right) \& \left(b_1 + b_2\right) \in Z.$$

$\therefore$ R is closed under +.

2. Associative: Let $x_1 = a_1 + b_1\sqrt{2}$, $x_2 = a_2 + b_2\sqrt{2}$, $x_3 = a_3 + b_3\sqrt{2} \in R$ where $a_1, a_2, a_3, b_1, b_2, b_3 \in Z$

$$\left(x_1 + x_2\right) + x_3 = \left[\left(a_1 + b_1\sqrt{2}\right) + \left(a_2 + b_2\sqrt{2}\right)\right] + \left(a_3 + b_3\sqrt{2}\right)$$

$$= \left[\left(a_1 + a_2\right) + \left(b_1 + b_2\right)\sqrt{2}\right] + \left(a_3 + b_3\sqrt{2}\right)$$

$$= \left[\left(a_1 + a_2\right) + a_3\right] + \left[\left(b_1 + b_2\right) + b_3\right]\sqrt{2}$$

$$= \left[a_1 + \left(a_2 + a_3\right)\right] + \left[b_1 + \left(b_2 + b_3\right)\right]\sqrt{2}$$

$$= \left(a_1 + b_1\sqrt{2}\right) + \left[\left(a_2 + a_3\right) + \left(b_2 + b_3\right)\sqrt{2}\right]$$

$$= \left(a_1 + b_1\sqrt{2}\right) + \left[\left(a_2 + b_2\sqrt{2}\right) + \left(a_3 + b_3\sqrt{2}\right)\right] = x_1 + \left(x_2 + x_3\right)$$

3. Identity: $0 + 0\sqrt{2} \in R$

$$\left(a + b\sqrt{2}\right) + \left(0 + 0\sqrt{2}\right) = (a + 0) + (b + 0)\sqrt{2} = a + b\sqrt{2}$$

4. Inverse: $a + b\sqrt{2}, -a - b\sqrt{2} \in R$

$$\left(a+b\sqrt{2}\right)+\left(-a-b\sqrt{2}\right)=(a-a)+(b-b)\sqrt{2}=0+0\sqrt{2}$$

$(-a)+(-b)\sqrt{2}$ is the identity inverse of $a+b\sqrt{2}$

5. Commutative law:

$$x_1+x_2=\left(a_1+b_1\sqrt{2}\right)+\left(a_2+b_2\sqrt{2}\right)=\left(a_1+a_2\right)+\left(b_1+b_2\right)\sqrt{2}$$
$$=\left(a_2+a_1\right)+\left(b_2+b_1\right)\sqrt{2}$$
$$=\left(a_2+b_2\sqrt{2}\right)+\left(a_1+b_1\sqrt{2}\right)=x_2+x_1$$

Under Multiplication

6. Closure Axioms:

$$x_1x_2=\left(a_1+b_1\sqrt{2}\right).\left(a_2+b_2\sqrt{2}\right)=\left(a_1a_2+2b_1b_2\right)+\left(a_2b_1+a_1b_2\right)\sqrt{2}$$

$a_1a_2+2b_1b_2, a_1b_2+a_2b_1 \in Z$

$\therefore x_1x_2 \in R$

7. Associative:

$$\left(x_1\cdot x_2\right)\cdot x_3=\left[\left(a_1+b_1\sqrt{2}\right)\cdot\left(a_2+b_2\sqrt{2}\right)\right]\cdot\left(a_3+b_3\sqrt{2}\right)$$
$$=\left[\left(a_1a_2+2b_1b_2\right)+\left(a_2b_1+a_1b_2\right)\sqrt{2}\right]\cdot\left(a_3+b_3\sqrt{2}\right)$$
$$=\left[\left(a_1a_2+2b_1b_2\right)a_3+2\left(a_2b_1+a_1b_2\right)b_3\right]+\left[\left(a_1a_2+2b_1b_2\right)b_3+\left(a_2b_1+a_1b_2\right)a_3\right]\cdot$$
$$=x_1\cdot\left(x_2\cdot x_3\right)$$

8. Distributive Laws :

$$x_1\cdot\left(x_2+x_3\right)=\left(a_1+b_1\sqrt{2}\right)\cdot\left[\left(a_2+b_2\sqrt{2}\right)+\left(a_3+b_3\sqrt{2}\right)\right]$$
$$=\left(a_1+b_1\sqrt{2}\right)\cdot\left[\left(a_2+a_3\right)+\left(b_2+b_3\right)\sqrt{2}\right]$$
$$=\left[a_1\left(a_2+a_3\right)+2\left(b_2+b_3\right)b_1\right]+\left[b_1\left(a_2+a_3\right)+\left(b_2+b_3\right)a_1\right]\sqrt{2}$$
$$=\left(a_1+b_1\sqrt{2}\right)\cdot\left(a_2+b_2\sqrt{2}\right)+\left(a_1+b_1\sqrt{2}\right)\cdot\left(a_3+b_3\sqrt{2}\right)$$
$$=a_1a_2+a_1a_3+2b_1b_2+2b_1b_3+\sqrt{2}a_2b_1+\sqrt{2}a_3b_1+\sqrt{2}a_1b_2+\sqrt{2}a_1b_3$$
$$=\left[\left(a_1a_2+2b_1b_2\right)+\left(a_1b_2+a_2b_1\right)\sqrt{2}\right]+\left[\left(a_1a_3+2b_1b_3\right)+\left(a_1b_3+a_3b_1\right)\sqrt{2}\right]$$

$$x_1\cdot\left(x_2+x_3\right)=x_1\cdot x_2+x_1\cdot x_3$$

$$\left(x_2+x_3\right)\cdot x_1=x_2\cdot x_1+x_3\cdot x_1$$

Hence the given set is a ring.

2. Prove that the set $Z_4=\{0,1,2,3\}$ is a commutative ring with respect to the binary operation $+_4$ and $\times_4$.

Answer:

Composition table for additive modulo 4.

$+_4$	[0]	[1]	[2]	[3]
[0]	0	1	2	3
[1]	1	2	3	0
[2]	2	3	0	1
[3]	3	0	1	2

Composition table for multiplicative modulo 4.

$\times_4$	[0]	[1]	[2]	[3]
[0]	0	0	0	0
[1]	0	1	2	3
[2]	0	2	0	2
[3]	0	3	2	1

From tables, we get

(i) all the entries in both tables belongs to Z_4

Therefore Z_4 is closed under the both operations addition and multiplication.

(ii) From the both tables, entries in the first, second, third and fourth row is equal to entries in the first, second, third and fourth columns respectively.

Hence the operations are commutative.

(iii) Modular addition and Modular multiplications are always associative.

(iv) 0 is the additive identity and 1 is the multiplicative identity.

(v) Additive inverse of 0, 1, 2, 3 are respectively 0, 3, 2, 1. Multiplicative inverses of the non-zero elements 1, 2 and 3 are 1, 2 and 3 respectively.

(vi) If $a, b, c \in Z_4$ then

$$a\times(b+c)=(a\times b)+(a\times c)$$

$$(a+b)\times c=(a\times c)+(b\times c)$$

The operation multiplication is distributive over addition

Hence $(Z_4, +_4, \times_4)$ is a commutative ring with unity.

3. **Let** $A=\left\{\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} / a \in R\right\}$ **(a) Show that A is a ring under matrix addition and multiplication (b) Prove that R is isomorphic to A.**

Proof:

(a) For any $B=\begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix}$ and $C=\begin{bmatrix} c & 0 \\ 0 & c \end{bmatrix}$, we have

,

$$B + C = \begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix} + \begin{bmatrix} c & 0 \\ 0 & c \end{bmatrix} = \begin{bmatrix} b+c & 0 \\ 0 & b+c \end{bmatrix} \in A \text{ and}$$

$$B \cdot C = \begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix} \cdot \begin{bmatrix} c & 0 \\ 0 & c \end{bmatrix} = \begin{bmatrix} bc & 0 \\ 0 & bc \end{bmatrix} \in A$$

Also for any $B = \begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix}$, the additiveinverse $-B = \begin{bmatrix} -b & 0 \\ 0 & -b \end{bmatrix}$ exists such that

$$B + (-B) = \begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix} + \begin{bmatrix} -b & 0 \\ 0 & -b \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in A.$$

Distributive Laws:

$$A.(B+C) = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \cdot \left\{ \begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix} + \begin{bmatrix} c & 0 \\ 0 & c \end{bmatrix} \right\} = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \cdot \left\{ \begin{bmatrix} b+c & 0 \\ 0 & b+c \end{bmatrix} \right\}$$

$$A.(B+C) = \begin{bmatrix} a.(b+c) & 0 \\ 0 & a.(b+c) \end{bmatrix} = \begin{bmatrix} (a.b+a.c) & 0 \\ 0 & (a.b+a.c) \end{bmatrix}$$

$$= \begin{bmatrix} a.b & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} a.c & 0 \\ 0 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \cdot \begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix} + \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \cdot \begin{bmatrix} c & 0 \\ 0 & c \end{bmatrix} = A.B + A.C$$

Similarly, (B+C).A=B.A+C.A

Thus A is a ring.

(b) To prove isomorphism, consider a one-to-one and onto function f from R onto A defined as follows

For all $r \in R, f : R \to A$ where $f(r) = \begin{bmatrix} r & 0 \\ 0 & r \end{bmatrix}$ i.e., for any real number we associate a 2^{nd} order scalar matrix.

Now for any r, s ∈ R

$$f(r+s) = \begin{bmatrix} r+s & 0 \\ 0 & r+s \end{bmatrix} = \begin{bmatrix} r & 0 \\ 0 & r \end{bmatrix} + \begin{bmatrix} s & 0 \\ 0 & s \end{bmatrix} = f(r) + f(s)$$

$$f(r \cdot s) = \begin{bmatrix} rs & 0 \\ 0 & rs \end{bmatrix} = \begin{bmatrix} r & 0 \\ 0 & r \end{bmatrix} \cdot \begin{bmatrix} s & 0 \\ 0 & s \end{bmatrix} = f(r) \cdot f(s)$$

Thus two operations +, ·are preserved and f is 1 −1and onto.

∴ f is an isomorphism from R to A.

Integral domain:

A commutative ring R with a unit element is called an integral domain if R has no zero divisors.

Zero Divisors

A ring (R, +, ·) is said to be ring with zero divisors, if there exists non zero elements

a, b in R, such that ab=0.

Example:

$(\{0,1,2,3,4,5\}, +_6, \times_6)$ is a ring and $2 \times_6 3 = 0$. However $2 \neq 0$ & $3 \neq 0$.

2 and 3 are zero divisors of the ring

1. Show that a finite integral domain is a field

Proof:

Let {D, +, · } be a finite integral domain.

Then D has a finite number of distinct elements, say $\{a_1, a_2, a_3, \ldots a_n\}$.

Let a($\neq 0$) be any element of D.

Then the elements $a \cdot a_1, a \cdot a_2, a \cdot a_3, \ldots a \cdot a_n \in D$, since D is closed under multiplication.

The elements $a \cdot a_1, a \cdot a_2, a \cdot a_3, \ldots a \cdot a_n$ are distinct, because if $a \cdot a_i = a \cdot a_j \in D$, then $a \cdot (a_i - a_j) = 0$.

But $a \neq 0$. Hence $a_i - a_j = 0$, since D is an integral domain i.e., $a_i = a_j$, which is not true because $a_1, a_2, a_3, \ldots a_n$ are distinct elements of D.

Hence the sets $\{a \cdot a_1, a \cdot a_2, a \cdot a_3, \ldots a \cdot a_n\}$ and $\{a_1, a_2, a_3, \ldots a_n\}$ are the same. Since $a \in D$ is in both sets,

let $a \cdot a_k = a$, for some k —(1)

Then a_k is the unity of D, detailed as follows:

Let $a_j = a \cdot a_i$, $a_j \in D$ —(2)

Now $a_j \cdot a_k = a_k \cdot a_j$, by commutative property

$= a_k \cdot (a \cdot a_i)$, by(2)

$= (a_k \cdot a) \cdot a_i$

$= (a \cdot a_k) \cdot a_i$, by commutative property

$= a \cdot a_i$, by (1)

$= a_j$, by(2)

Since a_j is an arbitrary element of D, a_k is the unity of D

Let it be denoted by 1.

Since $1 \in D$, there exits a($\neq 0$) and $a_i \in D$ such that $a \cdot a_i = a_i \cdot a = 1$

$\therefore$ a has an inverse.

Hence {D, +, · } be a finite integral domain.

Field:

A commutative ring (F, +, ·) which has more than one element such that every nonzero element of F has a multiplicative inverse in F is called a field.

Example: (Q,+, .), (R,+, .) and (C,+, .) are all fields.

Note:

But (Z,+, .) is an integral domain and not a field.

1. Every field is an integral domain.

Proof:

Let (F, +, ·) be a field .

$\Rightarrow$ then it is a commutative ring with identity

To prove that F is an integral domain, it is enough to prove that it has no zero divisors.

Suppose a,b$\in$F with a.b=0 with a $\neq$ 0

Since a is a non zero element, its multiplicative inverse a^{-1} exists

$\therefore a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0$

$\Rightarrow (a^{-1} a) \cdot b = 0$

$\Rightarrow 1 \cdot b = 0$

$\Rightarrow b = 0$

Thus $a \cdot b = 0, a \neq 0 \Rightarrow b = 0$

$\therefore$ F has no zero divisors.

Hence F is an integral domain.

2. Prove that Z_n is a field if and only if n is a prime.

Proof:

We have $Z_n = \{[0],[1],[2], \ldots [n-1]\}$

We know $(Z_n, +, \cdot)$ is a commutative ring with identity $1 [\,.\,]$

Let n be a prime, and suppose that 0 < a < n then gcd (a , n)=1

$\therefore$ there exists integers s, t such that as + tn = 1 $\Rightarrow$ sa – 1= (- t) n

$\therefore$ sa-1 is divisible by n

$\Rightarrow$ $sa \equiv 1 (\mathrm{mod} n)$

$\Rightarrow$ $[s][a] = [1]$

$\therefore [s]$ is the multiplicative inverse of $[a]$.

Thus $[a]$ is a unit of $Z_{n,}$ which is consequently a field

Conversely, let Z_n be a field.

So Z_n is a commutative ring with identity and without zero divisions of zero.

To prove n is a prime.

if n is not a prime, then n= n_1 n_2, where 1 < n_1 ,n_2 <n. So $[n_1] \neq [0]$ and $[n_2] \neq [0]$

But $[n_1][n_2] = [n_1 n_2] = [n] = [0]$

$\therefore$ $[n_1], [n_2]$ are divisors of zero which contradicts the fact Z_n is a field.

Hence n is a prime.

Euclidean Algorithm:

The **Euclidean algorithm** is a way to find the greatest common divisor of two positive integers, a and b.

Suppose we want to compute gcd(27,33). First, we have to divide the bigger one by the smaller one.

Divide 33 by 27, quotient is 1 and remainder is 6.

So, 33=1×27+6

Thus gcd(33,27)=gcd(27,6). Repeating this (i.e., divide 27 by 6, quotient is 4 and remainder is 3)

So, 27=4×6+3

and we see gcd(27,6)=gcd(6,3). Finally divide 6 by 3, quotient is 2 and remainder is 0

so, $6=2\times3+0$
Since 6 is a perfect multiple of 3, gcd(6,3)=3, and thus we have found that gcd(33,27)=3.

1. Find $[100]^{-1}$ in Z_{1009}.

SOLUTION:

gcd(100, 1009)=1,

By Euclidean Algorithm,

1009 = 10 (100) + 9 ----------(1)

100 = 11 (9) + 1 ----------(2)

By (2) $\Rightarrow$ 1 = 100 – 11(9)

= 100 – 11 [1009– 10(100)] (by (1))

= 100 + 110 (100) – 11(1009)

= 111(100) – 11 (1009)

= (111) (100) (mod 1009)

$\therefore$ [1] = [111] [100] (mod 1009)

$\Rightarrow [100]^{-1}$ is [111] in Z_{1009}.

MOHAMED SATHAK A .J .COLLEGE OF ENGINEEING

MA8551 Algebra and Number Theory

Unit II – Finite Fields and Polynomials

Notes

Introduction

You have studied in school polynomials with integer coefficients, rational coefficients and real coefficients. A polynomial is an expression of the form $a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$, where n is a non-negative integer and $a_0, a_1, a_2, \dots, a_n$ are integers (rational or real numbers).

We know how to add two polynomials, subtract one polynomial from another and multiply two polynomials.

We shall now define polynomial with coefficients from a ring and this collection of all polynomials with respect to addition and multiplication is a ring.

Polynomials

Definition: Let $(R, +,)$ be a ring. An expression of the form

$$a_0 + a_1 x + a_2 x^2 + \quad + a_n x^n ,$$

where n is a non-negative integer and a_0 , a_1 , a_2 , , $a_n \in R$, is called a **polynomial over** R **in the indeterminate** x and it is denoted by $f(x)$ thus,

$$f(x) = a_0 + a_1 x + a_2 x^2 + \quad + a_r x^r + \quad + a_n x^n,$$

a_r is called the coefficient of x^r and $a_r x^r$ is a term of the polynomial $f(x)$.

Definition: Let $f(x) = a_0 + a_1 x + a_2 x^2 + \quad + a_n x^n$ over a ring R.

If $a_n \neq 0$, where 0 is the zero element of R, then a_n is called the **leading coefficient** of $f(x)$ and we say $f(x)$ is of degree n.

We write $\deg f(x) = n$ and a_0 is called the constant term of $f(x)$.

The set of all polynomials in x over R is denoted by $R[x]$.

Definition: Equal polynomials

Let $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$, and $g(x) = b_0 + b_1 x + b_2 x^2 + \ldots + b_n x^n$, be two polynomials in $R[x]$, then $f(x) = g(x)$ if $m = n,\ a_i = b_i\ \forall i = 0,1,2,3,\cdots,n.$

Definition: Zero polynomial

A polynomial in $R[x]$ with all coefficients zero is called the **zero polynomial** and is denoted by 0.

Zero polynomial has no degree.

That is, degree is not defined for zero polynomial.

Definition: Constant polynomial

A polynomial of the form $f(x) = a_0$, where a_0 is a constant is called a **constant polynomial.**

Degree of non-zero constant polynomial is zero.

Definition: Monic polynomial

A polynomial in which the leading coefficient is 1 (identity of R) is called a **monic polynomial.**

For example,

$a_0 + a_1 x + a_2 x^2 + a_3 x^3$ Is a monic polynomial of degree 3.

Definition: Addition and Multiplication of polynomials in $R[x]$.

Let $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n,$

and

$g(x) = b_0 + b_1 x + b_2 x^2 + \ldots + b_n x^n,$

Be two polynomials in $R[x]$.

Then $f(x) + g(x) = C_0 + C_1 x + C_2 x_2 + \cdots + C_s x_s$

Where $C_i = a_i + b_i\ \forall i.$

	And the product $f(x)\cdot g(x)=\left(a_0+a_1x+a_2x^2+\cdots+a_nx^n\right)\cdot\left(b_0+b_1x+b_2x^2+\cdots+b_mx^m\right)$ $=C_0+C_1x+C_2x^2+\cdots+C_rx^r+\cdots C_kx^k$ Where $C_0=a_0b_0$ $C_1=a_0b_1+a_1b_0$ $C_2=a_0b_2+a_1b_1+a_2b_0$ $\vdots$ $C_r=a_0b_r+a_1b_{r-1}+\cdots+a_rb_0$ **Note:** Though the definition of multiplication appear to be complicated, it is the familiar process of using distributive property and collecting like terms. For example consider $f(x)=2+3x+2x^2+x^3$ and $g(x)=1+x+2x^2$, in $Z[x]$ Then $f(x)+g(x)=(2+1)+(3+1)x+(2+2)x^2+(1+0)x^3$ $=3+4x+4x^2+x^3$ And $f(x)\cdot g(x)=\left(2+3x+2x^2+x^3\right)\cdot\left(1+x+2x^2\right)$ $=2\cdot1+(3\cdot1+2\cdot1)x+(2\cdot1+2\cdot2+3\cdot1)x^2+(1+2\cdot1+3\cdot2)x^3+(1+2\cdot2)x^4+1\cdot2x^5$ $=2+5x+9x^2+9x^3+5x^4+2x^5$
1	**Theorem:** Let R be a ring, then $(R[x],+,\bullet)$ is a ring.
	Proof: Given R is a ring. Let $f(x)$ and $g(x)\in R[x]$ Let $f(x)=a_0+a_1x+a_2x^2+\ldots+a_nx^n$,

and

$g(x) = b_0 + b_1 x + b_2 x^2 + \ldots + b_n x^n$,

Be two polynomials in $R[x]$.

Then $f(x) + g(x) = C_0 + C_1 x + C_2 x_2 + \cdots + C_s x_s$

Where $C_i = a_i + b_i \forall i$.

Since $a_i + b_i \in R$, $C_i \in R$.

$f(x) + g(x) \in R[x]$

And

$f(x) \cdot g(x) = C_0 + C_1 x + C_2 x_2 + \cdots + C_r x_r + \cdots C_k x_k$

Where

$C_r = a_0 b_r + a_1 b_{r-1} + a_2 b_{r-2} + \cdots + a_r b_0 \in R$.

$f(x) \cdot g(x) \in R[x]$

Since addition + and multiplication · are associative in R, addition and multiplication of polynomials are associative in $R[x]$.

The zero polynomial 0 in $R[x]$ is the identity for + in $R[x]$. Since

$f(x) + 0 = f(x) \quad \forall f(x) \in R[x]$

If $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$ in $R[x]$,

then $f(x), g(x), h(x) \in R[x]$ and let

$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$

$g(x) = b_0 + b_1 x + b_2 x^2 + \ldots + b_m x^m$

$h(x) = C_0 + C_1 x + C_2 x_2 + \cdots + C_p x_p$

Then the coefficient of x^i in the expansion of $(f(x)\, g(x))h(x)$ is the sum of the products of the form $(a_r b_s)\, c_t$, where r, s, t are non-negative integers such that $r + s + t = i$.

