# MOHAMED SATHAK A.J.COLLEGE OF ENGINEERING 

MA8551 - Algebra and Number Theory
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. $\mathrm{N}=\{1,2,3,4, \ldots . \infty\}=$ Set of all natural numbers.
2. $\mathrm{Z}=\{0, \pm 1, \pm 2, \pm 3, \pm 4, \ldots \infty\}=$ Set of all integers.
3. $\mathrm{Q}=$ Set of all rational numbers.
4. $\mathrm{R}=$ Set of all real numbers.
5. $\mathrm{C}=$ 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 $\mathrm{a} * \mathrm{~b} \in \mathrm{~A} \quad$ for all $\quad \mathrm{a}, \mathrm{b} \in \mathrm{A} \quad$ (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 $\mathrm{a}, \mathrm{b}, \mathrm{c}$ in A .

Ex. $(\mathrm{N},+)$ is a semi group.
Ex. ( N, .) is a semi group.
Ex. ( $\mathrm{N},-$ ) 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 ( $\mathrm{T}, *$ ) 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.

Mhoid: 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 $\mathrm{e} \square \mathrm{T}$, then ( $\mathrm{T},{ }^{*}$ ) 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 $\mathrm{a} * \mathrm{~b}=\mathrm{b} * \mathrm{a}$ for all $\mathrm{a}, \mathrm{b}$ in G .

1. Prove that if every element of the group is its own inverse, then $\mathbf{G}$ is abelian.

## Solution:

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

$$
\begin{aligned}
& \Rightarrow(a b)^{-1} \quad a b \quad a, b \quad G \\
& \Rightarrow b^{-1} c E^{-1} \quad a b \quad\left(\square(a \mathrm{~b})^{-1}=\mathrm{b}^{-1} \mathrm{a}^{-1}\right) \\
& \Rightarrow b=a \quad a b \quad\left(\square \mathrm{~b}^{-1}=\mathrm{b} \text { and } \mathrm{a}^{-1}=\mathrm{a}\right)
\end{aligned}
$$

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 $\mathrm{e}_{1}$ is the identity, then

$$
\mathrm{e}_{1} * \mathrm{e}_{2}=\mathrm{e}_{2} * \mathrm{e}_{1}=\mathrm{e}_{2}
$$

Suppose $\mathrm{e}_{2}$ 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 $\llbracket a b \rrbracket^{-1}=a^{-1} b^{-1} \forall a, b \in G$.

## Solution:

By closure property $\forall a, b \in G \Rightarrow a b \quad G$
Let $x=(a b)^{-1}$, then $x(a b)=e$
By associative property $\Rightarrow(x a)=b \quad e$
post multiply by $\mathrm{b}^{-1} \Rightarrow \quad(x a) \boldsymbol{b}={ }^{-1} \quad e b^{-1}$

$$
(x a)=b^{-1}
$$

post multiply by $\mathrm{a}^{-1} \Rightarrow(x a) a_{=}^{-1} \quad b^{-1} a^{-1}$

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

Assume that G is an abelian group
$\therefore(a b)^{-1}=b^{-1} a^{-1}=a^{-1} b^{-1} \quad$ ( Gisabelian) ${ }^{-}$
Conversely assume that $(a b)^{-1}=a^{-1} b^{-1} \forall a, b \in G$
To Prove : G is abelian
$a b=\left((a b)^{-1}\right)^{-1}=\left(a^{-1} b^{-1}\right)^{-1}=\left(b^{-1}\right)^{-1}\left(a^{-1}\right)^{-1}=b a$.
Thus G is abelian.
4. Prove that if every element of the group is its own inverse, then $\mathbf{G}$ is abelian.

If every element of the group is its own inverse, then $a^{-1}=a$ for all $a \in \mathrm{G}$
$\Rightarrow(a b)^{-1} \quad a \not b \quad a, b \quad G$
$\Rightarrow b^{-1} c E^{-1} \quad a b \quad\left(\square(a \mathrm{~b})^{-1}=\mathrm{b}^{-1} \mathrm{a}^{-1}\right)$
$\Rightarrow b=a \quad a b \quad\left(\square \mathrm{~b}^{-1}=\mathrm{b}\right.$ and $\left.\mathrm{a}^{-1}=\mathrm{a}\right)$
Therefore G is abelian.
5. Give an example of semi group but not a Mioid.