Again the coefficient of x^i in the expansion of $f(x)\big(g(x)h(x)\big)$ is sum of the products of the form $a_r(b_sc_t)$, where r,s,t are non-negative integers such that $r+s+t=i.$

Since multiplication is associative in R.

$a_r(b_sc_t)=(a_rb_s)c_t,$

Coefficient of x^i in $\big(f(x)\,g(x)\big)h(x)$ is equal to the coefficient of x^i in

$f(x)\big(g(x)\,h(x)\big)$

Multiplication of polynomials is associative.

$\big(f(x)\,g(x)\big)h(x)=f(x)\big(g(x)\,h(x)\big)$

Now $f(x)\big[g(x)+h(x)\big]=f(x)g(x)+f(x)h(x),$ since the coefficient of x^i in the $L.H.S$ is $a_r(b_s+c_t)$ and the coefficient of x_i in the $R.H.S$ is

$a_rb_s+a_rc_t=a_r(b_s+c_t).$

Hence $\big(R[x],+,\bullet\big)$ is a ring under polynomial addition and multiplication.

Note:

1. This ring $R[x]$ is called the ring of polynomials over R or the ring of polynomials with coefficients in R.
2. If R is commutative, then $R[x]$ is alsocommutative.

   For, if $f(x)=a_0+a_1x+a_2x^2+\ldots+a_nx^n$ and $g(x)=b_0+b_1x+b_2x^2+\ldots+b_mx^m$

   Then coefficient of x^r in $f(x)\,g(x)$ is

   $=a_0b_r+a_1b_{r-1}+a_2b_{r-2}+\cdots+a_rb_0$

   $=b_ra_0+b_{r-1}a_1+b_{r-2}a_2+\cdots+b_0a_r$ $\big[\because$ R is commuative$\big]$

   $=b_0a_r+b_1a_{r-1}+b_2a_{r-2}+\cdots+b_ra_0$

   = Coefficient of x^r in $g(x)\,f(x)$

   $f(x)\,g(x)=g(x)\,f(x)\;\forall\,f(x),g(x)\in R[x]$

	$\therefore R[x]$ is commutative. 3. If R is a ring with identity 1, then $R[x]$ is a ring with identity 1, Since $1 = 1 + 0x + 0x^2 + \cdots + 0x^t \in R[x]$ and $f(x)\cdot 1 = (a_0 + a_1 x + a_2 x + \cdots + a_n x^n)\cdot(1 + 0x + 0x^2 + \cdots + 0x^t)$ $= a_0 + a_1 x + a_2 x + \ldots + a_n x^n$ $= f(x)$ Thus 1 is the identity in $R[x]$.
2	**Theorem: prove that $R[x]$ is an integral domain iff R is an integral domain.**
	Proof: Let R be an integral domain. Then R is a commutative ring with identity and without zero divisors. Hence $R[x]$ is commutative ring with identity 1, since $f(x)\cdot 1 = f(x)$. We have to prove $R[x]$ is without zero divisors. To prove $f(x) \neq 0, g(x) \neq 0 \Rightarrow f(x)\, g(x) \neq 0$ Let $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$, $a \neq 0$ then $g(x) = b_0 + b_1 x + b_2 x^2 + \ldots + b_m x^m$, $b_m \neq 0$. Then $f(x)\cdot g(x) = c_0 + c_1 x + c_2 x^2 + \ldots + c_{n+m} x^{n+m}$, where $c_r = a_0 b_r + a_1 b_r + \ldots + a_r b_0$ and $c_{m+n} = a_n \cdot b_m$ Since R is without zero divisors $a_n \neq 0, b_m \neq 0 \Rightarrow a_n b_m \neq 0 \Rightarrow c_{n+m} \neq 0$ $\therefore f(x)\, g(x) \neq 0$ Hence $R[x]$ is an integral domain. Conversely, let $R[x]$ be an integral domain.

	We have to prove that R is an integral domain. We know R is a subring of $R[x]$. Therefore, R is an integral domain.
3	**Corollary: If F is a field, then $F[x]$ is an integral domain.**
	Proof: If F is a field, then F is an integral domain. $\therefore F[x]$ is an integral domain by above theorem. Note that if F is a field, the $F[x]$ is not a field. **Proof:** We know if F is a filed, then $F[x]$ is an integral domain by Corollary 1. Let $f(x) = x \in F[x]$. Suppose it has the multiplicative inverse $g(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$, then $xg(x) = 1$ $x(a_0 + a_1 x + \cdots + a_n x^n) = 1 + 0x + 0x^2 + \cdots$ $a_0 x + a_1 x^2 + \cdots + a_n x^{n+1} = 1 + 0x + 0x^2 + \cdots + 0x^{n+1}$ By definition of equality of polynomials, we find $1 = 0$ (equating constant terms). Which is a contradiction $\therefore f(x) = x$ has no multiplicative inverse. Hence, $F[x]$ is not a field.
4	**Theorem: If R is an integral domain, then $\deg(f(x) \cdot g(x)) = \deg f(x) + \deg g(x)$.**
	Proof: Let R be an integral domain. Then R is a commutative ring with identity and without zero divisions. *i.e.*, $a \neq 0, b \neq 0 \Rightarrow ab \neq 0$. Let $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$, $a_n \neq 0$ therefore $\deg f(x) = n$ and $g(x) = b_0 + b_1 x + b_2 x^2 + \ldots + b_m x^m$, $b_m \neq 0$ therefore $\deg g(x) = m$

Since R is an integral domain, $a_n \cdot b_m \neq 0$.

Now $f(x)g(x) = c_0 + c_1 x + c_2 x^2 + \ldots + c_{n+m} x^{n+m}$ where $c_{n+m} = a_n b_m \neq 0$

$\therefore \deg\left(f(x)\,g(x)\right) = n + m = \deg f(x) + \deg g(x)$

Note:

1. If R is a ring and $f(x)$ and $g(x)$ are non-zero polynomials then either

   $f(x) \cdot g(x) = 0$ or $\deg f(x)\,g(x) \leq \deg f(x) + \deg g(x)$.

   In the product, $f(x)g(x) = c_0 + c_1 x + c_2 x^2 + \ldots + c_s x^s$.

   If $c_i = 0\ \forall i$, then $f(x)\,g(x) = 0$

   Otherwise $f(x)\,g(x) \neq 0$

   If $a_n b_m = 0$, then $\deg f(x)g(x) < \deg f(x) + \deg g(x)$.

   If $a_n b_m \neq 0$, then $\deg f(x)g(x) = \deg f(x) + \deg g(x)$.

   $\therefore \deg f(x)\,g(x) \leq \deg f(x) + \deg g(x)$

2. $f(x) + g(x) = 0$ or $\deg\left(f(x) + g(x)\right) \leq \max\left\{\deg f(x), \deg g(x)\right\}$

Definition: Root of a polynomial

Let R be a ring with identity 1 and let

$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \in R[x]$

With $\deg f(x) \geq 1$.

An element $a \in R$ is called a root of $f(x)$ if

$f(a) = a_0 + a_1 a + a_2 a^2 + \ldots + a_n a^n = 0$

If $f(a) = 0$, then a is root of $f(x)$.

Note: If $R = (Z_6, +, \bullet)$, where $Z_6 = \{0,1,2,3,4,5\}$ by writing $[a]$ a s a.

A polynomial over Z_6 can be written differently.

$f(x) = 2x^3 + 5x^2 + 3x - 2$ over Z_6 is a polynomial

	Since $[4] = [-2]$, this polynomial $f(x)$ can also be written as $2x^3 + 5x^2 + 3x + 4$. What is its degree? Since $[2] \neq [0]$ or $2 \not\equiv 0 \pmod 6$, the leading coefficient of $f(x)$ is non zero. $\deg f(x) = 3$
5	**Example: What is the degree of the polynomial** $f(x) = 6x^3 + 5x^2 + 3x - 2$ **over** Z_6?
	Solution: Given $f(x) = 6x^3 + 5x^2 + 3x - 2$ Since the coefficients are from $Z_6 = \{0,1,2,3,4,5\}$ $6 \equiv 0 \pmod 6$ is $[6] = [0]$, $[4] = [-2]$ The polynomial is $0x^3 + 5x^2 + 3x + 4 = 5x^2 + 3x + 4$. So, the leading coefficient is $5 \neq 0$ in Z_6. Hence the $\deg f(x) = 2$.
6	**Example: Let** $f(x) = 4x^2 + 3$ **and** $g(x) = 2x + 5$ **be two polynomials over** Z_8. **Find the** $\deg f(x) \cdot g(x)$
	Solution: Given $f(x) = 4x^2 + 3$, $g(x) = 2x + 5$ are polynomials over Z_8. *i.e.*, $f(x), g(x) \in Z_8[x]$. The $\deg f(x) = 2$ and $\deg g(x) = 1$, since $4 \neq 0, 2 \neq 0$ in Z_8. Now, $f(x) \cdot g(x) = (4x^2 + 3)(2x + 5)$ $= 8x^3 + 20x^2 + 6x + 15$ Normally we expect degree of the product = sum of the degrees. Since the coefficients belong to Z_8, we find $8 \equiv 0 \pmod 8$ *i.e.*, $[8] = [0]$, $20 \equiv 4 \pmod 8$ and $15 \equiv 7 \pmod 8$ $\therefore f(x)\, g(x) = 4x^2 + 6x + 7$ over Z_8 $\therefore \deg f(x)\, g(x) = 2 < 3 = \deg f(x) + \deg g(x)$

7	**Example: Find the roots of the polynomial x^2-2 over the real numbers R.**
	Solution: Given polynomial is x^2-2 over R. To find the roots of x^2-2, we solve $x^2-2=0 \Rightarrow x^2=2 \Rightarrow x=\pm\sqrt{2}$. The roots are $\sqrt{2}, -\sqrt{2}$ in R. If we consider the polynomial x^2-2 over Q, then the roots $\sqrt{2}, -\sqrt{2}$ do not belong to Q. So, the polynomial $x^2-2 \in Q[x]$ had no roots in Q.
8	**Example: Find all the roots of $f(x)=x^2+4x$ in $Z_{12}[x]$.**
	Solution: Given $f(x)=x^2+4x$ in Z_{12} and $Z_{12}=\{0,1,2,3,4,5,6,7,8,9,10,11\}$ We verify and find the roots. Now $f(0)=0+0=0$ $\therefore 0$ is a root of $f(x)$ $f(1)=1+4=5\neq 0$ $\therefore 1$ is not a root $f(2)=2^2+4\cdot 2=4+8=12\equiv 0 \pmod{12}$ $\therefore 2$ is a root of $f(x)$ $f(3)=3^2+4\cdot 3=9+12=21\equiv 9 \pmod{12} \neq 0$ $\therefore 3$ is not a root of $f(x)$ $f(4)=4^2+4\cdot 4=16+16=32\equiv 8 \pmod{12} \neq 0$ $\therefore 4$ is not a root of $f(x)$ $f(5)=5^2+4\cdot 5=25+20=45\equiv 9 \pmod{12} \neq 0$ $\therefore 5$ is not a root of $f(x)$

	$f(6) = 6^2 + 4 \cdot 6 = 36 + 24 = 60 \equiv 0 \pmod{12}$ $\therefore$ 6 is a root of $f(x)$ $f(7) = 7^2 + 4 \cdot 7 = 49 + 28 = 77 \equiv 5 \pmod{12} \neq 0$ $\therefore$ 7 is not a root of $f(x)$ $f(8) = 8^2 + 4 \cdot 8 = 64 + 32 = 96 \equiv 0 \pmod{12}$ $\therefore$ 8 is a root of $f(x)$ $f(9) = 9^2 + 4 \cdot 9 = 81 + 36 = 117 \equiv 9 \pmod{12} \neq 0$ $\therefore$ 9 is not a root of $f(x)$ $f(10) = 10^2 + 4 \cdot 10 = 100 + 40 = 140 \equiv 8 \pmod{12} \neq 0$ $\therefore$ 10 is not a root of $f(x)$ $f(11) = 11^2 + 4 \cdot 11 = 121 + 44 = 165 \equiv 9 \pmod{12} \neq 0$ $\therefore$ 11 is not a root of $f(x)$ $\therefore$ $x = 0, 2, 6, 8$ are the roots of $f(x)$ over Z_{12}.
	Note: In your earlier classes you have seen that a polynomial of degree 2 had at most two roots, which is not true here for a polynomial over a ring.
9	**Example: Determine all the roots of** $f(x) = x^3 + 5x^2 + 2x + 6$ **over** $Z[x]$.
	Solution: Given $f(x) = x^3 + 5x^2 + 2x + 6$ over Z and $Z = \{0, 1, 2, 3, 4, 5, 6\}$. We verify and find the roots. Now $f(0) = 6 \equiv -1 \pmod{7} \neq 0$ $\therefore$ 0 is not a root of $f(x)$ $f(1) = 1 + 5 + 2 + 6 = 14 \equiv 0 \pmod{7}$ $\therefore$ 1 is a root of $f(x)$ $f(2) = 2^3 + 5 \cdot 2^2 + 2 \cdot 2 + 6 = 8 + 20 + 4 + 6 = 38 \equiv 3 \pmod{7} \neq 0$

	$\therefore$ 2 is not a root of $f(x)$ $f(3) = 3^3 + 5 \cdot 3^2 + 2 \cdot 3 + 6 = 27 + 45 + 6 + 6 = 84 \equiv 0 \pmod 7$ $\therefore$ 3 is a root of $f(x)$ $f(4) = 4^3 + 5 \cdot 4^2 + 2 \cdot 4 + 6 = 64 + 80 + 8 + 6 = 128 \equiv 2 \pmod 7 \neq 0$ $\therefore$ 4 is not a root of $f(x)$ $f(5) = 5^3 + 5 \cdot 5^2 + 2 \cdot 5 + 6 = 125 + 125 + 10 + 6 = 266 \equiv 0 \pmod 7$ $\therefore$ 5 is a root of $f(x)$ $f(6) = 6^3 + 5 \cdot 6^2 + 2 \cdot 6 + 6 = 216 + 180 + 12 + 6 = 434 \equiv 0 \pmod 7$ $\therefore$ 6 is a root of $f(x)$ Therefore the roots of $f(x)$ are 1, 3, 5, 6 in Z_7.
10	**Example: Determine all the roots of** $f(x) = x^2 + 3x + 2 \in Z_6[x]$.
	Solution: Given $f(x) = x^2 + 3x + 2 \in Z_6[x]$ and $Z_6 = \{0,1, 2, 3, 4, 5\}$. We verify and find the roots. Now $f(0) = 2 \neq 0$ $\therefore$ 0 is not a root of $f(x)$ $f(1) = 1^2 + 3 \cdot 1 + 2 = 1 + 3 + 2 = 6 \equiv 0 \pmod 6$ $\therefore$ 1 is a root of $f(x)$ $f(2) = 2^2 + 3 \cdot 2 + 2 = 4 + 6 + 2 = 12 \equiv 0 \pmod 6$ $\therefore$ 2 is a root of $f(x)$ $f(3) = 3^2 + 3 \cdot 3 + 2 = 9 + 9 + 2 = 20 \equiv 2 \pmod 6 \neq 0$ $\therefore$ 3 is not a root of $f(x)$ $f(4) = 4^2 + 3 \cdot 4 + 2 = 16 + 12 + 2 = 30 \equiv 0 \pmod 6$ $\therefore$ 4 is a root of $f(x)$

	$f(5) = 5^2 + 3 \cdot 5 + 2 = 25 + 15 + 2 = 42 \equiv 0 \pmod 6$ $\therefore 5$ is a root of $f(x)$ Therefore the roots of $f(x)$ are $1, 2, 4, 5$ in Z_6.
11	**Example: Determine all the polynomials of degree 2 in $Z_2[x]$.**
	Solution: We have to find all the polynomials of degree 2 over $Z_2 = \{0,1\}$ Let the general polynomial of degree 2 is $f(x) = a_0 + a_1 x + a_2 x^2, a_2 \neq 0$ The possible coefficients are from Z_2, where $a_2 \neq 0$, so $a_2 = 1$ $f(x) = a_0 + a_1 x + x^2$ If $a_0 = 0, a_1 = 1$ then $f(x) = x^2$ If $a_0 = 0, a_1 = 1$ then $f(x) = x + x^2$ If $a_0 = 1, a_1 = 0$ then $f(x) = 1 + x^2$ If $a_0 = 1, a_1 = 1$ then $f(x) = 1 + x + x^2$ Therefore, there are four possible polynomials of degree 2, $2, x^2, x + x^2, 1 + x^2, 1 + x + x^2 \in Z_2[x]$.
	Definition: Divisor of a polynomial Let F be a field and $f(x) \neq 0$ and $g(x)$ be polynomials in $F[x]$. $f(x)$ **is called a factor or a divisor of** $g(x)$ if there exists $h(x) \in F[x]$ such that $g(x) = f(x)\,h(x)$ We also say that $f(x)$ divides $g(x)$ or $g(x)$ is a multiple of $f(x)$. We have division algorithm for an integer a and positive integer n, $a = nq + r, 0 \leq r < n$ We are familiar with division of polynomials with real coefficients. For example, divide $g(x) = x^3 - 3x^2 + 4x + 5$ by $f(x) = x - 2$ The division is shown here

$$
\begin{array}{r}
x^2 - x + 2 \\
\hline
x-2 \;\big)\; x^3 - 3x^2 + 4x + 5 \\
x^3 - 2x^2 \\
\hline
-x^2 + 4x \\
-x^2 + 2x \\
\hline
2x + 5 \\
2x - 4 \\
\hline
9
\end{array}
$$

Here quotient $q(x) = x^2 - x + 2$ and the remainder $r(x) = 9$

$\therefore\ x^3 - 3x^2 + 4x + 5 = (x-2)(x^2 - x + 2) + 9$

$\Rightarrow g(x) = q(x)\, f(x) + r(x)$.

This division can be extended to polynomials over finite fields.

12 **Theorem: Division algorithm**

Let $f(x) \neq 0$ **and** $g(x)$ **be polynomials in** $F[x]$. **Then there exists unique polynomials** $q(x)$ **and** $r(x)$ **belonging to** $F[x]$ **such that**

$g(x) = q(x)\, f(x) + r(x)$

where

$r(x) = 0$ **or** $\deg r(x) < \deg f(x)$.

Proof: Given $f(x) \neq 0$ and $g(x) \in F[x]$

Consider the set $S = \{g(x) - t(x)\, f(x) \mid t(x) \in F[x]\}$

If $0 \in S$, then for some $t(x) \in F[x]$ we have

$g(x) - t(x)\, f(x) = 0$

$g(x) = t(x)\, f(x)$

Then $q(x) = t(x)$ and $r(x) = 0$, we have $g(x) = q(x)\, f(x) + r(x)$

If $0 \notin S$, then non-zero elements exists in S and among these elements in S, we can find an element $r(x)$ in S with least degree [by well ordering principle].

Since $r(x) \neq 0$, the result follows if

$\deg r(x) < \deg f(x)$

If not, let $\deg r(x) \geq \deg f(x)$

Let $r(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$, $a \neq 0$ and

$f(x) = b_0 + b_1 x + b_2 x^2 + \ldots + b_m x^m$, $b_m \neq 0$

$\therefore \quad n \geq m$

Define

$$h(x) = r(x) - a_n b_m^{-1} x^{n-m} f(x) \qquad \left[\because\ b_m \neq 0, b_m^{-1} \text{ exist in } F\right]$$

$$= a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n - a_n b_m^{-1} x^{n-m}\left(b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m\right)$$

$$= a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n - a_n b_m^{-1} b_0 x^{n-m} - a_n b_m^{-1} b_1 x^{n-m+1} - a_n b_m^{-1} b_2 x^{n-m+2} - \cdots - a_n b_m^{-1} b_m x^m$$

$\therefore \deg h(x) < n = \deg r(x)$

Since $r(x) \in S$, $r(x) = g(x) - q(x)\, r(x)$

$$h(x) = g(x) - q(x) f(x) - a_n b_m^{-1} x^{n-m} f(x)$$

$$= g(x) - \left[q(x) - a_n b_m^{-1} x^{n-m}\right] f(x)$$

$$= g(x) - p(x) f(x)$$

Where $p(x) = q(x) - a_n b_m^{-1} x^{n-m} \in F[x]$

$\therefore h(x) \in S$ and $\deg h(x) < \deg r(x)$

Which is contradiction to the fact that $\deg r(x)$ is minimum.

$\therefore \deg r(x) < \deg f(x) = n$

Where $r(x) = 0$ or $\deg r(x) < \deg f(x)$

	We now prove the uniqueness Suppose we also have $g(x) = q_1(x) f(x) + r_1(x)$ Where $r_1(x) = 0$ or $\deg r_1(x) < \deg f(x)$ Then $q(x) f(x) + r(x) = q_1(x) f(x) + r_1(x)$ $\left[q(x) - q_1(x)\right] f(x) = r_1(x) - r(x)$ If $q(x) - q_1(x) \neq 0$, then $\deg\left[q(x) - q_1(x)\right] f(x) \geq \deg f(x)$ $\Rightarrow \deg\left[r_1(x) - r(x)\right] \geq \deg f(x)$, which is a contradiction $\therefore q(x) - q_1(x) = 0 \Rightarrow q(x) = q_1(x)$ Then (3) $r_1(x) - r(x) = 0 \Rightarrow r_1(x) = r(x)$ Hence in the equation (1) $q(x)$ and $r(x)$ are unique.
	Note: The polynomials $q(x)$ and $r(x)$ in the division algorithm are called the **quotient** and **remainder** in the division of $g(x)$ by $f(x)$. When we consider polynomials over a filed F, we can find $q(x)$ and $r(x)$ by usual long division method, which you are used to do in school.
13	**Example: Consider** $f(x) = 3x^4 + x^3 + 2x^2 + 1$ **and** $g(x) = x^2 + 4x + 2$ **in** $Z_5[x]$. **Find** $q(x)$ **and** $r(x)$ **when** $f(x)$ **is divided by** $g(x)$.
	Solution: Given $f(x) = 3x^4 + x^3 + 2x^2 + 1$ and $g(x) = x^2 + 4x + 2$ Since Z_5 is a field, to find $f(x)$ and $r(x)$ when $f(x)$ is divided by $g(x)$, we perform long division, keeping in mind the addition and multiplication are performed modulo 5. $Z_5 = \{0, 1, 2, 3, 4\}$ is a field.

The division is shown here

$$
\begin{array}{r}
3x^2+4x \\
\hline
x^2+4x+2\,\big)\,3x^4+x^3+2x^2+0x+1 \\
3x^4+2x^3+x^2 \\
\hline
4x^3+x^2+0x+1 \\
4x^3+x^2+3x \\
\hline
2x+1
\end{array}
\qquad
\left[\begin{array}{l}
12\equiv 2\pmod 5 \\
6\equiv 1\pmod 5 \\
-1\equiv 4\pmod 5 \\
16\equiv 1\pmod 5 \\
8\equiv 3\pmod 5 \\
-3\equiv 2\pmod 5
\end{array}\right]
$$

Therefore, the quotient $q(x)=3x^2+4x$ and the remainder $r(x)=2x+1$

$\therefore\ 3x^4+x^3+2x^2+1=(x^2+4x+2)(3x^2+4x)+(2x+1)$

14

Example: If $f(x)=2x^4+5x^2+2$, $g(x)=6x^2+4$, **then determine** $q(x)$ **and** $r(x)$ **in** $Z_7[x]$, **when** $f(x)$ **is divided by** $g(x)$.

Solution: Given $f(x)=2x^4+5x^2+2$, and $g(x)=6x^2+4$,

Since $Z_7=\{0,1,2,3,4,5,6\}$ is a field, to find $f(x)$ and $r(x)$ when $f(x)$ is divided by $g(x)$, we use long division method keeping in mind addition and multiplication are done under modulo 7.

The division is shown here

$$
\begin{array}{r}
5x^2+1 \\
\hline
6x^2+0x+4\,\big)\,2x^4+0x^3+5x^2+0x+2 \\
2x^4+0x^3+6x^2 \\
\hline
6x^2+0x+2 \\
6x^2+0x+4 \\
\hline
5
\end{array}
\qquad
\left[\begin{array}{l}
30\equiv 2\pmod 7 \\
20\equiv 6\pmod 7 \\
-1\equiv 6\pmod 7 \\
-2\equiv 5\pmod 7
\end{array}\right]
$$

Therefore the quotient $q(x)=5x^2+1$ and the remainder $r(x)=5$

	$\therefore\ 2x^4+5x^2+2=\left(5x^2+1\right)\left(6x^2+4\right)+5$
15	**Example: If** $f(x)=3x^2+4x+2$ **and** $g(x)=6x^4+4x^3+5x^2+3x+1$, **are polynomials in** $Z_7[x]$, **then find** $q(x)$ **and** $r(x)$ **in when** $g(x)$ **is divided by** $f(x)$.
	Solution: Given $f(x)=3x^2+4x+2$ and $g(x)=6x^4+4x^3+5x^2+3x+1$, Since $Z_7=\{0,1,2,3,4,5,6\}$ is a field, to find $f(x)$ and $r(x)$ when $f(x)$ is divided by $g(x)$, we use long division method keeping in mind addition and multiplication are done under modulo 7. The division is shown here

$$
\begin{array}{r}
2x^2+x+6 \\
\hline
3x^2+4x+2\,\big)\,6x^4+4x^3+5x^2+3x+1 \\
6x^4+\ x^3+3x^2 \\
\hline
3x^3+\ x^2+3x \\
3x^3+4x^2+2x \\
\hline
4x^2+4x+1 \\
4x^2+4x+1 \\
\hline
5x+3
\end{array}
\qquad
\left[\begin{array}{l}
8\equiv 1\pmod 7 \\
-3\equiv 4\pmod 7 \\
8\equiv 4\pmod 7 \\
1 \\
24\equiv 3\pmod 7 \\
12\equiv 5\pmod 7 \\
-2\equiv 5\pmod 7 \\
-4\equiv 3\pmod 7
\end{array}\right]
$$

Therefore, the quotient $q(x)=2x^2+x+6$ and the remainder $r(x)=5x+3$

$\therefore\ 6x^4+4x^3+5x^2+3x+1=\left(2x^2+x+6\right)\left(3x^2+4x+2\right)+\left(5x+3\right)$

16	**Example: If** $f(x)=x^5+3x^4+x^3+x^2+2x+2\in Z_5[x]$ **is divided by** $(x-1)$, **find the quotient and remainder.**
	Solution: Given $f(x)=x^5+3x^4+x^3+x^2+2x+2$ and $g(x)=x-1$

	Since $Z_7 = \{0,1,2,3,4,5,6\}$ is a field, to find $f(x)$ and $r(x)$ when $f(x)$ is divided by $g(x)$, we use long division method keeping in mind addition and multiplication are done under modulo 7. The division is shown here

$$
\begin{array}{r}
x^4 + 4x^3 + x + 3 \\
\hline
x-1 \;\big)\; x^5 + 3x^4 + x^3 + x^2 + 2x + 2 \\
x^5 - x^4 \\
\hline
4x^4 + x^3 \\
4x^4 - 4x^3 \\
\hline
x^2 + 2x \\
x^2 - x \\
\hline
3x + 2 \\
3x - 3 \\
\hline
0
\end{array}
\qquad \left[5 \equiv 0 \pmod 5\right]
$$

Therefore, the quotient $q(x) = x^4 + 4x^3 + x + 3$ and the remainder $r(x) = 0$

$(x-1)$ is a factor of $f(x)$

$f(x) = (x^4 + 4x^3 + x + 3)(x-1)$

17	**Example:** $f(x) = x^3 + 5x^2 + 2x + 6 \in Z_7[x]$, **then write** $f(x)$ **as a product of first degree polynomials.**
	Solution: We know that $Z_7 = \{0,1,2,3,4,5,6\}$ Given $f(x) = x^3 + 5x^2 + 2x + 6$

	Now $f(0) = 6 \equiv -1 (\text{mod } 7) \neq 0$ $f(1) = 1 + 5 + 2 + 6 = 14 \equiv 0 \ (\text{mod } 7)$ $\therefore$ 1 is a root of $f(x)$ and so, $(x-1)$ is a factor of $f(x)$ $f(2) = 2^3 + 5 \times 2^2 + 2 \times 2 + 6 = 8 + 20 + 4 + 6 = 38 \equiv 3 \ (\text{mod } 7) \neq 0$ $\therefore$ 2 is not a root of $f(x)$ and so, $(x-1)$ is a factor of $f(x)$ $f(3) = 3^3 + 5 \times 3^2 + 2 \times 3 + 6 = 27 + 45 + 6 + 6 = 84 \equiv 0 (\text{mod } 7)$ $\therefore$ 3 is a root of $f(x)$ and so, $(x-1)$ is a factor of $f(x)$ $f(4) = 4^3 + 5 \times 4^2 + 2 \times 4 + 6 = 64 + 80 + 8 + 6 = 128 \equiv 2 \ (\text{mod } 7) \neq 0$ $\therefore$ 4 is not a root of $f(x)$ and so, $(x-1)$ is a factor of $f(x)$ $f(5) = 5^3 + 5 \times 5^2 + 2 \times 5 + 6 = 125 + 125 + 10 + 6 = 266 \equiv 0 (\text{mod } 7)$ $\therefore$ 5 is a root of $f(x)$ and so, $(x-1)$ is a factor of $f(x)$ $f(6) = 6^3 + 5 \times 6^2 + 2 \times 6 + 6 = 216 + 90 + 12 + 6 = 414 \equiv 1 (\text{mod } 7) \neq 0$ $\therefore$ 6 is not a root of $f(x)$ and so, $(x-1)$ is a factor of $f(x)$ $f(x) = (x-1)(x-3)(x-5)$ in $Z_7[x]$.
18	**Example: If** $f(x) = (2x^3 + 1)(5x^3 + 5x + 3)(4x - 3) \in Z_7[x]$, **then write** $f(x)$ **as a product of a unit and three monic polynomials.**

Solution:

Given $f(x)=(2x^3+1)(5x^3+5x+3)(4x-3)\in Z_7[x]$,

We have $Z_7=\{0,1,2,3,4,5,6\}$

To write $f(x)$ as product of three monic polynomials, we have to take out 2 from first factor, 5 from second factor and 4 from third factor.

2 from $2x^2+1$

5 from $5x^3+5x+2$

4 from $4x-3$

Now

$1\equiv 8\pmod 7$

$3\equiv 10\pmod 7$

$-3\equiv 4\pmod 7$

$f(x)=(2x^3+8)(5x^3+5x+10)(4x+4)$

$=2(x^2+4)5(x^3+x+2)4(x+1)$

$=40(x^2+4)(x^3+x+2)(x+1)$

$=5(x^2+4)(x^3+x+2)(x+1)$ $\quad[\because\ 40\equiv 5\pmod 7]$

Note: Instead of $-3\equiv 4\pmod 7$ in the 3rd factor.

	We may write $3 \equiv 24 \pmod 7$ Then we get $f(x) = 2(x^2+4)5(x^3+x+2)4(x-6)$ $= 40(x^2+4)(x^3+x+2)(x-6)$ $= 5(x^2+4)(x^3+x+2)(x-6)$
	As corollaries of the division algorithm, we get the remainder theorem and factor theorem.
19	**Corollary: The remainder theorem** **Let F be a field, $a \in F$ and $f(x) \in F[x]$. Then $f(a)$ is the remainder when $f(x)$ is divided by $(x-a)$.**
	Proof: Given $f(x) \in F[x]$ and $a \in F$ and so, $(x-a) \in F[x]$ By division algorithm, $f(x) = q(x)(x-a) + r(x)$ Where $r(x) = 0$ or $\deg r(x) < \deg(x-a) = 1$ $\therefore \deg r(x) = 0$ $\Rightarrow r(x) = r$ (a constant), an element is F. $f(x) = q(x)(x-a) + r$ Put $x = a$

	$f(a) = q(a) \cdot 0 + r = r \Rightarrow r = f(a)$ $f(x) = q(x)(x-a) + f(a)$ So, the remainder is $f(a)$.
20	**Corollary: Factor theorem** **Let F be a field, $a \in F$ and $f(x) \in F[x]$. Then a is a root of $f(x)$ if and only if $(x-a)$ is a factor of $f(x)$.**
	Proof: Given $f(x) \in F[x]$ and $a \in F$ $(x-a) \in F[x]$. if $(x-a)$ is a factor of $f(x)$, then $f(x) = (x-a)\,q(x)$ for some $q(x) \in F[x]$. $f(a) = (a-a)\,q(a) = 0 \cdot q(a) = 0$ Hence, a is a root of $f(x)$. Conversely, let $a \in F$ be a root of $f(x)$. $f(a) = 0$ By remainder theorem, above corollary there exists $q(x) \in F[x]$ such that $f(x) = (x-a)q(x) + f(a)$ $f(x) = (x-a)q(x)$

	$(x-a)$ is a factor of $f(x)$.
21	**Example: What is the remainder when** $f(x)=x^5+2x^3+x^2+2x+3 \in Z_5[x]$ **is divided by** $(x-1)$?
	Solution: Given $f(x)=x^5+2x^3+x^2+2x+3$. When $f(x)$ is divided by $(x-1)$, the remainder is $f(1)$. $f(1)=1+2+1+2+3=9\equiv 4 \pmod 5$ the remainder is 4 in Z_5.
22	**Example: What is the remainder when** $f(x)=2x^3+x^2+2x+3 \in Z_5[x]$ **is divided by** $(x-2)$?
	Solution: Given $f(x)=2x^3+x^2+2x+3$ and $Z_5=\{0,1,2,3,4\}$. When $f(x)$ is divided by $(x-2)$, the remainder is $f(2)$. $f(2)=2\cdot 2^3+2^2+2\cdot 2+3=27\equiv 2 \pmod 5$ the remainder is 2 in Z_5.
23	**Example: What is the remainder when** $f(x)=x^{100}+x^{90}+x^{80}+x^{50}+1$ **is divided by** $g(x)=x-1$ **is** $Z_2[x]$.
	Solution: Given $f(x)=x^{100}+x^{90}+x^{80}+x^{50}+1$ and $g(x)=x-1$ The remainder when $f(x)$ is divided by $g(x)$ is $f(1)$. $f(1)=1+1+1+1+1+1=6\equiv 0 \pmod 2$ Since the remainder is 0,

	$(x-1)$ is a factor of $f(x)$.
24	**Theorem: If $f(x) \in F[x]$ is of degree $n \geq 1$, then $f(x)$ has at most n roots if F.**
	Proof: Given $f(x) \in F[x]$ is of degree n where $n \geq 1$. We prove the theorem by induction on n. If $n = 1$, then $f(x) = ax + b, a, b \in F, a \neq 0$. Clearly $-\frac{b}{a}$ or $-a^{-1}b \in F$ and $f(-a^{-1}b) = a(-a^{-1}b) + b = -b + b = 0$. $\therefore f(x)$ has (at least) one root in F. If c_1, c_2 in F are two roots of $f(x)$, then $f(c_1) = 0 \Rightarrow ac_1 + b = 0$ And $f(c_2) = 0 \Rightarrow ac_2 + b = 0$ $ac_1 + b = ac_2 + b \Rightarrow ac_1 = ac_2$ Since F is a field, it is an integral domain and so cancellation laws hold. $ac_1 = ac_2 \Rightarrow c_1 = c_2$ Therefore there is exactly one root of F for $f(x) = ax + b, a \neq 0$

Now assume that the theorem is true for all polynomials of degree $k\,(\geq 1)$ in $F[x]$.

i.e., any polynomial of degree $k \geq 1$ has at most k roots in F.

consider a polynomial $f(x)$ of degree $k+1$.

if $f(x)$ has no roots in F, then the theorem is true.

Otherwise, let $r \in F$ be a root of $f(x)$.

$f(r)=0$

Therefore by factor theorem $f(x)=(x-r)\,g(x)$, where $g(x)$ is of degree k.

Hence by induction hypothesis, $g(x)$ has at the most k roots in F. and $r \in F$ is a root of $f(x)$.

Hence $f(x)$ has at most $k+1$ roots.

Hence by first principle of induction, the theorem is true for all $n \geq 1$.

Irreducible Polynomials

Let F be a field and $f(x) \in F[x]$ is of degree ≥ 2. We call $f(x)$ is reducible over F if there exist $g(x)$, $h(x) \in F[x]$ such that $f(x) = g(x)\,h(x)$, where deg $g(x) \geq 1$ and deg $h(x) \geq 1$. If $f(x)$ is not reducible, then we call it irreducible (or prime) over F.

In other words, $f(x)$ is irreducible over F if one of $g(x)$ or $h(x)$ is of degree 0 (or a non-zero constant).

25	**Test whether the polynomial $f(x) = 2x^2 + 4$ is irreducible over Z, Q, R and C.**
	Solution: Given $f(x) = 2x^2 + 4 = 2(x^2 + 2)$ Since 2 is constant polynomial in Z[x] whose degree is 0 and $x^2 + 2 \in$ Z[x]. Now $2x^2 + 4 = 0 \Rightarrow x^2 + 2 = 0 \Rightarrow x^2 = -2 \Rightarrow x = \pm i\sqrt{2}$ The roots do not belong to Z, Q and R. But $i\sqrt{2}$ and $-i\sqrt{2}$ belong to C. Hence $f(x) = 2x^2 + 4$ is reducible over C.
26	**Is $f(x) = x^2 + 1$ in $Z[x]$ irreducible over Z?**
	Solution: Given $f(x) = x^2 + 1$ in Z[x]. Now $x^2 + 1 = 0 \Rightarrow x^2 = -1 \Rightarrow x = \pm i$ $\therefore$ the roots $i, -i$ do not belong to Z. Hence $f(x) = x^2 + 1$ is irreducible over Z.
27	**Let $f(x) = x^3 + x^2 + x + 1 \in Z_2[x]$. Is it reducible or irreducible? If reducible find the other factor.**
	Solution: Given $f(x) = x^3 + x^2 + x + 1 \in Z_2[x]$ and $Z_2 = \{0, 1\}$ $f(0) = 0 + 0 + 0 + 1 = 1 \neq 0$ $\therefore$ 0 is not a root in Z_2. $f(1) = 1 + 1 + 1 + 1 = 4 \equiv 0 \pmod 2$ $\therefore$ 1 is a root in Z_2.

	Hence $(x-1)$ is a factor of $f(x)$ in $Z_2[x]$. $\therefore f(x)$ is reducible. $$\begin{array}{r} x^2+1 \\ \hline x-1\,\big)\, x^3+x^2+x+1 \\ x^3-x^2 \\ \hline x+1 \\ x-1 \\ \hline 0 \end{array}$$ $\therefore f(x) = (x^2+1)(x-1)$
28	**Test the polynomial $x^2 + x + 4 \in Z_{11}[x]$ is irreducible over Z_{11}.**
	Solution: Let $f(x) = x^2 + x + 4 \in Z_{11}[x]$ and $Z_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ is a field, since 11 is a prime. $f(x) = x^2 + x + 4$ is a polynomial of degree 2 in $Z_{11}[x]$. We search for an element $a \in Z_{11}$ such that $f(a) = 0$. We have $f(0) = 0 + 0 + 4 = 4 \neq 0 \pmod{11}$ $f(1) = 1 + 1 + 4 = 6 \equiv -5 \pmod{11} \neq 0$ $f(2) = 2^2 + 2 + 4 = 10 \equiv -1 \pmod{11} \neq 0$ $f(3) = 3^2 + 3 + 4 = 16 \equiv 5 \pmod{11} \neq 0$ $f(4) = 4^2 + 4 + 4 = 24 \equiv 2 \pmod{11} \neq 0$ $f(5) = 5^2 + 5 + 4 = 34 \equiv 1 \pmod{11} \neq 0$ $f(6) = 6^2 + 6 + 4 = 46 \equiv 2 \pmod{11} \neq 0$ $f(7) = 7^2 + 7 + 4 = 60 \equiv 5 \pmod{11} \neq 0$

	$f(8) = 8^2 + 8 + 4 = 76 \equiv 10 \pmod{11} \neq 0$ $f(9) = 9^2 + 9 + 4 = 94 \equiv 6 \pmod{11} \neq 0$ $f(10) = 10^2 + 10 + 4 = 114 \equiv 4 \pmod{11} \neq 0$ $\therefore$ there is no root in Z_{11}. Hence $f(x)$ is irreducible over Z_{11}.
29	**Find two non-zero polynomials $f(x)$ and $g(x)$ in $Z_{12}[x]$ such that $f(x)g(x) = 0$.**
	Solution: We know $Z_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ Consider $f(x) = 3x^2 \in Z_{12}[x]$ and $g(x) = 4x + 8 \in Z_{12}[x]$. We know $f(x)$ and $g(x)$ are non-zero polynomials. But $f(x)\ g(x) = 3x^2\,(4x + 8) = 12\ x^3 + 24x^2 = 0 + 0 = 0$ $f(x)\ g(x)$ is a zero polynomial in $Z_{12}[x]$.
30	**Find two non-zero polynomials $f(x)$, $g(x)$ in $Z_7[x]$ such that $f(x)g(x) \neq 0$.**
	Solution: We know $Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$. Let $f(x) = 2x^2 + 4x + 1$ and $g(x) = 6x^3$ be two non-zero polynomials in $Z_7[x]$. $f(x)g(x) = (2x^2 + 4x + 1)\ 6x^3$ $= 12x^5 + 24x^4 + 6x^3$ Since $12 \equiv 5 \pmod 7$ and $24 \equiv 3 \pmod 7$ $= 5x^5 + 3x^4 + 6x^3 \neq 0.$

31

Reducibility Test

Let F be a field and $f(x) \in F(x)$. Then

(i) If $f(x)$ is of degree 1, then $f(x)$ is irreducible.

(ii) If $f(x)$ is of degree 2 or 3, then $f(x)$ is reducible iff $f(x)$ has a root in F.

Proof:

(i) Let $f(x) = ax + b$, $a \neq 0$ in $F[x]$.

Suppose $f(x)$ is reducible, then there exist $g(x)$, $h(x) \in F[x]$ such that $f(x) = g(x)h(x)$, where $1 \leq \deg g(x) < \deg f(x)$ and $1 \leq \deg h(x) < \deg f(x)$

$\therefore ax + b = g(x)\ h(x)$

$\therefore \deg (ax + b) = \deg g(x) + \deg h(x)$

$\Rightarrow 1 = \deg g(x) + \deg h(x)$

This is impossible, since $\deg g(x) + \deg h(x) \geq 2$

$\therefore f(x)$ is irreducible over F.

(ii) Let $f(x) \in F[x]$ be of degree 2 or 3.

Suppose $f(x)$ is reducible over F, then $f(x) = g(x)\ h(x)$ for some $g(x)$, $h(x) \in F[x]$, where $1 \leq \deg g(x) < \deg f(x)$ and $1 \leq \deg h(x) < \deg f(x)$.

Since $\deg f(x) = \deg g(x) + \deg h(x)$ and $\deg f(x) = 2$ or 3, we have $\deg g(x) + \deg h(x) = 2$ or 3.

$\therefore$ at least one of $g(x)$ and $h(x)$ has degree 1.

Let $\deg g(x) = 1 \Rightarrow g(x) = ax + b$, $a \neq 0$.