## 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 $\left\langle Z,{ }^{*}\right\rangle$

## Solution:

$$
\begin{aligned}
& a=a * e=a+e-2 \\
& a=a+e-2 \Rightarrow=a \quad 2
\end{aligned}
$$



## multiplication.

Solution: $I=\left[\begin{array}{ll}{[1} & 0 \\ 0 & 1\end{array} \left\lvert\,, A=\left[\begin{array}{cc}\lceil-1 & 0 \\ 0 & 1\end{array}\left|, B=\left|\begin{array}{cc}1 & 0 \\ 0 & -1\end{array}\right|\right.\right.\right.$ and $C=\left|\begin{array}{cc}-1 & 0 \\ 0 & -1\end{array}\right|\right.$
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

Eknorthat matrix multiplication is alays associative

## Claim 3: Identity property

From the above table evobserve that the matrix $\quad I \in G$ is the Identity matrix.

## Claim 4: Inverse property

From the above table vobserve that all the matrices are inverse to each other.
Hence Inverse element exists.

## Claim 5: Commutative property

From the table evhave

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

Therefore commutative property exists.

### 1.3TESN <br> Addition adulo $\mathrm{m}\left(+{ }_{\mathrm{m}}\right.$ )

let ris a positive integer. For any two positive integers a and b

$$
a+_{m} b=a+b, \text { if } a+b<m
$$

$$
a+{ }_{m} b=\quad r, \quad \text { if } a+b \square \quad m \text { where } r \text { is the reainder obtained by dividing }(a+b)
$$

with m

## Qutiplication odulo p ( $x$ p)

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

$$
a \times_{p} b=a b, \text { if } a b<p
$$

$a x_{p} b=r$, if $a b \geq p$ where $r$ is the reainder obtained by dividing (ab) with $p$.
Ex. $3 \times_{5} 4=2 \quad, \quad 5 \times_{5} 4=0 \quad, 2 \times_{5} 2=4$.

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 |

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 $+\underset{6}{\text { is associative in } G \text {. }}$

$$
\begin{gathered}
\text { for ex. }(2+\underset{6}{ } 3)++_{6} 4=5+{ }_{6} 4=3 \text { and } \\
2+\underset{6}{ }(3+\underset{6}{4})=2+1 \underset{6}{=3}
\end{gathered}
$$

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 $+\underset{6}{\text { is commutative. }}$
Hence, $(\mathrm{G},+\underset{6}{+}$ is an abelian group.

## Symmetry Group:

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

## Isometry:

An isometry of $n$-dimensional space $\mathbf{R}^{\mathbf{n}}$ is a function from $\mathbf{R}^{\mathbf{n}}$ onto $\mathbf{R}^{\mathbf{n}}$ that preserves distance.
Note: More precisely, $\pi$ is an isometry from $\mathbb{R}^{n}$ to $\mathbb{R}^{n}$ if for all $x, y \in \mathbb{R}^{*}$ we have
$d(x, y)=d(\pi(x), \pi(y))$
where $d$ is a metric on $\mathbb{K}^{n /}$.

## Dihedral Groups

The symmetries of a regular n --gon form the dihedral group, $\left\langle D_{n},\right\rangle$, which consists of 2 n permutations.


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

1. Let $\mathbf{G}$ be the set of all rigid motions of a equilateral triangle. Identify the elements of $\mathbf{G}$.

Show that it is a non-abelian group of order six.
Proof:
Consider an equilateral triangle with vertices named as $1,2,3$.
Let $\pi_{0}, \pi_{1}, \pi_{2}$ 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 $120^{\circ}, 240^{\circ}, 360^{\circ}$ respectively.
These rotations are called rigid motions of the triangle and are given by $\left.\left.2_{0}=\left(\begin{array}{lll}1 & 2 & 3\end{array}\right) \quad \begin{array}{lll}1 & 2 & 3\end{array}\right), \quad \begin{array}{lll}1 & 2 & 3\end{array}\right)$.