Now $-a^{-1}b \in F$ and $g(-a^{-1}b) = a(-a^{-1}b) + b$

$= -(a\ .\ a^{-1})\ b + b$

$= -b + b = 0$

	$\therefore -a^{-1}b$ is a root of $g(x)$. Hence $-a^{-1}b$ is a root of $f(x)$ in F. So $f(x)$ has a root in F. Conversely, let $f(x)$ have a root $a \in F$. Then $(x-a)$ is a factor of $f(x)$. [By factor theorem] $f(x) = (x-a)\,g(x)$. Hence $f(x)$ is reducible over F.
	Greatest common divisor (g. c. d) Let F be a field and f(x), g(x) ∈ F[x]. A greatest common divisor (g. c. d) of f(x) and g(x) is a non-zero polynomial d(x) such that (i) d(x) divides f(x) and g(x) (ii) if c(x) is a divisor of f(x) and g(x), then c(x) divides d(x).
32	**Find the g. c. d of $x^4 + x^3 + 2x^2 + x + 1$ and $x^3 - 1$ over Q.**
	Solution: Let $f(x) = x^4 + x^3 + 2x^2 + x + 1$ and $g(x) = x^3 - 1$ and deg $g(x)$ < deg $f(x)$ Divide $f(x)$ by $g(x)$ by division algotithm successively. $x + 1$ $x^3 - 1 \overline{)\, x^4 + x^3 + 2x^2 + x + 1}$ $x^4 - x$ $x^3 + 2x^2 + 2x + 1$ $x^3 - 1$ $2x^2 + 2x + 2$ $\therefore f(x) = (x+1)(x^3-1) + (2x^2 + 2x + 2)$, deg$(2x^2 + 2x + 2)$ < deg$(x^3 - 1)$

$$
\begin{array}{r}
\frac{1}{2}x - \frac{1}{2} \\
2x^2 + 2x + 2 \;\overline{)\; x^3 - 1} \\
x^3 + x^2 + x \\
\hline
-x^2 - x - 1 \\
-x^2 - x - 1 \\
\hline
0
\end{array}
$$

$$x^3 - 1 = \left(\frac{x}{2} - \frac{1}{2}\right)\left(2x^2 + 2x + 2\right) + 0$$

$$= (x - 1)(x^2 + x + 1)$$

$\therefore$ The last non-zero remainder is $x^2 + x + 1$, which is the g.c.d

Characteristic of a Ring

Characteristic of a ring R is the least positive integer n such that na = 0 $\forall$ a $\in$ R and we write char(R) = n. If no such positive integer exists, then R is said to have characteristic 0.

For example,

1. The ring (Z3, +, •) has characteristic 3.

   In Z3 = {0, 1, 2}, $1 + 1 + 1 = 3(1) \equiv 0 \pmod 3$

   $2 + 2 + 2 = 3(2) \equiv 0 \pmod 3$

   $3(a) = 0 \;\forall\; a \in Z_3$.

   $\therefore$ Characteristic is 3. That is Char(Z_3) = 3.

   More generally, characteristic of the ring (Z_n, +, •) is n.

2. (Z, +, •) and (Q, +, •) are rings.

   For any a $\in$ Z (or Q), there is no positive integer n such that na = 0.

   $\therefore$ chat(Z) = 0 and char(Q) = 0

33	**Theorem: The characteristic of a field (F, +, •) is either 0 or a prime number.**
	Proof: Let (F, +, •) be a field. If char(F) = 0, then there is nothing to prove. If char(F) ≠ 0, then let char(F) = n. **To prove n is a prime.** Suppose n is not prime, then $n = pq$, where $1 < p < n$, $1 < q < n$. i.e., p and q are proper factors of n. Since char(F) = n, we have $na = 0 \ \forall \ a \in F$. Take $a = 1$, then $n \bullet 1 = 0$ (1 is identity of F) $\Rightarrow (pq) \bullet 1 = 0 \Rightarrow (p \bullet 1)(q \bullet 1) = 0$ $\left[\because (pq) \bullet 1 = \underbrace{1+1+1+\ldots+1}_{pq \text{ terms}} = \underbrace{(1+1+1+\ldots+1)}_{p \text{ terms}} \underbrace{(1+1+1+\ldots+1)}_{q \text{ terms}} \right]$ Since F is a filed, F is an integral domain and so, it has no divisor of zero. $\therefore$ either $p \cdot 1 = 0$ or $q \cdot 1 = 0$ Since p and q are less than n, it contradicts the definition of characteristic of F. $\therefore$ n is a prime number.

34	**Theorem: The number of elements of a finite field is P^n, wher P is a prime number and n is a positive integer.**
	Proof: We know for a prime p, Zp is a field having p elements and char(Zp) = p, since $pa = 0 \ \forall \ a \in Zp$. Consider the polynomial $f(x) = x^{p^n} - x$ in $Z_p[x]$. Now $f'(x) = p^n x^{p^n - 1} - 1$ Since char(Z_p) = p, char($Z_p[x]$) = p and $p\,g(x) = 0 \ \forall \ g(x) \in Z_p[x]$. Hence $p\,x^{p^n - 1} = 0 \Rightarrow p^n\, x^{p^n - 1} = 0$ $\therefore$ $f'(x) = -1$, a constant polynomial. Hence $f(x)$ and $f'(x)$ have no common root. Hence $f(x)$ has no multiple roots. $\therefore$ the roots of $f(x)$ are all distinct. If K is the smallest extendsion field containing all the roots of $f(x)$. i.e., K is the splitting field of $f(x)$. Then $f(x)$ has p^n distinct roots in K. In K, let F be the set of all elements satisfying $f(x)$. ie. F= $\left\{a \in K : a^{p^n} = a\right\}$ Hence F has only p^n elements. We now prove F is a field. Let $a, b \in F$. Then $a^{p^n} = a$ and $b^{p^n} = b$. $(ab)^{p^n} = a^{p^n} \cdot b^{p^n} = a \cdot b \in F$ $(a+b)^{p^n} = a^{p^n} + p^n C_1 a^{p^n - 1} b + p^n C_2 a^{p^n - 2} b^2 + \ldots + b^{p^n}$ Since char(K) = p, $p^n C_r\, a^{p^n - r} b^r = 0$, $r = 1, 2, 3\ldots$ $\therefore (a+b)^{p^n} = a^{p^n} + b^{p^n} = a + b \in F$ Similarly, $(a-b)^{p^n} = a - b \in F$

	$\therefore$ F is a subfield of K. Hence F is a field having p^n elements.
	Congruence Relation in F[x] Definition: Let $s(x) \in F[x]$ and $s(x) \neq 0$ and $f(x), g(x) \in F[x]$. We say that $f(x)$ is congruent to $g(x)$ modulo $s(x)$ and write $f(x) \equiv g(x) \pmod{s(x)}$ if $s(x)$ divides $f(x) - g(x)$. i.e., $f(x) - g(x) = q(x)\, s(x)$ for some $q(x) \in F[x]$.
	Definition: Ideal of a ring Let $(R, +, \bullet)$ be a ring. A non-empty subset I of a ring is called an ideal of R, if (i) for all $a, b \in I$, we have $a - b \in I$ (ii) for all $r \in R$ and $a \in I$, we have $ar, ra \in I$. Example: For any positive integer n, the subset $nZ = \{0, \pm n, \pm 2n, \dots\}$ is the ring $(Z, +, \bullet)$ is an ideal of Z. Note: An ideal is always a subring, but a subring is not an ideal. Ideal is something more than a subring. For example, $(Z, +, \bullet)$ is a subring of $(Q, +, \bullet)$, but is not an ideal, because if we take $2 \in Z$ and $\frac{1}{3} \in Q$, then $\frac{1}{3}.2 = \frac{2}{3} \notin Z$.
	Definition: Factor ring Let I be an ideal of the ring R. Then the set $\{r + I : r \in R\}$ is a ring under addition and multiplication defined as $(a + I) + (b + I) = a + b + I$ and $(a + I) \cdot (b + I) = ab + I$ $\forall\, a, b \in R$. This ring is called factor ring or quotient ring and is denoted by R/I.

	Definition: Principal ideal An ideal generated by single element a is called a principal ideal and is denoted by <a>. Thus <a> = {ra : r ∈ R}. Then quotient ring is R/<a> Let $F = Z_p$, p is a prime and $f(x)$ be an irreducible polynomial of degree n over Z_p, the $\frac{F[x]}{\langle f(x)\rangle}$ is a field having p^n element, $\langle f(x)\rangle$ is the ideal generated by f(x).
35	**Construct a field consisting of four elements.** **[Hint: Using the irreducible binary polynomial** $x^2 + x + 1$**]**
	Solution: Consider $Z_2 = \{0,1\}$ $f(x) = x^2 + x + 1 \in Z_2[x]$ $f(0) = 0 + 0 + 1 = 1 \neq 0$ $f(1) = 1 + 1 + 1 = 3 \equiv 1 (\text{mod } 2) \neq 0$ $\therefore f(x)$ is irreducible over Z_2. $\therefore \frac{Z_2[x]}{\langle f(x)\rangle} = \frac{Z_2[x]}{\langle x^2 + x + 1\rangle}$ is a field having $2^2 = 4$ elements. To find the four elements Consider $g(x) \in Z_2[x]$ and $x^2 + x + 1 \in Z_2[x]$.

By division algorithm,

$$g(x) = q(x)(x^2 + x + 1) + r(x)$$

whereeither $r(x) = 0$ or deg $r(x) <$ deg$(x^2 + x + 1) = 2$

$$\therefore \quad \deg r(x) = 0 \text{ or } 1.$$

Hence $r(x) = ax + b$, where $a, b \in Z_2$

Since $g(x) = q(x)(x^2 + x + 1) + r(x)$

$$g(x) - r(x) = q(x)(x^2 + x + 1)$$

$$g(x) \equiv r(x) \bmod (x^2 + x + 1)$$

$$[g(x)] = [r(x)]$$

So, to find the equivalence classes mod$(x^2 + x + 1)$,

it is enough to find the possible values of $r(x) = ax + b$

If $a = 0, b = 0 \Rightarrow r(x) = 0$

If $a = 0, b = 1 \Rightarrow r(x) = 1$

If $a = 0, b = 1 \Rightarrow r(x) = x$

If $a = 1, b = 1 \Rightarrow r(x) = x + 1$

$\therefore$ the equivalence classes are $[0],[1],[x],[x + 1]$

$\therefore$ the 4 elements of the field $\dfrac{Z_2[x]}{\langle x^2 + x + 1 \rangle}$ are $[0],[1],[x],[x+1]$.

36 **In the above example, find $[x]^{-1}$**

Solution:

In the above example, we have proved $\frac{Z_2[x]}{\langle x^2+x+1\rangle}$ is a field having the four elements $[0], [1], [x], [x+1]$. The non-zero elements $[1], [x], [x+1]$ form a group under multiplication, because $\frac{Z_2[x]}{\langle x^2+x+1\rangle}$ is a field. We write $[1] = 1, [x] = x, [x+1] = x+1$.

•	1	x	$x+1$
1	1	x	$x+1$
x	x	$x+1$	1
$x+1$	$x+1$	1	x

$x \bullet x = x^2 \Rightarrow$

$$x^2 \overline{)\, x^2+x+1} \quad (1$$
$$x^2$$
$$\overline{\quad x+1}$$

$x \bullet (x+1) = x^2 + x \Rightarrow$

$$x^2+x \overline{)\, x^2+x+1} \quad (1$$
$$x^2+x$$
$$\overline{\quad 1}$$

$(x+1)\bullet(x+1) = x^2 + 2x + 1$

$= x^2 + 0x + 1 \quad [\text{since } 2 \equiv 0 (\text{mod } 2)]$

$= x^2 + 1$

$\Rightarrow$

$$x^2+1 \overline{)\, x^2+x+1} \quad (1$$
$$x^2+1$$
$$\overline{\quad x}$$

Since 1 is the identity element, we see that $x \bullet (x+1) = 1$.

$\therefore$ inverse of x is $x+1$. Hence $[x]^{-1} = [x+1]$.

37 **In $Z_3[x]$, $s(x) = x^2 + x + 2$. Show that s(x) is irreducible over Z_3 and construct that the field $\frac{Z_3[x]}{\langle s(x)\rangle}$. What is the order of this field?**

Solution:

Consider $Z_3 = \{0,1, 2\}$

$s(x) = x^2 + x + 2 \in Z_3[x]$

$s(0) = 0 + 0 + 2 = 2 \neq 0$

$s(1) = 1 + 1 + 2 = 4 \equiv 1 (\text{mod } 3) \neq 0$

$s(2) = 4 + 2 + 2 = 8 \equiv 2 (\text{mod } 3) \neq 0$

$\therefore$ $s(x)$ is irreducible over Z_3.

$\therefore \frac{Z_3[x]}{\langle s(x)\rangle} = \frac{Z_3[x]}{\langle x^2 + x + 2\rangle}$ is a field having $3^2 = 9$ elements.

To find the nine elements

Consider $g(x) \in Z_3[x]$ and $x^2 + x + 2 \in Z_3[x]$.

By division algorithm,

$$g(x) = q(x)(x^2 + x + 2) + r(x)$$

where either $r(x) = 0$ or $\deg r(x) < \deg(x^2 + x + 1) = 2$

$\therefore$ $\deg r(x) = 0$ or 1.

Hence $r(x) = ax + b$, where $a, b \in Z_3$

Since $$g(x) = q(x)(x^2 + x + 2) + r(x)$$

$$g(x) - r(x) = q(x)(x^2 + x + 2)$$

$$g(x) \equiv r(x) \bmod(x^2 + x + 2)$$

$$[g(x)] = [r(x)]$$

So, to find the equivalence classes $\bmod(x^2 + x + 2)$,

it is enough to find the possible values of $r(x) = ax + b$

If $a = 0, b = 0 \Rightarrow r(x) = 0$

If $a = 0, b = 1 \Rightarrow r(x) = 1$

If $a = 0, b = 2 \Rightarrow r(x) = 2$

If $a = 1, b = 0 \Rightarrow r(x) = x$

If $a = 1, b = 1 \Rightarrow r(x) = x + 1$

If $a = 1, b = 2 \Rightarrow r(x) = x + 2$

If $a = 2, b = 0 \Rightarrow r(x) = 2x$

If $a = 2, b = 1 \Rightarrow r(x) = 2x + 1$

If $a = 2, b = 2 \Rightarrow r(x) = 2x + 2$

$\therefore$ the equivalence classes are $[0],[1],[2],[x],[x + 1],[x + 2],[2x],[2x + 1],[2x + 2]$

$\therefore$ the 9 elements of the field $\frac{Z_3[x]}{\langle s(x) \rangle}$ are $[0],[1],[2],[x],[x + 1],[x + 2],[2x],[2x + 1],[2x + 2]$.

Hence the number of elements = 9.

MOHAMED SATHAK A.J.COLLEGE OF ENGINEERING

MA8551- Algebra and Number Theory

NOTES

UNIT-III DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS

Division algorithm – Base – b representations – Number patterns – Prime and composite numbers – GCD – Euclidean algorithm – Fundamental theorem of arithmetic – LCM.

DIVISIBILITY:

An integer b is divisible by an integer 'a' $(a \neq 0)$ if there is an integer x such that b=ax and we write it as $a|b$. If b is not divisible by a, then we write it as $a \nmid b$.

Theorem:

1. Prove the following:

(1). $a|b$ implies $a|bc$ for any integer

Proof:

Given $a|b$ by definition b=ax .....(1) for some integer x

Multiply (1) by c

$\Rightarrow bc = acx$

$\Rightarrow bc = a(cx)$, where $z = cx$ an integer

$bc=az \Rightarrow a|bc$

(2). $a|b$ and $b|c \Rightarrow a|c$ for any integer

Proof:

Assume that a/b and b/c

$a|b \Rightarrow b=ax \cdots (1)$ for some integer x

$b|c \Rightarrow c = by \cdots (2)$ for some integer y

Substitute (1) in (2),

$c = (ax)y = a(xy) = az$, where $z = xy$ is an integer

$\Rightarrow a|c$

(3). $a|b$ and $a \mid c \Rightarrow a|(bx+cy)$ for any integer x & y

Proof:

By definition, $b=ax_1$, where x_1 is an integer.

Multiply both side by x, $bx = a \times x_1$….(1)

$$\text{Assume that } a|c \text{ then } c = ay_1, \text{ for some integer } y_1$$
$$cy = ayy_1 \cdots (2)$$

$$\text{Adding } (1) \text{ and } (2)$$
$$bx+cy = axx_1 + ayy_1 = a(xx_1 + yy_1) = az, \text{ where } z = xx_1 + yy_1 \text{ is an integer}$$
$$\Rightarrow a|(bx+cy)$$

(4). $a|b$ and $b|a \Rightarrow a = \pm b$

Proof:

Given $a|b$ by definition b=ax …..(1) for some integer x

$$b|a \Rightarrow a=by \cdots (2) \text{ for some integer } y$$

Multiply (1) and (2),

$$ab = (ax)(by)$$
$$\Rightarrow 1 = xy$$
$$\Rightarrow x=1 \ \& \ y=1 \text{ or } x=-1 \ y=-1$$
$$\Rightarrow a= \pm b$$

(5). If $m \neq 0$, $a|b \Leftrightarrow ma|mb$

Proof:

Given $a|b$ by definition b=ax …..(1) for some integer x.

Multiply (1) both sides by m , $m \neq 0$

mb=max $\Rightarrow$ ma|mb

Assume that ma|mb

by definition, mb=max for some integer x

b=ax

$\Rightarrow$ a|b

THE DIVISION ALGORITHM:

Let a be any integer and b be a positive integer. Then there exist unique q and r such that

$a = b \cdot q + r$, where $0 \le r < b$, and where a is dividend, b is divisor, q is quotient and r is remainder.

Proof:

Existence Part

Let $S = \{a - bn : n \in Z \text{ and } a - bn \ge 0\}$

Then, first we prove that S is non-empty.

Case(i): Let $a \ge 0$ Then $a - b(0) = a \ge 0$ with $0 \in Z$. By the definition S, $a \in S$. Hence S is non-empty.

Case(ii):

Let $a < 0$ since b is a positive integer $b \ge 1$
Hence $ab \le a$, since $a < 0$
$\Rightarrow a - b \cdot a \ge 0$, *with* $a \in Z$.

By the definition of S, $a - b \cdot a \in S$.
Thus in both cases S contains atleast one element. So S is a non-empty subset of W.
Therefore, by the well ordering principle, S contains a least element r.
Since $r \in S$, an integer q exists such that $r = bq$, where $r \ge 0$

To show that $r < b$:
We will prove by contradiction.
Assume $r \ge b$. Then $r - b \ge 0$. But $r - b = (a - bq) - b = a - b(q + 1)$.

Since $a - b(q+1)$ is of the form $a - bn$ and is ≥ 0, $a - b(q+1) \in S$
$\Rightarrow r - b \in S$. Since $b > 0$, $r - b < r$. Thus $r - b$ is smaller than r and is in S.
This contradicts our assumption of r, *So* $r < b$.
Thus, there are integers q and r such that $a = b \cdot q + r$, where $0 \le r < b$.

Uniqueness Proof:

Let there be two sets of integers q, r and q', r' such that
$a = bq + r$ $-----(1)$
and $a = bq' + r'$ $-----(2)$

Assume that $q \geq q'$, from (1) and (2)

$bq + r = bq' + r' \Rightarrow b(q - q') = r' - r \quad -----(3)$

with $r' - r < b \quad -----(4)$

$\sin ce\ r' < b$ and $r < b$

Assume that $q > q'$. Then $q - q' \geq 1$. Since $b > 0$. $b(q - q') \geq b$.

Hence from (3) $r' - r \geq b$, contradicts (4).

$\therefore q \ngeq q'$. hence q = q' , Therefore, from (3) $0 = r' - r \Rightarrow r = r'$

Thus, the integers q and r are unique.

i.e., There exist unique integers q and r such that

$a = b \cdot q + r$, where $0 \leq r < b$

Examples:

Find the quotient and the remainder

1. when 207 is divided be 15 : $207 = 15 \cdot 13 + 12,\ q = 13$ and $r = 12$

2. when -23 is divided by 5 :

$-23 = 5 \cdot (-4) + (-3)$, the remainder however, can never be negative.

so -23 written as $-23 = 5 \cdot (-5) + 2$, where $0 \leq r < 5$ $(r = 2)$. Thus $q = -5, r = 2$

The Pigenhole Principle.

If m pigeons are assigned to n pigenholes where m>n, then atleast two pigeons must occupy the same pigenhole.

Proof:

Suppose the given conclusion is false. That is no two pigeons occupy the same pigeonhole. Then every pigeon must occupy a distinct pigeonhole, so $n \geq m$, which is a contradiction. Thus, two or more pigeons must occupy some pigeonhole.

1. Let b be an integer ≥ 2 . Suppose b+1 integers are randomly selected. Prove that difference of two of them is divisible by b.

Proof:

When an integer is divisible by b, the possible remainder is one of 0, 1, 2… b-1. They are totally b. Therefore, when b+1 integers are divisible by b, by the Pigeonhole principle at least 2 of these b+1 integers, say x and y, leave the same remainder.

i.e., $x = bq_1 + r$ *and* $y = bq_2 + r$

$\Rightarrow x - y = b(q_1 - q_2) \Rightarrow b \mid (x - y)$.

Hence difference of two of them is divisible by b.

Inclusion-Exclusion Principle:

Let A and B be finite sets. Then

$|A \cup B| = |A| + |B| - |A \cap B|$

If $A_1, A_2, \ldots A_n$ are finite sets, then $\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{1 \le i \le n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j| + \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| - \ldots\ldots + (-1)^{n+1} \left|\bigcap_{i=1}^{n} A_i\right|$

Problem:

1. Find the number of positive integer ≤ 2076 and divisible by neither 4 or 5.

Soln:

Let $A = \{x \in N / x \le 2076 \text{ and divisible by } 4\}, B = \{x \in N / x \le 2076 \text{ and divisible by } 5\}$

then $|A \cup B| = |A| + |B| - |A \cap B|$

$= \lfloor 2076/4 \rfloor + \lfloor 2076/5 \rfloor - \lfloor 2076/20 \rfloor$

$= 519 + 415 - 103 = 831$

Thus, among the first 2076 positive integer, there are 2076-831=1245 integers not divisible by 4 or 5.