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.
$r_{1}=\left(\begin{array}{lll}1 & 2 & 3 \\ 2 & 1 & 3\end{array}\right), \quad{ }_{2}=\left(\begin{array}{lll}1 & 2 & 3\end{array}\right) \quad, \quad r_{3}=\left(\begin{array}{lll}1 & 2 & 3\end{array}\right)$,


Let $\mathrm{G}=\left\{\pi_{0}, \pi_{1}, \pi_{2}, \mathrm{r}_{1}, \mathrm{r}_{2}, \mathrm{r}_{3}\right\}$.
Define binary operations on G as follows

$$
0_{1} r_{1}=\left(\begin{array}{lll}
1 & 2 & 3 \\
3 & 2 & 1
\end{array}\right)=\mathrm{r}_{3} \in \mathrm{G}
$$

Cayley's table for G is given by

|  | $\pi_{0}$ | $\pi_{1}$ | $\pi_{2}$ | $\mathrm{r}_{1}$ | $\mathrm{r}_{2}$ | $\mathrm{r}_{3}$ |
| :--- | :--- | :--- | :--- | :--- | :--- | :--- |
| $\pi_{0}$ | $\pi_{0}$ | $\pi_{1}$ | $\pi_{2}$ | $\mathrm{r}_{1}$ | $\mathrm{r}_{2}$ | $\mathrm{r}_{3}$ |
| $\pi_{1}$ | $\pi_{1}$ | $\pi_{2}$ | $\pi_{0}$ | $\mathrm{r}_{3}$ | $\mathrm{r}_{1}$ | $\mathrm{r}_{2}$ |
| $\pi_{2}$ | $\pi_{2}$ | $\pi_{0}$ | $\pi_{1}$ | $\mathrm{r}_{2}$ | $\mathrm{r}_{3}$ | $\mathrm{r}_{1}$ |
| $\mathrm{r}_{1}$ | $\mathrm{r}_{1}$ | $\mathrm{r}_{2}$ | $\mathrm{r}_{3}$ | $\pi_{0}$ | $\pi_{1}$ | $\pi_{2}$ |
| $\mathrm{r}_{2}$ | $\mathrm{r}_{2}$ | $\mathrm{r}_{3}$ | $\mathrm{r}_{1}$ | $\pi_{2}$ | $\pi_{0}$ | $\pi_{1}$ |
| $\mathrm{r}_{3}$ | $\mathrm{r}_{3}$ | $\mathrm{r}_{1}$ | $\mathrm{r}_{2}$ | $\pi_{1}$ | $\pi_{2}$ | $\pi_{0}$ |

From the table it is clear that G is a group.
Note that ${ }_{2}{ }_{2} r_{1}=r_{2}$ and $r_{1}{ }^{0}{ }_{2}=r_{3}$
$\therefore]_{2} r_{1} \neq r_{1}{ }_{2}$, G is not an abelian group of order six.

Subgroup :
Let G be a group and $0 \neq H \subseteq G$. If H is a group under the same binary operation of G then H is binary subgroup of G.
Example:

$$
H=\{0,2,4\} \text { or } K=\{0,3\} \text { are the proper subgroups of }\left(Z_{6},+\right) \text {. }
$$

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

## Solution:

## Necessary Condition:

Let us assume that $H$ is a subgroup of G . Since $H$ itself a group, ehave if $a, b \in H$ implies $a^{*} b \in H$

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

## Sufficient Condition:

Let $a^{*} b^{-1} \in H$, for $a^{*} b \in H$
Claim 1: Identity property
If $a \in H$, hich implies $\quad a * a^{-1}=e \in H$
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 issociative.
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 twsubgroups of a group $G$. eneed to prove that $\quad A \square B$ is a subgroup.
(i.e.) It is enough to prove that $A \square B \neq \mathrm{E} \quad$ and $a, b \in A \square B \Rightarrow a * b \in \quad A \square B$.

Since $A$ and $B$ are subgroups of G , the identity element $e \in A$ and $B$.
$\therefore A \square B \neq \square$
Let
$a, b \in A \square B \Rightarrow a \nexists \quad A \quad$ and $a, b \in B$
$\Rightarrow a^{*} b \in \quad A$ and $a^{*} b^{-1} \in B$
$\Rightarrow a^{*} b \bar{\epsilon}^{-1} \quad A \square B$
Hence $A \square B$ is a subgroup of G .

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

Consider the folloing example,
Consider the group $(Z,+)$, here $\quad Z$ is the set of all integers and the operation + represents usual addition.

Let $A=2 Z=\{0, \pm 2, \pm 4, \pm 6, \ldots\}$ and $B=3 Z=\{0, \pm 3, \pm 6, \pm 9, \ldots\}$.
Here $(2 Z,+)$ and $(3 Z,+)$ are both subgroups of $(Z,+)$
Let $H=2 Z \square 3 Z=\{0, \pm 2, \pm 3, \pm 4, \pm 6, \ldots\}$
Note that $2,3 \in H$, but $2+3=5 \notin H \Rightarrow \neq 5 \quad 2 Z] 3 Z$
(i.e.) $2 Z \square 3 Z$ is not closed under addition.