2. Find the number of positive integers in the range 1976 through 3776 that are divisible by13.
Soln:

The number of positive integers ≤ 1976 that are divisible by $13 = \left[\frac{1976}{13}\right] = [152] = 152$

The number of positive integers ≤ 3776 that are divisible by $13 = \left[\frac{3776}{13}\right] = [290.46] = 290$

$\therefore$ The number of positive integers 1976 to 3776 that are divisible by 13

$= 290 - 152 + 1$

$= 139$ [$\because$ 1976 is included in the list of numbers divisible by 13]

3. Find the number of positive integer's ≤ 3000 and divisible by 3, 5, or 7.
Soln:
Let A,B,C be the set of numbers ≤ 3000 and divisible by 3, 5,7 respectively.
Required $|A \cup B \cup C|$
By inclusion and exclusion principle, we get
$|A \cup B \cup C| = S_1 - S_2 + S_3$
Now

$|A| = \left[\frac{3000}{3}\right] = [1000] = 1000$

$|B| = \left[\frac{3000}{5}\right] = [600] = 600$

$|C| = \left[\frac{3000}{7}\right] = [428.57] = 428$

$S_1 = |A| + |B| + |C| = 1000 + 600 + 428 = 2028$

$|A \cap B| = \left[\frac{3000}{3\times 5}\right] = [200] = 200$

$|A \cap C| = \left[\frac{3000}{3\times 7}\right] = [142.85] = 142$

$|B \cap C| = \left[\frac{3000}{5\times 7}\right] = [85.71] = 85$

$S_2 = |A \cap B| + |A \cap C| + |B \cap C| = 200 + 142 + 85 = 427$

Now $S_3 = |A \cap B \cap C| = \left[\frac{3000}{3\times 5\times 7}\right] = [28.57] = 28$

$|A \cup B \cup C| = S_1 - S_2 + S_3 = 2028 - 427 + 28 = 1629$

4. Prove that $n^2 + n$ is an even integer, where n is arbitrary integer.

To prove:

$p(n) = n^2 + n$ is an even integer

$p(1) = 1^2 + 1 = 2$ is an even number

We assume that the result is true for all k, k be the arbitrary number. $\Rightarrow p(k) = k^2 + k$ is an even integer

consider $p(k+1) = (k+1)^2 + (k+1)$

$= k^2 + 2k + 1 + k + 1 = (k^2 + k) + (2k + 2) =$ Even number

hence $p(n) = n^2 + n$ is even integer $\forall$ n.

5. Show that for any integer n, $n^2 - n$ is divisible by 2 and $n^5 - n$ is divisible by 6

Soln:

$n^2 - n = n(n-1)$ It is two consecutive number. So it is divisible by 2

To Prove: $n^5 - n$ **is** divisible by 6

$n^5 - n = n(n^4 - 1) = n(n^2 - 1)(n^2 + 1) = n(n-1)(n+1)(n^2 + 1) = (n-1)n(n+1)(n^2 + 1)$

Now, as we know that product of 3consecutive natural numbers is always divisible by3and that of 2 consecutive natural numbers is always divisible by2 so this expression is always divisible by6.

6. Show that $30 | n^5 - n$, where n is an arbitrary integer

Soln:

First we prove $n^5 - n$ isdivisible by 6

$n^5 - n = n(n^4 - 1) = n(n^2 - 1)(n^2 + 1) = n(n-1)(n+1)(n^2+1) = (n-1)n(n+1)(n^2+1)$

Now, as we know that product of 3consecutive natural numbers is always divisible by3 and that of 2 consecutive natural numbers is always divisible by2 so this expression is always divisible by6.

Now to prove divisibility by5,First we write the factorisation as under

$$\begin{aligned} n(n-1)(n+1)(n^2+1) &= n(n-1)(n+1)\left((n^2-4)+5\right) \\ &= n(n-1)(n+1)\left((n-2)(n+2)+5\right) \\ &= n(n-1)(n+1)(n-2)(n+2)+5n(n-1)(n+1) \end{aligned}$$

We see that second term is divisible by 5and first term is also divisible by5 as it is product of 5 consecutive natural numbers.Hence the given expression is divisible by 5×6=30.

Hence the proof.

7. If the sum of the cubes of three consecutive integers is a cube k^3, prove that $3 \mid k$

Soln:

Let n, n+1, n+2 be the three consecutive integers.

Given $n^3 + (n+1)^3 + (n+2)^3$ is a cube k^3

$\Rightarrow n^3 + n^3 + 3n^2 + 3n + 1 + n^3 + 3n^2 \cdot 2 + 3n \cdot 2^2 + 2^3 = k^3$

$\Rightarrow 3n^3 + 9n^2 + 15n + 9 = k^3$

$\Rightarrow 3\left(n^3 + 3n^2 + 5n + 3\right) = k^3$

$\Rightarrow 3 \mid k^3 \Rightarrow 3 \mid k \cdot k \cdot k$

Since 3 is a prime, $3 \mid k$

Base-b representation:

The expression $a_k b^k + a_{k-1} b^{k-1} + ... + a_1 b + a_0$ is the base-b representation of the integer N.

Accordingly, we write $N = (a_k\, a_{k-1} ..... a_1 a_0)_b$ in base b.

For example, $(345)_{10} = 3(10)^2 + 4(10)^1 + 5(10)$

$(345)_8 = 3(8)^2 + 4(8)^1 + 5(8) = 165$

Hexadecimal Expansion:

The base 16 expansion of an integer is called its hexadecimal expansion. Hexadecimal Expansion uses the sixteen digits 0,1,2,3,…9,A,B,C,D,E,and F. Where the letters A to F represent the digits 10 to 15 respectively (in decimal notation).

Problem:

1. Express $(101011111)_2$ in base 10.

Soln:

$$(101011111)_2 = 1(2^8)+0(2^7)+1(2^6)+0(2^5)+1(2^4)+1(2^3)+1(2^2)+1(2^1)+1(2^0)$$
$$= 256+64+16+8+4+2+1 = 351$$

2. Express $(3AB0E)_{16}$ in base ten.

Soln:

We know A=10,B=11,E=14

$$(3AB0E)_{16} = 3(16^4)+A(16^3)+B(16^2)+0(16^1)+E(16^0)$$
$$= 3(16^4)+10(16^3)+11(16^2)+0(16^1)+14(16^0)$$
$$= 196608+40960+2816+14 = 240398$$

3. Express 1776 in the octal system.

Soln:

1776=222(8)+**0**

222=27(8)+**6**

27=3(8)+**3**

3=0(8)+**3**

$1776 = (3360)_8$

4. Find the value of the base b so that 144_b=49.

Soln:

$144_b=49 \Rightarrow 1\times b^2+4\times b^1+4\times b^0 = 49$

$\Rightarrow b^2+4b+4 = 49$

$\Rightarrow b^2+4b-45 = 0$

$\Rightarrow (b+9)(b-5) = 0$

$\sin ce \;\; b \neq -9,$

$\therefore b = 5$

Number Patterns:

Consider the following number patter,

$$1\cdot 9+2=11$$
$$12\cdot 9+3=111$$
$$123\cdot 9+4=1111$$
$$1234\cdot 9+5=11111$$

In general,

$$\mathbf{123\ldots(n)\cdot 9\ +\ (n+1)=\underbrace{111\ldots11}_{\text{n+1 ones}}}$$

1. Add two more rows to the following pattern, and write conjecture formula for the nthrow:

$$\mathbf{9\cdot 9+7=88}$$
$$\mathbf{98\cdot 9+6=888}$$
$$\mathbf{987\cdot 9+5=8888}$$
$$\mathbf{9876\cdot 9+4=88888}$$
$$\mathbf{98765\cdot 9+3=888888}$$

Soln:

The next two rows of the given patterns are,

$$987654\cdot 9+2=8888888$$
$$9876543\cdot 9+1=88888888$$

The general pattern is

$$98765.....(10-n)\cdot 9+(8-n)=\underbrace{888.....88}_{(n+1)\ Eights}$$

2. Consider the number pattern

$$\mathbf{10^2-10+1=91}$$
$$\mathbf{10^4-10^2+1=9901}$$
$$\mathbf{10^6-10^3+1=999001}$$
$$\mathbf{10^8-10^4+1=99990001}$$

Conjecture a formula for the nth row of this pattern and establish the validity of the formula.

Soln:

$$n^{th}\ row\ is: 10^{2n}-10^n+1=\underbrace{999\cdots9}_{\text{n times}}\underbrace{000\cdots0}_{\text{(n-1) times}}1$$

$$LHS:\ 10^{2n}-10^n+1=10^n\left(10^n-1\right)+1$$
$$=10^n(\underbrace{999\cdots9}_{\text{n times}})+1$$

$$= \underbrace{999\cdots9}_{\text{n times}}\ \underbrace{000\cdots0}_{\text{n zeros}} + 1$$

$$= \underbrace{999\cdots9}_{\text{n times}}\ \underbrace{000\cdots0}_{\text{(n−1) zeros}}\ 1$$

Prime and Composite Numbers:

A positive integer p>1 is called a prime number if its only positive factors are a and p. If P>1 is not a prime, then it is called a composite number.

1. Theorem (Euclid): There are infinitely many primes.

Proof:

We prove by contradiction method.

Assume that there are only n primes $p_1, p_2, ..., p_n$ where n is prime.

Now consider the integer

$m = p_1 \cdot p_2 \cdot p_3 ..., p_n$

Since $m > 1$, by theorem, every integer $n \geq 2$ has a prime factor. $\therefore$ m has a prime factor p.

But none of the primes $p_1, p_2, p_3, ..., p_n$ divide m

For, if $p_i | m$ and since $p_i \mid p_1 \cdot p_2 \cdot p_3 ..., p_n$

we get $p_i \mid m - p_1 \cdot p_2 \cdot p_3 ..., p_n \Rightarrow p_i \mid 1$, which is not true and hence a contradiction.

$\therefore\ p_i \nmid m$

So, we have a prime p which is not in the list of n primes. Thus, we have n+1 primes $p_1, p_2, p_3, ..., p_n, p_{n+1}$

Which contradicts the assumption there are only n primes.

So, our assumption of finiteness is wrong. Hence the number of primes is infinite.

2. Theorem: Every integer $n \geq 2$ has a prime factor.

Proof:

We prove the theorem by strong principle of induction on n.

If n=2, then the statement is true. Since 2 is a prime and 2 is a factor of 2.

Assume the statement is true for all integers upto k, k>2.

To prove it is true for k+1:

If k+1 is a prime, then k+1 is a prime factor of k+1.

If k+1 is not a prime, then k+1 must be a composite number.

So, it must have factor d, where $d \leq k$. Then by the induction hypothesis, d has a prime factor p.

Since p | d and d | k+1, we have p | k+1. So p is a factor of k+1.

Hence by second principle of induction the statement is true for every integer >1

$\therefore$ Every integer $n \geq 2$ has a prime factor.

3. Every composite number n has a prime factor $\leq \lfloor \sqrt{n} \rfloor$.

Proof:

Given n is a composite number.

Then there exist positive integer a and b such that n=ab, where 1<a<n, 1<b<n.

We will prove $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Suppose $a > \sqrt{n}$ and $b > \sqrt{n}$

Then $a \cdot b > \sqrt{n} \cdot \sqrt{n} = n$

$\Rightarrow a \cdot b > n$

which is impossible, either $a \leq \lfloor \sqrt{n} \rfloor$. or $b \leq \lfloor \sqrt{n} \rfloor$.

we know that every positive integer ≥ 2 has a prime factor.

Any such a factor a or b is also a factor of $a \times b = n$

So 'n' must have a prime factor $\leq \lfloor \sqrt{n} \rfloor$.

Theorem:

Let $p_1, p_2, ..., p_r$ be the primes $\leq \lfloor \sqrt{n} \rfloor$. Then the number of prime $\leq n$ is

$$\pi(n) = n - 1 + \pi\left(\sqrt{n}\right) - \sum_i \left\lfloor \frac{n}{p_i} \right\rfloor + \sum_{i<j} \left\lfloor \frac{n}{p_i p_j} \right\rfloor - \sum_{i<j<k} \left\lfloor \frac{n}{p_i p_j p_k} \right\rfloor + \ldots + (-1)^n \sum_{i<j<k\ldots<r} \left\lfloor \frac{n}{p_i p_j p_k \ldots p_r} \right\rfloor$$

Problem:

1. Show that 101 is a prime.

Soln:

Given number is 101.

First we find all prime $\leq \lfloor 101 \rfloor = 10$.

The primes are 2,3,5,7. Since none of these are a factor of 101.So 101 is prime number.

2. Determine if 1601 is a prime number.

Soln:

We know that if n has no prime factors $\le \left\lfloor \sqrt{n} \right\rfloor$, then n is a prime consider prime number $\le \left\lfloor \sqrt{1601} \right\rfloor \Rightarrow$ prime number ≤ 40 (approx.)

$\Rightarrow$ 2,3,5,7,11,13,17,19,23,29,31 and 37 and which are not factors of 1601

Therefore, 1601 is a prime

3. Find the number of primes ≤ 100

Soln:

Here n=100, and $\sqrt{100} = 10$

Primes which are less than or equal to 10 are:2,3,5,7.

Then the number of prime ≤ 100 is

$$\pi(\mathrm{n}) = n - 1 + \pi\left(\sqrt{\mathrm{n}}\right) - \sum_{i} \left\lfloor \frac{\mathrm{n}}{\mathrm{p_i}} \right\rfloor + \sum_{i<j} \left\lfloor \frac{\mathrm{n}}{\mathrm{p_i\, p_j}} \right\rfloor - \sum_{i<j<k} \left\lfloor \frac{\mathrm{n}}{\mathrm{p_i\, p_j\, p_k}} \right\rfloor + \ldots + (-1)^n \sum_{i<j<k\ldots<r} \left\lfloor \frac{\mathrm{n}}{\mathrm{p_i\, p_j\, p_k \ldots p_r}} \right\rfloor$$

$$\pi(100) = 100 - 1 + \pi\left(\sqrt{100}\right) - \left\{ \left\lfloor \frac{100}{2} \right\rfloor + \left\lfloor \frac{100}{3} \right\rfloor + \left\lfloor \frac{100}{5} \right\rfloor + \left\lfloor \frac{100}{7} \right\rfloor \right\}$$
$$+ \left\{ \left\lfloor \frac{100}{2\times 3} \right\rfloor + \left\lfloor \frac{100}{2\times 5} \right\rfloor + \left\lfloor \frac{100}{2\times 7} \right\rfloor + \left\lfloor \frac{100}{3\times 5} \right\rfloor + \left\lfloor \frac{100}{3\times 7} \right\rfloor + \left\lfloor \frac{100}{5\times 7} \right\rfloor \right\}$$
$$- \left\{ \left\lfloor \frac{100}{2\times 3\times 5} \right\rfloor + \left\lfloor \frac{100}{2\times 3\times 7} \right\rfloor + \left\lfloor \frac{100}{2\times 5\times 7} \right\rfloor + \left\lfloor \frac{100}{3\times 5\times 7} \right\rfloor \right\} + \left\lfloor \frac{100}{2\times 3\times 5\times 7} \right\rfloor$$

$$= 99 + 4 - \{50 + 33 + 20 + 14\} + \{16 + 10 + 7 + 6 + 4 + 2\} - \{3 + 2 + 1 + 0\} + 0$$
$$= 103 - 117 + 45 - 6$$
$$= 25$$

4. Find the smallest prime factor of 129.

Solution:

Here n=129, and $\left\lfloor \sqrt{129} \right\rfloor = 11$

Primes which are less than or equal to 11 are:2,3,5,7,11.

$2 \nmid 129$ and $3 \mid 129$ Hence the smallest prime factor of 129 is 3.

1. Theorem:

For every positive integer n, there are n consecutive integers that are composite numbers.

Proof:

Consider the n consecutive integers

$(n+1)!+2,\ (n+1)!+3,\ldots..,\ (n+1)!+(n+1)$ Where $n \geq 1$.

Let $2 \leq k \leq n+1$

Then $k|(n+1)!$ and always $k|k$

$\Rightarrow k|\left[(n+1)!+k\right]$, *for every* $k = 2,3,...(n+1)$

$\Rightarrow 2|\left[(n+1)!+2\right], 3|\left[(n+1)!+3\right],\ldots..,(n+1)|\left[(n+1)!+(n+1)\right]$

$\Rightarrow (n+1)!+2,\ (n+1)!+3,\ldots..,\ (n+1)!+(n+1)$ are n consecutive integer which are composite numbers.

2. Obtain six consecutive integers that are composite.

Soln:

By theorem, for every integer n, there are n consecutive integers that are composite numbers. Then the six consecutive composite numbers are

$(n+1)!+2,\ (n+1)!+3, (n+1)!+4,\ (n+1)!+5,\ (n+1)!+6,\ (n+1)!+7$

put $n = 6$

$\therefore$ The six consecutive composite numbers are $5042, 5043, 5044, 5045, 5046,$ and 5047

3. Prove that any prime of the form 3k+1 is of the form 6k+1.

Soln.:

Let the prime p=3k+1, then k must be even.

[if k is odd, then 3k is odd $\Rightarrow$3k+1 is even $\Rightarrow$ 3k+1 is not prime]

$\therefore$ k=2k′, then p=3(2k′)+1=6k′+1.

Hence any prime of the form 3k+1 is of the form 6k+1.

4. Show that product of k consecutive integers is divisible by k!

Proof:

Let $(n+1), (n+2), \cdots\cdot, (n+k)$ be the 'k' consecutive integer.

Product of 'k' consecutive integer $= (n+1)(n+2)\cdots\cdot(n+k)$

$$= \frac{n!}{n!}(n+1)(n+2)\cdots\cdot(n+k)$$

$$= \frac{(n+k)!}{n!}$$

Product of 'k' consecutive integer $= \dfrac{k!(n+k)!}{k!\ n!} = k!\ {}_{n+r}C_r = \text{Integer}$

Hence the product of k consecutive integers is divisible by k!

Greatest Common Divisor(GCD)

Definition:

The greatest common divisor of two integer a and b,not both zero, is the largest positive integer that divides bots a and b. It is denoted by gcd (a,b) or (a,b).

For example, (3,15)=3,(12,18)=6,(-15,20)=5

Since (a,-b)=(-a,b)=(-a,-b)=(a,b)we confine our discussion of gcd to positive integers.

Definition:

A positive integer d is the **gcd** of integers a and b if

$(i).\ d|a$ and $d|b$

$(ii).$If $c|a$ and $c|b$, then $c|d$, where c is a positive integer.

Relatively Prime:

If $(a,b)=1$, then the integers a and b are said to be relatively prime.

1. (Euler) Prove that the GCD of the positive integers a and b is linear combination of a &b.
Proof:

LetS be the set of positive linear combination of a and b; that is $S=\{ma+nb/\ ma+nb>0, m,n\in Z\}$

To show that S has a least element:

Since $a>0,\ a=1\cdot a+0\cdot b\in S,$ S is non empty. So, by the well-ordering principle,

S has a least positive element d.

To show that $d=(a,b)$:

Since d belongs to S, $d=\alpha a+\beta b$ for some integer α and β.

(1).First we will show that d / a and d / b:

By the division algorithm, there exist integers q and r such that $a=dq+r,$

where $0\le r<d$. Substituting for d.

$r=a-dq$

$=a-(\alpha a+\beta b)q$

$=(1-\alpha q)a+(-\beta q)b$

This shows r is a linear combination of a and b.

If $r>0$, then $r\in S$. Since $r<d$, r is less than the smallest element in S.

Which is a contrdiction. So $r=0;$ thus, a = dq, so d|a.

Similarly, d|b. Thus d is common divisor of a and b.

(2).To show that any positive common divisior d' of a and b is $\leq$ d :

Since $d'|$ a, and $d'|b \Rightarrow d'|(\alpha a+\beta b)$

that is $d'|d$. So $d' \leq d$.

Thus, by parts (1) and (2), d $=(a,b)$

2.Two positive integer a and b are relatively prime if and only iff there are integers α and β such that $\alpha a+\beta b=1$.

Proof:

Assume that a and b are relatively prime, then (a,b)=1

We know that, there exist integer α and β such that

$(a,b)=\alpha a+\beta b$

$\Rightarrow 1=\alpha a+\beta b$

Conversely, assume that there exist integers α and β such that $\alpha a+\beta b=1$.

Let d=(a,b). Then d|a and d|b.

$\Rightarrow d|(\alpha a+\beta b) \Rightarrow d|1 \Rightarrow d=1$

$\Rightarrow$ (a,b)=1 $\Rightarrow$ a and b are relatively prime.

3. If d=(a,b), then $\left(\frac{a}{d},\frac{b}{d}\right)=1$

Proof:

Since d is gcd of a and b $\Rightarrow$ d is positive integer

d=(a,b) $\Rightarrow$ there exist integers α and β such that $d=\alpha a+\beta b$

$\Rightarrow 1=\alpha\left(\frac{a}{d}\right)+\beta\left(\frac{b}{d}\right)$

$\Rightarrow$ by the above theorem $\frac{a}{d}$ and $\frac{b}{d}$ are relatively prime

$\Rightarrow\left(\frac{a}{d},\frac{b}{d}\right)=1$

4. If (a,b)=1=(a,c) then (a,bc)=1

Proof:

(a,b)=1$\Rightarrow$ there exist integers α and β such that $\alpha a+\beta b=1$-----(1)

(a,c)=1 $\Rightarrow$ there exist integers γ and δ such that γa+δc=1 $-----(2)$

Using (2) *in* (1),

$\alpha a + \beta b(1) = 1$

$\alpha a + \beta b(\gamma a + \delta c) = 1$

$\alpha a + \beta\gamma ab + \beta\delta bc = 1$

$(\alpha + \beta\gamma b)a + (\beta\delta)bc = 1 \Rightarrow (a,bc)=1$

5. Prove that $(a, a-b)=1$ if and only if $(a, b)=1$

Proof:

Let $(a, b)=1$

Then there exist integer l and m such that

$la + mb = 1$

$la + ma + mb - ma = 1$

$(l+m)a - m(a-b) = 1$

$(l+m)a + (-m)(a-b) = 1 \Rightarrow (a, a-b)=1$

Conversely, let $(a, a-b)=1$. To prove : $(a,b)=1$

Then there exist integer α and β such that

$\alpha a + \beta(a-b) = 1$

$\alpha a + \beta a - \beta b = 1$

$(\alpha+\beta)a + (-\beta)b = 1 \Rightarrow (a,b)=1$

Hence the proof**.**

6. If d=(a,b) and d' is any common divisor of a and b, then d'|d.

Proof:

Since d=(a,b) , ∃, α and β such that $d = \alpha a + \beta b$.

also since d' is common divisor of a & b. ∴ d'|a & d'|b

$\Rightarrow$ d'|(αa+βb); so d'|d.

Problem:

1. Find the GCD of 1819 & 3587.

Soln:

$(3587,1819) = 1\times1819 + 1768$

$(1819,1768) = 1\times1768 + 51$

$(1768,51) = 34\times51 + 34$

$(51,34) = 1\times34 + 17$

$(34,17) = 2\times17 + 0$

$\therefore$ gcd of $1819, 3587$ is 17

2. Find the GCD of $a+b, a^2-b^2$.

$GCD\left(a+b, a^2-b^2\right) = GCD\left(a+b,(a-b)(a+b)\right) = a+b$

3. If $(a,4)=2$ & $(b,4)=2$ **show that** $(a+b,4)=2$

Soln.:

$(a,4)=2 \Rightarrow$ gcd of $(a,4)=2 \Rightarrow 2/a$ but $4 \neq a \therefore a = 2k$, and k is odd

$(\mathrm{b},4)=2 \Rightarrow$ gcd of $(\mathrm{b},4)=2 \Rightarrow 2/\mathrm{b}$ but $4 \neq \mathrm{b} \therefore b = 2l$, and l is odd

$a+b = 2k+2l = 2(k+l) = 2(\text{even}) = 2(2m) = 4m$

$\therefore 4/a+b \Rightarrow \gcd(a+b,4) = 4$

3. Evaluate by apply Euclidean Algorithm(2076,1776)

Solu.:

By successive application of division algorithm, we get:

$2076 = 1\cdot1776 + 300$

$1776 = 5\cdot300 + 276$

$300 = 1\cdot276 + 24$

$276 = 11\cdot24 + 12$

$24 = 2\cdot12 + 1$

Since the last nonzero remainder is $(2076,1776) = 12$

4. Apply Euclidean Algorithm and express (4076, 1024) as a linear combination of 4076, 1024.

Soln.:

By successive application of division algorithm, we get:

$4076 = 3\cdot1024 + 1004$

$1024 = 1\cdot1004 + 20$

$1004 = 50\cdot20 + 4$

$20 = 5\cdot4 + 0$

Since the last nonzero remainder is $(4076,1024) = 4$

$$(4076,1024) = 4 = 1004 - 50 \cdot 20$$
$$= 1004 - 50(1024 - 1 \cdot 1004)$$
$$= 51 \cdot 1004 - 50 \cdot 1024$$
$$= 51(4076 - 3 \cdot 1024) - 50 \cdot 1024$$
$$= 51 \cdot 4076 + (-203) \cdot 1024$$

5. Apply Euclidean Algorithm to express the gcd of (1976, 1776) as a linear combination of 1976, 1776.

Soln.:

By successive application of division algorithm, we get:

$$1976 = 1 \cdot 1776 + 200$$
$$1776 = 8 \cdot 200 + 176$$
$$200 = 1 \cdot 176 + 24$$
$$176 = 7.24 + 8$$
$$24 = 3 \cdot 8 + 0$$

Since the last nonzero remainder is $(1976,1776) = 8$

$$(1976,1776) = 8 = 176 - 7 \cdot 24$$
$$= 176 - 7(200 - 1 \cdot 176)$$
$$= 8 \cdot 176 - 7 \cdot 200$$
$$= 8(1776 - 8 \cdot 200) - 7 \cdot 200$$
$$= 8 \cdot 1776 - 71 \cdot 200$$
$$= 8 \cdot 1776 - 71(1976 - 1.1776)$$
$$= 79.1776 - 71.1976$$
$$= 79.1776 + (-71).1976$$

Hence the gcd is a linear combination of numbers 1976,1776.

6. Using recursion, evaluate (15,28,50).

Soln.:

$$(15,28,50) = (15,50,28)$$
$$= ((15,50),28)$$
$$= (5,28) = 1$$

1 is the GCD $(15,28,50)$

7. Using recursion, evaluate (18, 30, 60, 75, 132).
Soln:

$$(18,30,60,75,132) = ((18,30,60,75),132)$$
$$= (((18,30,60),75),132)$$
$$= ((((18,30),60),75),132)$$
$$= (((6,60),75),132)$$
$$= ((6,75),132) = (3,132) = 3$$

Fundamental Theorem of Arithmetic:

Statement:

Every integer $n \geq 2$ either is a prime or can be expressed as a product of primes. The factorization into primes is unique except for the order of the factors.

Proof:

First, we will show by strong induction that n either is a prime or can be expressed as a product of primes.

Then we will establish the uniqueness of such a factorization.

Let P(n) denote the statement that n is a prime or can be expressed as a product of primes.

(i) To show that P(n) is true for every integer n ≥ 2:

Since 2 is a prime, clearly P(2) is true.

Now assume P(2), P(3),…..P(k) are true; that is every integer 2 through k either is a prime or can be expressed as a product of primes.

If k+1 is a prime, then P(k+1) is true. So suppose k+1 is composite. Then k+1 = ab for some integers a and b, where 1 < a, b < k+1. By the inductive hypothesis, a and b either are primes or can be expressed as products of primes; in any event, k+1=ab can be expressed as products of primes. Thus, P(k+1) is also true.

Thus by strong induction, the result holds for every integer $n \geq 2$

(ii) To Establish the Uniqueness of the Factorization:

Let n be a composite number with two factorization into primes; $n = p_1 p_2 \cdots\cdots p_r = q_1 q_2 \cdots\cdots q_s$

we will show that r = s and every p_i equals some q_j ,where $1 \leq i, j \leq r;$ that is, the primes $q_1, q_2, \ldots.. q_s$ are a permutation of the primes $p_1 p_2 \cdots\cdots p_r$

Assume, for convenience that $r \leq s.$ since $p_1 p_2 \cdots\cdots p_r = q_1 q_2 \cdots\cdots q_s,\ p_1 / q_1 q_2 \cdots\cdots q_s, \Rightarrow p_1 = q_i$ for some i.

Dividing both sides p_1, we get: $p_2 \ldots.. p_r = q_1 q_2 \ldots q_{i-1} q_i q_{i+1} \ldots q_s$

Now, p_2 *divides the RHS, so* $p_2 = q_j$ for some j. *cancel* p_2 form both sides :

$p_3 \ldots\ldots \mathrm{p}_r = q_1 q_2 \ldots q_{i-1} q_i q_{i+1} \ldots q_{j-1} q_j q_{j+1} q_s$

Since $r \le s$, continuing like this, we can cancel p_t with some q_k. This yields a 1 on the LHS at the end. Then the RHS cannot be left with any primes, since a product of primes can never yield a 1; thus, we must have exhausted all q_k's by now. therefore, r = s and hence the primes $q_1, q_2, \ldots\ldots q_s$ are the same as the primes $p_1 p_2 \cdots\cdots p_r$ in some order. Thus, the factorization on n is unique, except for the order in which the primes as written.

Note:

(i). Every composite number n can be factored into primes. Such a product is the **prime power decomposition** of n.

(ii). If the primes occur in increasing order, then it is called a **Canonical decomposition**.

Problem:

1. Using canonical decomposition of 168 and 180 find their GCD.

$168 = 2^3 \cdot 3 \cdot 7 \qquad 180 = 2^2 \cdot 3^2 \cdot 5$

$GCD = (168, 280) = 2^2 \cdot 3 = 12$

2. Find the canonical decomposition of $2^9 - 1$

$2^9 - 1 = \left(2^3\right)^3 - 1^3 = \left(2^3 - 1\right)\left(2^6 + 2^3 + 1\right) \quad \because\ a^3 - b^3 = (a-b)\left(a^2 + ab + b^2\right)$

$= (7)(73)$

Least Common Multiple (LCM):

The least common multiple of two positive integers a and b is the least positive integer divisible by both a and b; it is denoted by [a,b].

Problem:

1. Using canonical decomposition of 1050 and 2574.

Soln.:

$1050 = 2 \times 3 \times 5 \times 7$

$2574 = 2 \times 3^2 \times 11 \times 13$

$[1050, 2574] = 2 \times 3^2 \times 5^2 \times 7 \times 11 \times 13 = 450450$

2. Using canonical decomposition of 168 and 180 find their GCD and LCM.

Soln.:

$168 = 2^3 \cdot 3 \cdot 7 \qquad 180 = 2^2 \cdot 3^2 \cdot 5$

$GCD = (168, 280) = 2^2 \cdot 3 = 12$

$LCM = [168, 280] = 2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2520$

3. Find the canonical decomposition of 23!

Soln.:

The prime dividing 23! are 2,3,5.7,11,17,19,23

$$\text{The power of 2 dividing } 23! \text{ are} = \left[\frac{23}{2}\right] + \left[\frac{23}{2^2}\right] + \left[\frac{23}{2^3}\right] + \left[\frac{23}{2^4}\right]$$
$$= 11 + 5 + 2 + 1$$
$$= 19$$

$$\text{The power of 3 dividing } 23! \text{ are} = \left[\frac{23}{3}\right] + \left[\frac{23}{3^2}\right]$$
$$= 7 + 2$$
$$= 9$$

$$\text{The power of 5 dividing } 23! \text{ are} = \left[\frac{23}{5}\right] + \left[\frac{23}{5^2}\right]$$
$$= 4 + 0 = 4$$

$$\text{The power of 7 dividing } 23! \text{ are} = \left[\frac{23}{7}\right] = 3$$

$$\text{The power of 11 dividing } 23! \text{ are} = \left[\frac{23}{11}\right] = 2$$

$$\text{The power of 13 dividing } 23! \text{ are} = \left[\frac{23}{13}\right] = 1$$

$$\text{The power of 17 dividing } 23! \text{ are} = \left[\frac{23}{17}\right] = 1$$

$$\text{The power of 19 dividing } 23! \text{ are} = \left[\frac{23}{19}\right] = 1$$

$$\text{The power of 23 dividing } 23! \text{ are} = \left[\frac{23}{23}\right] = 1$$

$\therefore$ The canonical form of $23! = 2^{19} \cdot 3^9 \cdot 5^4 \cdot 7^3 \cdot 11^2 \cdot 13 \cdot 17 \cdot 19 \cdot 23$

Relation between GCD and LCM:

Theorem:

Let a and b be positive integers. Then $[a,b] = \dfrac{ab}{(a,b)}$ **(or)**

Prove that the product of gcd and lcm of any two positive integers a and b is equal to their products.

Proof:

Let $a = p_1^{a_1} p_2^{a_2} \ldots\ldots p_n^{a_n}$, $b = p_1^{b_1} p_2^{b_2} \ldots\ldots p_n^{b_n}$ be the canonical decomposition of a and b. Then

$$[a,b] = p_1^{\max\{a_1,b_1\}} p_2^{\max\{a_2,b_2\}} \ldots\ldots p_n^{\max\{a_n,b_n\}}$$

$$(a,b) = p_1^{\min\{a_1,b_1\}} p_2^{\min\{a_2,b_2\}} \ldots\ldots p_n^{\min\{a_n,b_n\}}$$

$$\Rightarrow [a,b](a,b) = p_1^{\max\{a_1,b_1\}+\min\{a_1,b_1\}} p_2^{\max\{a_2,b_2\}+\min\{a_2,b_2\}} \ldots\ldots p_n^{\max\{a_n,b_n\}+\min\{a_n,b_n\}}$$

$$= p_1^{a_1+b_1} p_2^{a_2+b_2} \ldots\ldots p_n^{a_n+b_n}$$

$$= \left(p_1^{a_1} p_2^{a_2} \ldots\ldots p_n^{a_n}\right)\left(p_1^{b_1} p_2^{b_2} \ldots\ldots p_n^{b_n}\right)$$

$$= ab$$

Hence $[a,b] = \dfrac{ab}{(a,b)}$

Problem:

1. Using (252, 360) compute [252, 360].

Since GCD of $(252,360) = 36$

$$[a,b] = \frac{ab}{(a,b)} \Rightarrow [252, 360] = \frac{252 \times 360}{36} = 2520$$

2. For positive integer n, find (n,n+1) and [n,n+1]

Soln.:

Since n and n+1 are the two consecutive integer. For any two consecutive integers are relatively primes. So (n, n+1)=1.

By formula, $[a,b] = \dfrac{ab}{(a,b)} = \dfrac{n(n+1)}{1} = n^2+n$

3. Find a positive integer a, if [a, a+1] =132.

Soln.:

We know that $[a,b] = \dfrac{ab}{(a,b)} \text{-----(1)}$

Since LCM *of* $[a, a+1]$=132 & GCD of $(a, a+1) = 1$

$(1) \Rightarrow 132 = \dfrac{a \times a+1}{1} \Rightarrow a^2 + a - 132 = 0 \Rightarrow a = -12, 11$ Since a is positive integer, $a = 11$

UNIT-IV LINEAR DIOPHANTINE EQUATIONS AND CONGRUENCES

Linear Diophantine Equation

The linear Diophantine equations are the simplest class of Diophantine equations.

The general form of a linear Diophantine equation (LDE) is two variables x and y is

$ax+by=c,$ where a,b,c are integers.

Theorem

The linear Diophantine equation $ax+by=c$ is solvable if and only if $d \mid c,$ where $d=(a,b)$. If

$x_{0,}\, y_0$ is a particular solution of the linear Diophantine equation, then all its solutions are given by

$$x=x_0+\left(\frac{b}{d}\right)t \qquad and \quad y=y_0-\left(\frac{a}{d}\right)t, \quad t\in Z$$

Proof:

Assume the linear Diophantine equation $ax+by=c$ is solvable.

To prove $d \mid c$

If $x=\alpha,\ y=\beta$ is a solution, then $\alpha a+\beta b=c$

Since $d=(a,b),\ d \mid a$ and $d \mid b$

$\Rightarrow \quad d \mid \alpha a+\beta b$

$\Rightarrow \quad d \mid c$

1. Determine whether the LDE $2x+3y+4z=5$ is solvable?

Solution:

The $\gcd(2,3,4)=1$

i.e., $(2,3,4)=1$ and $1/5$

The given LDE is Solvable.

2. Find the general solution of the LDE $15x+21y=39$

Solution:

$15x+21y=39 \Rightarrow a=15,\ b=21,\ c=39.$

$d=(15,21)$ and $d/39 \Rightarrow d=3$

So, the given LDE is solvable.

$15x+21y=39$

$\Rightarrow 5x+7y=13 \text{-------(1)}$

then $(5,7)=d=1$

$\therefore d/13$

$a=5, b=7, d=1$

We find $x_0=-3,\ y_0=4$ is a solution of (1) is

$$x=x_0+\frac{b}{d}t \quad \text{and} \quad y=y_0-\frac{a}{d}t,\quad t\in Z$$

$$x=-3+\frac{7}{1}t \quad \text{and} \quad y=4-\frac{5}{1}t,\quad t\in Z$$

$$x=-3+7t \quad \text{and} \quad y=4-5t,\quad t\in Z$$

3. Find the general solution of the LDE $6x+8y+12z=10$

Solution:

Given the LDE is $6x+8y+12z=10 \text{------(1)}$

Here $a_1=6,\ a_2=8,\ a_3=12,\ c=10$

$\therefore (a_1.a_2,a_3)=(6,8,12)=2$ and $c=10$

$\therefore \quad d=(a_1.a_2,a_3)=2$

Since $2\mid 10,\ d\mid c$

So, the given LDE is solvable.

Since $8y+12z$ is a linear combination of 8 and 12, *i*t must be a multiple of $(8,12)=4$

$\therefore \quad 8y+12z=4u \text{-------(2)}$

$\therefore (1)\Rightarrow \quad 6x+4u=10 \text{-------(3)}$

First we solve the LDE (3) in two variables x and u

Here $a=6, b=4,\ c=10$

$(a,b)=(6,4)=2$

$d=(a,b)=2$ and $c=10$

Since $2\mid 10,\ d\mid c$

So, the given LDE (3) is solvable.

We find $x_0=1,\ u_0=1$ is a solution of (3) is

$x = x_0 + \frac{b}{d}t \quad and \quad u = u_0 - \frac{a}{d}t, \quad t \in Z$

$x = 1 + \frac{4}{2}t \quad and \quad u = 1 - \frac{6}{2}t, \quad t \in Z$

$x = 1 + 2t \quad and \quad u = 1 - 3t, \quad t \in Z$

Substituting for u in (2), we get

$\therefore \qquad 8y + 12z = 4(1 - 3t)$

Since d=$\begin{pmatrix} a & b \\ 8, & 12 \end{pmatrix} = 4$ and $4 = 2.8 + (-1).12$ is a linear combination of 8 and 12.

Multiplying by $(1-3t)$, *we get*

$$4(1-3t) = 2(1-3t).8 + (-1)(1-3t).12$$
$$= (2-6t).8 + (-1+3t).12$$

$\therefore$ a solution of (2) is

$y_0 = 2 - 6t \quad$ and $\quad z_0 = -1 + 3t, \quad t \in Z$

So, the general solution of (2) is

$y = y_0 + \frac{b}{d}t' \quad and \quad z = z_0 - \frac{a}{d}t', \quad t' \in Z$

$y = 2 - 6t + \frac{12}{4}t' \quad and \quad z = -1 + 3t - \frac{8}{4}t', \quad t' \in Z$

$y = 2 - 6t + 3t' \quad and \quad z = -1 + 3t - 2t', \quad t' \in Z$

Thus the general solution of (1) is

$x = 1 + 2t,\ y = 2 - 6t + 3t',\ \ z = -1 + 3t - 2t', \quad t' \in Z$

Congruence modulo m

If an integer m ($\neq 0$) divides the difference $a - b$, we say that a is congruent to b modulo m.

(*i.e*) $a \equiv b (\mathrm{mod}\, m)$.

4. Solve the congruence $4x \equiv 5 (\mathrm{mod}\ 6)$.

Solution:

$4x \equiv 5 (\text{mod } 6)$

Here $a = 4,\ b = 5,\ m = 6$

$(a, m) = (4, 6) = 2$

$\Rightarrow 2 \nmid 5$ $(i.e)$ $(a, m) \nmid b$

$\therefore$ The congruence has no solution.

5. Show that $n^2 + n \equiv 0 (\text{mod } 2)$ for any positive integer n.

Proof:

$a \equiv b (\text{mod } k) \Rightarrow a - b \equiv km, \quad m \in z$

$a - b$ is divisible by k

$n = \text{even} = 2m$

$n^2 + n = (2m)^2 + (2m)$

$= 4m^2 + 2m$

$= 2(2m^2 + m)$

$n^2 + n$ is divisible by 2

$n = \text{odd} = 2m + 1$

$n^2 + n = (2m + 1)^2 + (2m + 1)$

$= 4m^2 + 4m + 1 + 2m + 1$

$= 4m^2 + 6m + 2$

$= 2(2m^2 + 3m + 1)$

$n^2 + n$ is divisible by 2

$\Rightarrow n^2 + n \equiv 0 (\text{mod } 2)$

6. Let $a \equiv b (\text{mod } m)$ *and* $c \equiv d (\text{mod } m)$, then prove that $ac \equiv bd (\text{mod } m)$.

Solution:

Since $a \equiv b (\text{mod } m)$ and $c \equiv d (\text{mod } m)$,

$a = b + lm$ *and* $c = d + km$ for some inegers *l and m.*

Then $ac - bd = (ac - bc) + (bc - bd)$

$= c(a - b) + b(c - d)$

$= clm + bkm$

$= (cl + bk)m$

So $ac \equiv bd (\text{mod } m)$

7. Let $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$, then prove that $a + c \equiv b + d \pmod{m}$.

Solution:

Since $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$,

$a = b + lm$ *and* $c = d + km$ for some inegers l and m.

Then $a + c = (b + lm) + (d + km)$

$= (b + d) + (l + k)m$

$= b + d \pmod{m}$

8.If $ac = bc \pmod{m}$ and $(c, m) = 1$, then prove that $a \equiv b \pmod{m}$.

Solution:

Suppose $ac \equiv bc \pmod{m}$, where $(c, m) = 1$.

Then $m \mid (ac - bc) = m \mid c(a - b)$.

we know that : *If* a and b are relatively prime, and if $a \mid bc$, then $a \mid c$.

But $(m, c) = 1$, $m \mid (a - b)$, (i.e) $a \equiv b \pmod{m}$

Complete residue system.

A set $x_1, x_2, ..., x_m$ is a complete residue system mod m if for integer y, there is one and only one x_j such that $y \equiv x_j \pmod{m}$.

9. Solve $x^7 + 1 \equiv 0 \pmod{7}$

Solution:

The complete residue system (*CRS*) *is* $\{0, 1, 2, 3, 4, 5, 6\}$

But $4 \equiv -3 \pmod{7}$

$5 \equiv -2 \pmod{7}$

$6 \equiv -1 \pmod{7}$

The CRS is $\{0, \pm 1, \pm 2, \pm 3\}$

The CRS does not satisfy the congruence $x^2 + 1 \equiv 0 \pmod{7}$

$\therefore$ The given congruence has no solution.

10.Find the remainder when 16^{53} is divided by 7.

Solution:

First reduce the base to its least residue

$16 \equiv 2 \pmod 7$.

We know that If a $\equiv b \pmod m$, then $a^n \equiv b^n \pmod m$ for any positive integer n

$16^{53} \equiv 2^{53} \pmod 7$.

Now express *a suitable power of* 2 *congruent* modulo 7 *to a number less than* 7,

$2^3 \equiv 1 \pmod 7$

$\therefore 2^{53} \equiv 2^{3(17)+2}$

$\equiv (2^3)^{17}.2^2$

$\equiv 1^{17}.4 \pmod 7$

$\equiv 4 \pmod 7$

So $16^{53} \equiv 4 \pmod 7$, by the transitive property.

Thus, when 16^{53} is divided by 7, the remainder is 4.

11. Find the remainder when $1!+2!+3!+....+300!$ is divided by 13.

Solution:

For divisibility by 13, we consider mod 13.

For $r \geq 13$, $r!$ will contain 13 as a facor.

$\therefore r! \equiv 0 \pmod{13}$

$1!+2!+3!+4!+.....+12!+.....+300!$

$\equiv 1!+2!+3!+4!+.....+12!+0+0+ \pmod{13}$

$\equiv 1!+2!+3!+4!+.....+12! \pmod{13}$

$\equiv 1+2+6+24+120+....+12! \pmod{13}$

But $2+24=26 \equiv 0 \pmod{13}$

$5! = 120 \equiv 3 \pmod{13}$

$6! = 5!6 = 3.6 \pmod{13}$

$\equiv 18 \pmod{13}$

$\equiv 5 \pmod{13}$

$7! = 6!7 = 5.7 \pmod{13}$

$\equiv 35 \pmod{13}$

$\equiv 9 \pmod{13}$

$8! = 7!8 = 9.8 \pmod{13}$

$\equiv 72 \pmod{13}$

$\equiv 7 \pmod{13}$

$9! = 8!9 = 7.9 (\text{mod} 13)$

$\equiv 63 (\text{mod} 13)$

$\equiv 11 (\text{mod} 13)$

$10! = 9!10 = 11.10 (\text{mod} 13)$

$\equiv 110 (\text{mod} 13)$

$\equiv 6 (\text{mod} 13)$

$11! = 10!11 = 6.11 (\text{mod} 13)$

$\equiv 66 (\text{mod} 13)$

$\equiv 1 (\text{mod} 13)$

$12! = 11!12 = 1.12 (\text{mod} 13)$

$\equiv 12 (\text{mod} 13)$

$1! + 2! + 3! + 4! + ... + 12! + ... + 300! \equiv 1 + 6 + 0 + 3 + 5 + 9 + 7 + 11 + 6 + 1 + 12 (\text{mod} 13)$

$\equiv 61 (\text{mod} 13) \equiv 9 (\text{mod} 13)$

$\therefore$ the remainder is 9 when $1! + 2! + 3! + 4! + ... + 12! + ... + 300!$ is divided by 13.

12. Find the remainder when 3^{181} is divided by 17 using modular exponentitation.

Solution:

$3^2 \equiv 9 (\text{mod} 17)$; $3^4 \equiv -4 (\text{mod} 17)$; $3^8 \equiv -1 (\text{mod} 17)$; $3^{16} \equiv 1 (\text{mod} 17)$

$3^{32} \equiv 1 (\text{mod} 17)$; $3^{64} \equiv 1 (\text{mod} 17)$;

$3^{128} \equiv 1 (\text{mod} 17)$

$\therefore 3^{181} = 3^{128}.3^{32}.3^{16}.3^4.3^1$

$\equiv 1.1.1.13.3 \ (\text{mod } 17)$

$\equiv 5 (\text{mod} 17)$

Thus the desired remainder is 5.

13. Find the remainder when 3^{31} is divided by 7.

$3^2 \equiv 2 (\text{mod} 7)$

$(3^2)^3 \equiv 2^3 (\text{mod} 7) = 1 (\text{mod} 7)$

$3^6 = 1 (\text{mod} 7)$

$\therefore 3^{31} = (3^6)^5.3$

$\equiv 1^5.3 \ (\text{mod } 7)$

$\equiv 3 (\text{mod} 7)$

Thus the remainder is 3.

14. Prove that $4^{2n} + 10n \equiv 1 (\text{mod } 25)$.

Solution:

$4^{2n} + 10n \equiv 1 (\text{mod } 25)$

proof by mathematical induction

$\Rightarrow n = 0$

$(4^0 + 0) - 1 = 1 - 1 = 0$

$\Rightarrow 0$ is divisible by 25

statement is true for $n = 0$.

$n = 1, \quad (4^2 + 10) - 1 = 25$

$\Rightarrow 25$ is divisible by 25

statement is true for $n = 1$.

Assume that the statement is true for $n = k$

$(ie), 4^{2k} + 10k - 1 = 25l$

Consider $4^{2k+2} + 10(k+1) - 1$

$$= 4^{2k}.16 + 10k + 10 - 1$$

$$= 16(25l - 10k + 1) + 10k + 9$$

$$= 16(25l) - 160k + 16 + 10k + 9$$

$$= 16(25l) - 150k + 25$$

$$= 25(16l - 6k + 1)$$

$$= 25(y)$$

$4^{2k+2} + 10(k+1) - 1$ is divisible by 25

Statement is true for $n = k + 1$

By principle of mathematical induction,

Statement is true for all *n*.

15. Find the remainder when $(n^2 + n + 41)^2$ is divisible by 12.

Solution:

First notice that product of four consecutive integers is divisible by 12,

$(ie), (n-1)n(n+1)(n+2) \equiv 0 (\text{mod } 12)$

$(n^2 + n + 41)^2 \equiv (n^2 + n + 5)^2 (\text{mod } 12)$

$$\equiv (n^4 + 2n^3 + 11n^2 + 10n + 25) \pmod{12}$$
$$\equiv n(n^3 + 2n^2 - n - 2) + 1 \pmod{12}$$
$$\equiv n\left[n^2(n+2) - (n+2) \right] + 1 \pmod{12}$$
$$\equiv n((n+2)(n^2 - 1) + 1 \pmod{12}$$
$$\equiv (n-1)n(n+1)(n+2) + 1 \pmod{12}$$
$$\equiv 1 \pmod{12}$$

Thus when $(n^2 + n + 41)^2$ is divided by 12, the remainder is 1.

16. Compute the remainder when 3^{247} is divisible by 25.

Solution:

We have to find the remainder when 3^{247} is divisible by 25.

We have $3^2 \equiv 9 \pmod{25}$

$$3^4 \equiv 9^2 = 81 \equiv 6 \pmod{25}$$

$$3^8 \equiv 6^2 = 36 \equiv 11 \pmod{25}$$

$$3^{16} \equiv 11^2 = 121 \equiv 21 \pmod{25}$$

$$3^{32} \equiv 21^2 \equiv 16 \pmod{25}$$

$$3^{64} \equiv 16^2 \equiv 6 \pmod{25}$$

$$3^{128} \equiv 6^2 \equiv 11 \pmod{25}$$

$$3^{247} = 3^{128+64+32+16+4+2+1}$$

$$= 3^{128}.3^{64}.3^{32}.3^{16}.3^4.3^2.3$$

$$3^{247} \equiv 11.6.16.21.6.9.3 \pmod{25}$$

$$\equiv 11\ (96)\ (21)\ (54)\ 3 \pmod{25}$$

$$\equiv 11\ (-4)\ (-4)\ (4)\ 3 \pmod{25}$$

$$\equiv 44.48 \pmod{25}$$

$\equiv(-6)\ (-2)\ (\text{mod}\,25)$

$\equiv 12\ (\text{mod}\,25)$

$\therefore$ the remainder is 12 when 3^{247} is divisible by 25.

17.Find the remainder when 3^{181} is divided by 17 using modular exponentitation.

Solution:

$3^2 \equiv 9(\text{mod}17);\ 3^4 \equiv -4(\text{mod}17);\ 3^8 \equiv -1(\text{mod}17);\ 3^{16} \equiv 1(\text{mod}17)$

$3^{32} \equiv 1(\text{mod}17);\ 3^{64} \equiv 1(\text{mod}17);\ 3^{128} \equiv 1(\text{mod}17)$

$\therefore 3^{181} = 3^{128}.3^{32}.3^{16}.3^4.3^1$

$\equiv 1.1.1.13.3\ (\text{mod}\ 17)$

$\equiv 5(\text{mod}17)$

Thus the desired remainder is 5.

18.Find the remainder when 16^{53} is divided by 7.

Solution:

First reduce the base to its least residue

$16 \equiv 2(\text{mod}\,7).$

We know that If a $\equiv b(\text{mod m})$, then $a^n \equiv b^n\ (\text{mod}\,m)$ for any positive integer n

$16^{53} \equiv 2^{53}\ (\text{mod}\,7).$

Now express *a suitable power of* 2 *congruent* modulo 7 *to a number less than* 7,

$2^3 \equiv 1\ (\text{mod}\,7)$

$\therefore 2^{53} \equiv 2^{3(17)+2}$

$\equiv (2^3)^{17}.2^2$

$\equiv 1^{17}.4(\text{mod}\,7)$

$\equiv 4(\text{mod}\,7)$

So $16^{53} \equiv 4(\text{mod}\,7)$, by the transitive property.

Thus, when 16^{53} is divided by 7, the remainder is 4.

19.Prove that p is a prime iff $(p-1)! + 1 \equiv 0(\text{mod}\ p)$.

Proof:

Suppose p is not a prime then $p = p_1 p_2$

where $1 < p_1$ & $p_2 < p - 1$

since $1 < p_1 < p_1 - 1$, we find p_1 is a factor of $(p-1)!$

(*ie*) $p_1/(p-1)!$ Also p_1/p

we are given $(p-1)!+1 \equiv 0 \pmod{p}$

$\therefore\ p\ /(p-1)!+1$

$\therefore\ p_1/(p-1)!+1$

Thus $p_1/(p-1)!+1$ & $p_1/(p-1)!$

$p_1/[(p-1)!+1]-(p-1)!$

$\therefore\ p_1/1$

which is not possible $\because p_1 > 1$

Hence p must be prime.

Linear Congruence

A congruence of the form $ax \equiv b \pmod{m}$, where m is a positive integer and a,b are integers and x is a variable, is called a linear congruence.

Chinese remainder theorem.

Let $m_1, m_2, ..., m_r$ denote r positive integers that are relatively prime in pairs and let $a_1, a_2, ..., a_r$ be any r integers. Then the congruence $x \equiv a_i \pmod{m_i}$, i = 1, 2, ..., r have common solution.

State and prove Chinese remainder theorem.

Let $m_1, m_2, ..., m_r$ denote r positive integers that are relatively prime in pairs and let $a_1, a_2, ..., a_r$ be any r integers. Then the congruence $x \equiv a_i \pmod{m_i}$, i = 1, 2, ..., r have common solution.

Proof:

First we prove the existence of the solution

Let $n = m_1.m_2.m_3...m_k$

Let $n_i = \dfrac{n}{m_i}$, $i = 1, 2, 3, ..., k.$

Since $m_1.m_2.m_3...m_k$ are pairwise relatively prime

$(n_i, m_i) = 1,\ \ i = 1, 2, 3, ..., k$

Also $n_i \equiv 0 \pmod{m_j}$, $i \neq j$

1. First we construct a solution to the linear system.

Since $(n_i, m_i) = 1$, the congruence $n_i y_i \equiv 1 \pmod{m_i}$ has a unique solution y_i, $i = 1, 2, 3, ..., k$

Let $x = a_1 n_1 y_1 + a_2 n_2 y_2 + ... + a_k n_k y_k$

Now, we will show that x is a solution of the system of congrunces.

Since $n_i \equiv 0 (\text{mod}\, m_k)$ *for* $i \neq k$, all terms except the k^{th} term in this are congruent to 0 modulo m_k

Since $n_k y_k \equiv 1 (\text{mod}\, m_k)$, we see that $x = a_k n_k y_k \equiv a_k \,(\text{mod}\, m_k)$, for $k = 1, 2, 3, ..., n$

Thus x satisfies every congruence in the system.

Hence x is a solution of the linear system.

2. Next to show that the solution is unique modulo $n = m_1 . m_2 .....m_k$.

Let x_1, x_2 be two solutions of the system

To prove $x_1 \equiv x_2 \,(\text{mod}\, n)$

Since $x_1 \equiv a_j \,(\text{mod}\, m_j)$ and $x_2 \equiv a_j \,(\text{mod}\, m_j)$, $j = 1, 2, 3, ..., k$

we have $x_1 - x_2 \equiv 0 (\text{mod}\, m_j)$

$\Rightarrow$ $m_j \mid x_1 - x_2$ for every j

Since $m_1, m_2, ..., m_k$ are pairwise ralatively prime,

$LCM[\, m_1, m_2, ..., m_k \,] = m_1, m_2, ..., m_k \mid x_1 - x_2$

$\Rightarrow$ $n \mid x_1 - x_2 \Rightarrow x_1 \equiv x_2 \,(\text{mod}\, n)$

Hence the solution is unique mod $m_1, m_2, ..., m_k$.

20. Use the Chinese remainder theorem to solve $x \equiv 1 (\text{mod}\ 3)$, $x \equiv 2 (\text{mod}\ 4)$, $x \equiv 3 (\text{mod}\ 5)$.

(OR)

Find the least positive integer that leaves the remainder 1 when divided by 3, 2 when divided by 4 and 3 when divided by 5.

Solution:

Given system is $x \equiv 1 (\text{mod}\ 3)$

$x \equiv 2 (\text{mod}\ 4)$

$x \equiv 3 (\text{mod}\ 5)$

Here $a_1 = 1, \quad a_2 = 2, \quad a_3 = 3$

$m_1 = 3, \; m_2 = 4, \quad m_3 = 5$

We find m_1, m_2, m_3 are pairwise relatively prime

Let $n = \mathrm{m}_1 m_2 m_3 = 3.4.5 = 60$

and $n_1 = \dfrac{n}{m_1} = \dfrac{3.4.5}{3} = 20$

$$n_2 = \frac{n}{m_2} = \frac{3.4.5}{4} = 15$$

$$n_3 = \frac{n}{m_3} = \frac{3.4.5}{5} = 12$$

1. We find y_1, y_2, y_3 from the congrunces

$n_1 y_1 \equiv 1 (\text{mod}\, m_1)$
$n_2 y_2 \equiv 1 (\text{mod}\, m_2)$
$n_3 y_3 \equiv 1 (\text{mod}\, m_3)$

We have $n_1 y_1 \equiv 1 (\text{mod}\, m_1)$,
$20 y_1 \equiv 1 (\text{mod}\, 3)$,
Since $20.2 \equiv 40 \equiv 1 (\text{mod}\, 3)$, we see $y_1 = 2$ is a solution

We have $n_2 y_2 \equiv 1 (\text{mod}\, m_2)$,
$15 y_2 \equiv 1 (\text{mod}\, 4)$,
Since $15.3 \equiv 45 \equiv 1 (\text{mod}\, 4)$, we see $y_2 = 3$ is a solution

We have $n_3 y_3 \equiv 1 (\text{mod}\, m_3)$,
$12 y_3 \equiv 1 (\text{mod}\, 5)$,
Since $12.3 \equiv 36 \equiv 1 (\text{mod}\, 5)$, we see $y_3 = 3$ is a solution

2. Then solution is $x \equiv a_1 n_1 y_1 + a_2 n_2 y_2 + a_3 n_3 y_3 \pmod{n}$
$\therefore \quad x \equiv 1.20.2 + 2.15.3 + 3.12.3 \pmod{60}$
$\Rightarrow \quad x \equiv 40 + 90 + 72 \pmod{60}$
$\Rightarrow \quad x \equiv 238 \pmod{60}$
$\Rightarrow \quad x \equiv 58 \pmod{60}$

$\therefore$ 58 is the unique solution $(\text{mod}\, 60)$
$\therefore$ the solution of the system is $x \equiv 58 (\text{mod}\, 60)$ and it is the unique solution.

21. Solve the congruence $x \equiv 1 (\text{mod}\, 4),\ x \equiv 0 (\text{mod}\, 3),\ x \equiv 5 (\text{mod}\, 7)$.

Solution:

Here $a_1 = 1,\ a_2 = 0,\ a_3 = 5$
$m_1 = 4,\ m_2 = 3,\ m_3 = 7$
$m = m_1 . m_2 . m_3$
$= 4.8.7$
$= 84$

$\frac{m}{m_1}=\frac{84}{4}=21,\ \frac{m}{m_2}=\frac{84}{3}=28,\ \frac{m}{m_3}=\frac{84}{7}=12$

$\left(\frac{m}{m_1},m_1\right)=(21,4)=1$

$\left(\frac{m}{m_2},m_2\right)=(28,3)=1$

$\left(\frac{m}{m_3},m_3\right)=(12,7)=1$

we know that

$\left(\frac{m}{m_j}\right)b_j=1(\text{mod}\,m_j)$

For $m_1 \Rightarrow \left(\frac{m}{m_1}\right)b_1\equiv 1(\text{mod}\,m_1)$

$(21)b_1\equiv 1(\text{mod}\,4)\Rightarrow 4/21b_1-1$

$\Rightarrow \quad 21b_1-1=4k,\quad k$ is an integer

$21\text{b}_1=1+4k$

$b_1=\frac{1+4k}{21}$

put $k=5,\quad b_1=1$

For $m_2 \Rightarrow \left(\frac{m}{m_2}\right)b_2\equiv 1(\text{mod}\,m_2)$

$(28)b_2\equiv 1(\text{mod}\,3)\Rightarrow 3/28b_2-1$

$\Rightarrow \quad 28b_2-1=3k,\quad k$ is an integer

$28\text{b}_2=1+3k$

$b_2=\frac{1+3k}{28}$

put $k=9,\quad b_2=1$

For $m_3 \Rightarrow \left(\frac{m}{m_3}\right)b_3\equiv 1(\text{mod}\,m_3)$

$(12)b_3\equiv 1(\text{mod}\,7)\Rightarrow 7/12b_3-1$

$\Rightarrow \quad 12b_3 - 1 = 7k_2, \quad k_2$ is an integer

$12b_3 = 1 + 7k_2$

$b_3 = \dfrac{1+7k_2}{12}$

put $k_2 = 5, \quad b_3 = 3$

By chinese remainder theorem,

$$x = \sum_{i=1}^{3} \left(\frac{m}{m_i} \right) a_i b_i \pmod{m}$$

$$= \left(\frac{m}{m_1} a_1 b_1 + \frac{m}{m_2} a_2 b_2 + \frac{m}{m_3} a_3 b_3 \right) \pmod{m}$$

$$= \left[(21 \times 1 \times 1) + (28 \times 0 \times 1) + (12 \times 5 \times 3) \right] \pmod{84}$$

$$= (21 + 180) \pmod{84}$$

$$= 201 \pmod{84}$$

22. Determine whether the system

$x \equiv 3 \pmod{10}; \quad x \equiv 8 \pmod{15}; \quad x \equiv 5 \pmod{84}$ has a solution and find them all if it exists.

Solution:

The first congruence $x \equiv 3 \pmod{10}$ is equivalent to the simultaneous congruences

$x \equiv 3 \pmod{2}$ -------(1)

$x \equiv 3 \pmod{5}$ --------(2)

The congruence $x \equiv 8 \pmod{15}$ is equivalent to,

$x \equiv 8 \pmod{3} - - - - - (3)$

$x \equiv 8 \pmod{5} - - - - - (4)$

The congruence $x \equiv 5 \pmod{84}$ is equivalent to,

$x \equiv 5 \pmod{3} - - - - - (5)$

$x \equiv 5 \pmod{4} - - - - - (6)$

$x \equiv 5 \pmod{7} - - - - - (7)$

The congruence (1) & (6)

$x \equiv 3 \pmod{2}$

$x \equiv 5 \pmod{4}$ reduces to $x \equiv 1 \pmod{4} - - - - - (8)$

The congruence (3) & (5)

$x \equiv 8 (\text{mod}\, 3)$

$x \equiv 5 (\text{mod}\, 3)$ reduces to $x \equiv 2 (\text{mod}\, 3) - - - - - (9)$

The congruence (2) & (4)

$x \equiv 3 (\text{mod}\, 5)$

$x \equiv 8 (\text{mod}\, 5)$ reduces to $x \equiv 3 (\text{mod}\, 5) - - - - - (10)$

From $(7) \Rightarrow x \equiv 2 (\text{mod}\, 7) - - - - - (11)$

we have solve the congruence of (8), (9), (10) & (11)

Here $a_1 = 1, \quad a_2 = 2, \quad a_3 = 3, \quad a_4 = 5$

$m_1 = 4, \; m_2 = 3, \quad m_3 = 5, \; m_4 = 7$

$m = m_1 . m_2 . m_3 . m_4$

$= 4.3.5.7$

$= 420$

$\frac{m}{m_1} = 105, \; \frac{m}{m_2} = 140, \; \frac{m}{m_3} = 84, \frac{m}{m_4} = 60$

we know that

$\left(\frac{m}{m_j} \right) b_j = 1 (\text{mod}\, m_j)$

For $m_1 \Rightarrow \left(\frac{m}{m_1} \right) b_1 \equiv 1 (\text{mod}\, m_1)$

$(105) b_1 \equiv 1 (\text{mod}\, 4) \Rightarrow 4 / 105 b_1 - 1$

$\Rightarrow \quad 105 b_1 - 1 = 4 k_1, \quad k_1$ is an integer

$105 \text{b}_1 = 1 + 4 k_1$

$b_1 = \frac{1 + 4 k_1}{105}$

put $k_1 = 26, \quad b_1 = 1$

For $m_2 \Rightarrow \left(\frac{m}{m_2} \right) b_2 \equiv 1 (\text{mod}\, m_2)$

$(140) b_2 \equiv 1 (\text{mod}\, 3) \Rightarrow 3 / 140 b_2 - 1$

$\Rightarrow \quad 140 b_2 - 1 = 3 k_2, \quad k_2$ is an integer

$140 \text{b}_2 = 1 + 3 k_2$

$$b_2 = \frac{1+3k_2}{140}$$

put $k_2 = 93, \quad b_2 = 2$

For $m_3 \Rightarrow \left(\frac{m}{m_3}\right) b_3 \equiv 1 (\text{mod}\, m_3)$

$$(84) b_3 \equiv 1 (\text{mod}\, 5) \Rightarrow 5 / 84 b_3 - 1$$

$\Rightarrow$ $84 b_3 - 1 = 5k_3, \quad k_3$ is an integer

$$84\text{b}_3 = 1 + 5k_3$$

$$b_3 = \frac{1+5k_3}{84}$$

For $m_4 \Rightarrow \left(\frac{m}{m_4}\right) b_4 \equiv 1 (\text{mod}\, m_4)$

$$(60) b_4 \equiv 1 (\text{mod}\, 7) \Rightarrow 7 / 60 b_4 - 1$$

$\Rightarrow$ $60 b_4 - 1 = 7k_4, \quad k_4$ is an integer

$$84\text{b}_4 = 1 + 7k_4$$

$$b_4 = \frac{1+7k_4}{84}$$

put $k_4 = 17, \quad b_3 = 2$

By chinese remainder theorem,

$$x = \sum_{i=1}^{4} \left(\frac{m}{m_i}\right) a_i b_i \, (\text{mod}\, m)$$

$$= \left(\frac{m}{m_1} a_1 b_1 + \frac{m}{m_2} a_2 b_2 + \frac{m}{m_3} a_3 b_3 + \frac{m}{m_4} a_4 b_4\right) (\text{mod}\, m)$$

$$= \left[(105 \times 1 \times 1) + (140 \times 2 \times 2) + (84 \times 3 \times 4) + (60 \times 5 \times 2)\right] (\text{mod}\, 420)$$

$$= (105 + 560 + 1008 + 600) \, (\text{mod}\, 420)$$

$$= 2273 (\text{mod}\, 420) = 173 (\text{mod}\, 420)$$

2x2 linear system

A 2×2 linear system is a system of linear congruences of the form,

$ax+by\equiv e(\bmod m)$

$cx+dy\equiv f(\bmod m)$

A solution of the linear system is a pair $x\equiv x_0(\bmod m), y\equiv y_0(\bmod m)$ that satisfies both congruences.

Theorem

The linear system of congruences $ax+by\equiv e(\bmod m)$ and $cx+dy\equiv f(\bmod m)$ has a unique solution if and only if $(\Delta,m)=1,$ where $\Delta\equiv ad-bc(\bmod m)$.

23. Verify that the linear system 2x+3y≡4(mod13) and 3x +4y ≡5 (mod 13) has a unique solution modulo 13.

Solution:

We know that the system has a unique solution modulo m if and only if $(\Delta,m)=1$

$$\Delta=ad-bc=\begin{vmatrix}2 & 3\\ 3 & 4\end{vmatrix}=-1\equiv 12(\bmod 13).$$

Since (12,13)=1

Therefore the system has a unique solution modulo 13.

24.Solve the linear system

$5x+6y\equiv 10(\bmod 13)$

$6x-7y\equiv 2(\bmod 13).$

Solution:

$5x+6y\equiv 10(\bmod 13)$

$6x-7y\equiv 2(\bmod 13)$

$\Rightarrow a=5, b=6, c=6, d=-7, e=10, f=2.$

$m=13,\ \Delta=ad-bc$

$=-35-36$

$=-71(\bmod 13)=7(\bmod 13)$

$(\Delta,m)=(13,1)=1.$

Hence unique solution.

$$x_0 = \Delta^{-1}\begin{vmatrix} 10 & 6 \\ 2 & -7 \end{vmatrix} (\text{mod}13) - - - - - - - (1)$$

$$y_0 = \Delta^{-1}\begin{vmatrix} 5 & 10 \\ 6 & 2 \end{vmatrix} (\text{mod}13) - - - - - - - - (2)$$

$\Delta\Delta^{-1} \equiv 1(\text{mod}13)$

$7\Delta^{-1} \equiv 1(\text{mod}13)$

$\Rightarrow \Delta^{-1} \equiv 2(\text{mod}13)$

$(1) \Rightarrow$

$$\begin{aligned} x_0 \equiv \Delta^{-1}(-70-12)(\text{mod}13) &\equiv 2(-70-12)(\text{mod}13) \\ &\equiv -8(\text{mod}13) \\ &\equiv 5(\text{mod}13) \end{aligned}$$

$(2) \Rightarrow$

$$\begin{aligned} y_0 \equiv \Delta^{-1}(10-60)(\text{mod}13) &\equiv 2(-50)(\text{mod}13) \\ &\equiv 2.2(\text{mod}13) \\ &\equiv 4(\text{mod}13) \end{aligned}$$

$\therefore x \equiv 5(\text{mod}13)$

$y \equiv 4(\text{mod}13).$

Wilson Theorem:

1. State and prove Wilson's Theorem

Statement:

If p is prime, then $(p-1)! \equiv -1 \pmod p$.

Proof :

We have to prove $(p-1)! \equiv -1 \pmod p$

When $p = 2$, $(p-1)! = (2-1)! = 1 \equiv -1 \pmod 2$.

So, the theorem is true when $p = 2$.

Now let $p > 2$ and let a be a positive integer such that $1 \le a \le p-1$.

Since p is a prime and $a < p$, $(a, p) = 1$.

Then the congruence $ax \equiv 1 \pmod p$ has a solution a' congruence modulo p.

$\therefore$ $aa' \equiv 1 \pmod p$, where $1 \le a' < p-1$

$\therefore$ a, a' are inverses of each other modulo p.

If $a' = a$, then $a \cdot a \equiv 1 \pmod p$

$\Rightarrow a^2 - 1 \equiv 0 \pmod p$

$\therefore$ $p \mid a^2 - 1 \Rightarrow p \mid (a-1)(a+1)$

$\Rightarrow p \mid a-1$ or $p \mid a+1$

Since $a < p$, if $p \mid a+1$ then $a = p-1$.

If $p \mid a-1$, then $a - 1 = 0 \Rightarrow a = 1$

$\Rightarrow a = 1$ or $p-1$ if $a = a'$

i.e., 1 and $p-1$ are their own inverses.

If $a' \neq a$, excluding 1 and $p-1$, the remaining $p-3$ residues 2, 3, 4, ..., $(p-3)$, $(p-2)$ can be grouped into $\frac{p-3}{2}$ pairs of the type a, a' such that $aa' \equiv 1 \pmod p$

Multiplying all these pairs together we get, $2 \cdot 3 \cdot 4 \ldots (p-3)(p-2) \equiv 1 \pmod p$

$\Rightarrow 1.2 \cdot 3 \cdot 4 \ldots (p-2)(p-1) \equiv p-1 \pmod p$

$(p-1)! \equiv -1 \pmod p$ (Since $p - 1 \equiv -1 \pmod p$)

Hence the theorem.

This can be rewritten as $(p-1)! + 1 \equiv 0 \pmod p$

$\Rightarrow$ $p \mid (p-1)! + 1$,

which is the result suggested by Wilson.

2. Let p be a prime and n any positive integer. Prove that $\frac{(np)!}{n!p^n} \equiv (-1)^n \pmod p$

Proof:

First, we can make an observation. Let a be any positive integer congruent to 1 modulo p. Then by Wilson's theorem , $a(a+1)\ldots(a+(p-2)) \equiv (p-1)! \equiv -1 \pmod p$

In other words, the product of the p-1 integers between any two consecutive multiples of p is congruent to -1 mod p.

Then $\frac{(np)!}{n!p^n} = \frac{(np)!}{p.2p.3p\ldots(np)}$

$$= \prod_{r=1}^{n} \left[(r-1)p+1 \right] \ldots \left[(r-1)p+(p-1) \right]$$

$$\equiv \prod_{r=1}^{n} (p-1)! (\mathrm{mod}\, p)$$

$$\equiv \prod_{r=1}^{n} (-1) (\mathrm{mod}\, p) \equiv (-1)^n (\mathrm{mod}\, p)$$

Fermat's Little Theorem:

1. State and prove Fermat's little theorem.

If p is a prime and *a* is any integer not divisible by p, then $a^{p-1} \equiv 1 (\mathrm{mod}\ p)$

Proof:

Given p is a prime and *a* is any integer not divisible by p

When an integer is divided by p, the set of possible remainders are 0, 1, 2, 3, ...,$p-1$

Consider the set of integers $1 \cdot a, 2 \cdot a, 3 \cdot a, \ldots . (p-1) \cdot a$ ----------(1)

Suppose $ia \equiv 0 (\mathrm{mod}\ p)$, then $p \mid ia$.

But $p \nmid a \ \therefore \ p \mid i$, which is impossible, since $i < p$.

$$ia \not\equiv 0 (\mathrm{mod}\ p) \ \text{for } i = 1, 2, \ldots, p-1.$$

So, no term of (1) is zero.

Next we prove they are all distinct

Suppose $ia \equiv ja (\mathrm{mod}\ p)$, where $1 \le i, j \le p-1$.

Then $(i-j)a \equiv 0 (\mathrm{mod}\ p) \Rightarrow p \mid (i-j)\, a$

Since $p \nmid a$, $p \mid i-j$ and $i, j < p \Rightarrow \mid i-j \mid < p$.

$\therefore i - j = 0 \Rightarrow i \equiv j (\mathrm{mod}\ p)$

$\therefore \quad i \neq j \Rightarrow ia \neq ja$.

This means, no two of the integers in (1) are congruent modulo p.

$\therefore$ The least residues (or remainders) of the integers $a, 2a, 3a, \ldots, (p-1)a$ modulo p are the same as the integers $1, 2, 3, \ldots, p-1$ in some order.

So, their products are congruent modulo p.

$$a \cdot 2a \cdot 3a \ldots (p-1)\, a \equiv 1 \cdot 2 \cdot 3 \ldots (p-1) (\mathrm{mod}\ p)$$

$\Rightarrow \quad 1 \cdot 2 \cdot 3 \ldots (p-1) \cdot a^{P-1} \equiv (p-1)! (\mathrm{mod}\ p)$

$\Rightarrow \quad (p-1)!\, a^{P-1} \equiv (p-1)! (\mathrm{mod}\ p)$

$\Rightarrow \quad a^{P-1} \equiv 1 (\mathrm{mod}\ p)$ (since $p \nmid (p-1)$)

The result $a^{p-1} \equiv 1 (\mathrm{mod}\ p)$ is equivalent to $a^{p} \equiv a (\mathrm{mod}\ p)$.

2. Find the remainder when 24^{1947} is divided by 17

Solution.

We have to find the remainder when 241947 is divided by 17.

Here a = 24, p = 17

We know 17 is a prime & 17|24

$\therefore$ By Fermats theorem, $24^{17-1} \equiv 1 (\mathrm{mod}\ 17)$

$\Rightarrow \quad 24^{16} \equiv 1 (\mathrm{mod}\ 17)$

$\therefore \quad (24^{16})^{121} \equiv 1^{121} (\mathrm{mod}\ 17)$

$\Rightarrow \quad 24^{1936} \equiv 1 (\mathrm{mod}\ 17)$

Now **$24^{1947} = 24^{1936+11} = 24^{1936} \cdot 24^{11}$**

$242 = 576 \equiv -2 \pmod{17}$

$\therefore \quad (242)^2 \equiv (-2)^2 \pmod{17}$

$\Rightarrow \quad 244 \equiv 4 \pmod{17}$

$(244)^2 \equiv 4^2 \pmod{17}$

$\Rightarrow \quad 248 \equiv 16 \pmod{17}$

$\equiv -1 \pmod{17}$

$2411 = 248.242.24 \equiv (-1)(-2).7 \pmod{17}$

$\equiv 14 \pmod{17}$

$\therefore \quad 241947 \equiv 14 \pmod{17}$

$\equiv 14 \pmod{17}$

∴ The remainder is 14 when 241947 is divided by 17.

Euler's Theorem:

1. State and prove Euler's theorem.

Let m be a positive integer and a be any integer such that (a, m) = 1.

Then $a^{\Phi(m)} \equiv 1 \pmod{m}$.

Proof :

Given m is a positive integer and a is any integer such that (a, m) = 1.

Let $r_1, r_2, \ldots, r_{\Phi(m)}$ **be all the positive integers < m and relatively prime to m.**

Since $r_i - r_j < m$, **clearly** $r_i \neq r_j \pmod{m}$ **if** $i \neq j$

Consider the products $ar_1, ar_2, \ldots, ar_{\Phi(m)}$

Since $(a, m) = 1, ar_i \neq ar_j \pmod{m}$ **if** $i \neq j$

we find $ar_1, ar_2, \ldots, ar_{\Phi(m)}$ **mod m are distinct.**

We now prove $(ar_i, m) = 1$

For, suppose $(ar_i, m) > 1$, **then let p be a prime factor of** $(ar_i, m) = d$.

$\therefore \quad p \mid a$ **and** $p \mid m$

$\Rightarrow \quad p \mid a$ **or** $p \mid r_i$ **and** $p \mid m$.

If $p \mid r_i$ **and** $p \nmid m$ **then,** $(r_i, m) \neq 1$, **a contradiction.**

If $p \mid a$ **and** $p \mid m$, **then** $p \mid (a, m) \Rightarrow (a, m) \neq 1$, **which is again a contradiction.**

$\therefore \quad (ar_i, m) = 1, \; i = 1, 2, 3, \ldots, \Phi(m)$

∴ the Φ(m) least residues $ar_1, ar_2, \ldots, ar_{\Phi(m)}$ **modulo m are distinct and relatively prime to m.**

So, they are the same as integers $r_1, r_2, \ldots, r_{\Phi(m)}$, **in some order modulo m.**

∴ their product $ar_1 \cdot ar_2 \cdot \ldots \cdot ar_{\Phi(m)} \equiv r_1 \cdot r_2 \cdot \ldots \cdot r_{\Phi(m)} \pmod{m}$

$\Rightarrow \quad a_{\Phi(m)} r_1 . r_2, , r_{\Phi(m)} \equiv r_1 r_2 .. r_{\Phi(m)} \pmod{m}$

Since each r_i **is relatively prime to m,** $(r_1 r_2 .. r_{\Phi(m)}, m) = 1$

We get $a^{\Phi(m)} \equiv 1 \pmod{m}$

2. Using Euler's theorem, find the remainder when 245^{1040} **is divided by 18.**

Solution.

We have to find the remainder when 2451040 is divided by 18.

Here $a = 245 = 5 \cdot 72$ **and** $m = 18 = 32 \cdot 2$, $(a, m) = 1$

Hence by Euler's theorem,

$a^{\varphi(m)} \equiv 1 \pmod{m} \Rightarrow 245^{\varphi(m)} \equiv 1 \pmod{m}$

$$\varphi(18) = \varphi(3^2 .2) = \varphi(3^2).\varphi(2) = 3^2\left(1 - \frac{1}{3}\right).1 = 6$$

But

$$\therefore \; 245^6 \equiv 1 \pmod{18}$$

$\therefore (245^6)^{173} \equiv 1^{173} (\text{mod} 18)$

$245^{1038} \equiv 1 (\text{mod} 18)$

$245^{1040} = 245^{1038+2} = 245^{1038} 245^2$

But $245 \equiv 11 (\text{mod} 18)$

$2452 \equiv 11^2$ (mod 18)

$\equiv$121 (mod 18)

$\equiv$ 13 (mod 18)

$245l040 \equiv 1 \cdot 13$ (mod 18)

$\equiv$ 13 (mod 18)

$\therefore$ The remainder is 13 when 2451040 is divided by 18.

If $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$ is the canonical decomposition of a positive integer n then derive the formula for the phi function $\phi(n)$ and use it to find $\varphi(6860)$

Proof:

To prove : If p is prime and e any positive integer then prove that $\varphi(p^e) = p^e - p^{e-1} = p^e(1-\frac{1}{p})$

$\varphi(p^e) =$ **number of positive integers** $\leq p^e$ **and relatively prime to it**

= {number of positive integers $\leq p^e$ **}-{ number of positive integers** $\leq p^e$ **and not relatively prime to it}**

The number of positive integers $\leq p^e$ **is** p^e **(because they are 1, 2, 3, ...,** p^e **)**

The number of positive integers $\leq p^e$ **and not prime to it are the various multiples of p.**

They are $p, 2p, 3p, \ldots\ldots, (p^{e-1})p$

The number of such numbers $= p^{e-1}$

Hence $\varphi(p^e) = p^e - p^{e-1} = p^e(1-\frac{1}{p})$

Since $\varphi(p^e) = p^e - p^{e-1} = p^e(1-\frac{1}{p})$ **is a multiplicative function,**

$\varphi(n) = \varphi(p_1^e p_2^e \ldots p_k^e) = \varphi(p_1^e)\varphi(p_2^e)\ldots\varphi(p_k^e)$

$= p_1^e(1-\frac{1}{p_1}) p_2^e(1-\frac{1}{p_2})\ldots p_k^e(1-\frac{1}{p_k})$

$= p_1^e p_2^e \ldots p_k^e(1-\frac{1}{p_1})(1-\frac{1}{p_2})\ldots(1-\frac{1}{p_k})$

$= n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\ldots(1-\frac{1}{p_k})$

To find $\varphi(6860)$**:**

$\varphi(6860) = \varphi(2^2).\varphi(5).\varphi(7^3)$

$= 2^2\left(1-\frac{1}{2}\right)4.7^3\left(1-\frac{1}{7}\right) = 252$

<u>Euler phi function:</u>

Let $\varphi : N \to N$ **be a function defined by**

φ(1)= 1 and

for n>1 φ(n)=the number of positive integer ≤ n and relative prime to n.

1. Prove that Euler phi function is multiplicative:

Proof:

Let m and n be positive integers such that (m, n) = 1.

To prove φ(mn) = φ(m) φ(n)

Arrange the mn integers 1, 2, 3, ..., mn in m rows of n numbers each.

1	$m+1$	$2m+1$	$3m+1$	...	$(n-1)m+1$
2	$m+2$	$2m+2$	$3m+2$	...	$(n-1)m+2$
3	$m+3$	$2m+3$	$3m+3$	...	$(n-1)m+3$
:	:	:	:	:	:
:	:	:	:	:	:
r	$m+r$	$2m+r$	$3m+r$	...	$(n-1)m+r$
:	:	:	:	:	:
rth row m	$2m$	$3m$	$4m$	...	nm

Let r be a positive integer ≤ m such that (r, m) > 1.

We will now show that no element of the rth row in the array is relatively prime to mn.

Let d = (r, m). Then d ∣ r and d ∣ m⇒ d ∣km + r for any integer k

This means d is a factor of every element in the rth row.

Thus, no element in the rth row is relatively prime to m and hence to mn if (r, m) > 1.

In other words, the elements in the array relatively prime to mn come from the rth row only if (r, m) = 1.

Since r < m and relatively prime to m, we find there are φ(m) such integers r and have φ(m) such rows.

Now let us consider the rth row where (r, m) = 1.

The elements in the rth row are r, m + r, 2m + r, ..., (n-1)m + r.

When they are divided by n, the remainders are 0, 1, 2, ..., n - 1 in some order of which φ(n) arc relatively prime to n.

Therefore, exactly φ(n) elements in the rth row are relatively prime to n and hence to mn.

Thus there are φ(m) rows containing positive integers relatively prime to mn and each row contain φ(n) elements relatively prime to it.

Hence the array contains φ(m) φ(n) positive integers ≤ mn and relatively prime to mn.

That is φ(mn) = φ(m) φ(n).

Hence φ is multiplicative function.

2. If p is prime and e any positive integer then prove that $\varphi(p^e)=p^e-p^{e-1}$ **. Also show that** $\varphi(n)=\frac{n}{2}$ **when** $n=2^k$

Proof:

$\varphi(p^e)=$ **number of positive integers** $\le p^e$ **and relatively prime to it**

= {number of positive integers $\le p^e$ **}-{ number of positive integers** $\le p^e$ **and not relatively prime to it}**

The number of positive integers $\le p^e$ **is** p^e **(because they are 1, 2, 3, ...,** p^e **)**

The number of positive integers $\le p^e$ **and not prime to it are the various multiples of p.**

They are $p, 2p, 3p, \ldots\ldots, (p^{e-1})p$

The number of such numbers $= p^{e-1}$

Hence $\varphi(p^e) = p^e - p^{e-1}$

To prove that $\varphi(n) = \frac{n}{2}$ **when** $n = 2^k$

Given $n = 2^k$

$$\therefore \varphi(n) = \varphi(2^k) = 2^k\left(1-\frac{1}{2}\right) = 2^k.\frac{1}{2} = \frac{n}{2}$$

3. Find the primes p for which $\frac{2^{p-1}-1}{p}$ **is a square.**

Solution:

Suppose $\frac{2^{p-1}-1}{p} = n^2$ **for some positive integer n. Then** $2^{p-1} - 1 = p\,n^2$

Clearly both p and n must be odd.

Let p=2k+1 for some positive integer k.

Then $2^{2k} - 1 = p\,n^2$

$\Rightarrow \quad (2^k - 1)(2^k + 1) = pn^2$

Suppose $(2^k - 1)$ **is a perfect square,** $(2^k - 1) = r^2 \;\Rightarrow\; 2^k = r^2 + 1$

$2^{p-1} = 2^{2k} = (2^k)^2 = (r^2+1)^2$

Since r≥1 and is odd, r = 2i + 1 for some integer i ≥ 0.

Then r2 = (2i + 1)2 has to be an odd number.

But r2 + 1= 2k ⇒ r2 + 1 has to divide 2.

⇒ r2 + 1 = 1 or 2.

⇒ r =0 or 1

$r = 0, \;\; 2^{p-1} = (0^2+1)^2 = 1$ **⇒ p=0 which is not possible**

$r = 1, \;\; 2^{p-1} = (1^2+1)^2 = 4$ **⇒ p=3**

Suppose $(2^k + 1)$ **is a perfect square**

$(2^k + 1) = s^2 \;\Rightarrow\; 2^k = s^2 - 1$

$2^{p-1} = (s+1)^2(s-1)^2$

Then both s -1 and s+1 both must be the factors of 2

$s - 1 = 1 \text{ or } 2, \quad \& \quad s + 1 = 1 \text{ or } 2$

$\Rightarrow s = 0,\ 1,\ 2 \text{ or } 3$

If $s = 0;\ 2^{p-1} = (0+1)^2(0-1)^2 = 1 \Rightarrow p = 1$ **which is not possible**

If $s = 1;\ 2^{p-1} = (1+1)^2(1-1)^2 = 0$ **which is not possible**

If $s = 2;\ 2^{p-1} = (2+1)^2(2-1)^2 = 9$ **which is not possible**

$If \quad s=3;\ 2^{p-1}=(3+1)^2(3-1)^2=2^6 \Rightarrow p=7$.

Thus p must be 3 or 7

Tau function:

Let n be a positive integer then

$\tau(n)$ denotes the number of positive factors of n that is $\tau(n)=\sum_{d/n}1$

Sigma function:

Let n be a positive integer then $\sigma(n)$ denotes the sum of the positive factors of n that is

$\sigma(n)=\sum_{d/n}d$

Problems:

1. Evaluate $\tau(18)$ and $\tau(23)$

Solution:

The positive divisors of 18 are 1,2,3,6,9,18 so that $\tau(18)=6$

23 being a prime , has exactly two positive divisors so $\tau(23)=2$

2. Evaluate $\sigma(12)$ and $\sigma(28)$

Solution:

The positive divisors of 12 are 1,2,3,4,6,12 so that $\sigma(12)=1+2+3+4+6+12=28$

The positive divisors of 28 are 1,2,4,7,14,28 so that $\sigma(28)=1+2+4+7+14+28=56$