Therefore $2 Z \square 3 Z$ is not a group
Therefore $(\mathrm{H},+)$ is not a subgroup of $(\mathrm{Z},+)$.

Cyclic group:
A group $\left(\mathrm{G},{ }^{*}\right)$ is said to be cyclic if there exists an element $\mathrm{a} \in \mathrm{G}$ 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 $\langle i$.

## 1. Show that every cyclic group is abelian.

Let $\left(G,{ }^{*}\right)$ be a cyclic group with ' $a$ ' as generator

$$
\therefore \forall x, y \in G \Rightarrow x \quad a^{m} \Rightarrow y \quad a_{0}^{n} * x \Rightarrow y \quad a^{m} \quad e^{n} \quad a^{m+n}=a^{n+m}=y x .
$$

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

The element 3 is a cyclic generator since
$31 \bmod 7=3$
$32 \bmod 7=9 \bmod 7=2$
$3^{3} \bmod 7=\left(3^{2} \cdot 3\right) \bmod 7=(2 \cdot 3) \bmod 7=6 \bmod 7=6$
$3^{4} \bmod 7=\left(3^{3} \cdot 3\right) \bmod 7=(6 \cdot 3) \bmod 7=18 \bmod 7=4$
$3^{5} \bmod 7=\left(3^{4} \cdot 3\right) \bmod 7=(4 \cdot 3) \bmod 7=12 \bmod 7=5$
$3^{6} \bmod 7=\left(3^{5} \cdot 3\right) \bmod 7=(5 \cdot 3) \bmod 7=15 \bmod 7=1$
whereas the element 4 is not a generator but only generates a the cyclic subgroup $\{1,2,4\}$ of $Z_{7}^{*}$ since

$$
\begin{aligned}
& 4^{1} \bmod 7=4 \\
& 4^{2} \bmod 7=16 \bmod 7=2 \\
& 4^{3} \bmod 7=\left(4^{2} \cdot 4\right) \bmod 7=(2 \cdot 4) \bmod 7=1
\end{aligned}
$$

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 ( $\mathrm{G}, *$ ) be the cyclic group generated by an element $\mathrm{a} \in \mathrm{G}$ and let H be the subgroup of G .
Claim: H is cyclic
If $\mathrm{H}=\mathrm{G}$ or $\{\mathrm{e}\}$ 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 $\mathrm{a}^{-\mathrm{r}} \in \mathrm{H}$.

Let " $m$ " be the smallest positive integer such that $\mathrm{a}^{\mathrm{m}} \in \mathrm{H} . \quad$ (1)
Let $\mathrm{a}^{\mathrm{n}}$ be any arbitrary element of H . Let q be the quotient and r be the remainder when n is divided by $m$.

Then $\mathrm{n}=\mathrm{qm}+\mathrm{r}$ where $0 \leq \mathrm{r}<\mathrm{m}$.
Now $\mathrm{a}^{\mathrm{n}}=\mathrm{a}^{\mathrm{qm}+\mathrm{r}}=\left(\mathrm{a}^{\mathrm{m}}\right)^{\mathrm{q}} \cdot \mathrm{a}^{\mathrm{r}}$

$$
a^{r}=\left(a^{m}\right)^{-q} \cdot a^{n}=a^{n-m q} .
$$

Since $\mathrm{a}^{\mathrm{m}} \in \mathrm{H},\left(\mathrm{a}^{\mathrm{m}}\right)^{\mathrm{q}} \in \mathrm{H}$ by closure property
$a^{m q} \in H$
$\left(\mathrm{a}^{\mathrm{mq}}\right)^{-1} \in \mathrm{H}$, by existence of inverse, as H is a subgroup
$\mathrm{a}^{-\mathrm{mq}} \in \mathrm{H}$
Since $a^{n} \in H$ and $a^{-m q} \in H$
$\mathrm{a}^{\mathrm{n}-\mathrm{mq}} \in \mathrm{H}$
$\therefore \mathrm{a}^{\mathrm{T}} \in \mathrm{H}$
By (1) \& (2), we get $\mathrm{r}=0, \therefore \mathrm{n}=\mathrm{mq}$

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

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 $\mathrm{a}^{\mathrm{m}}$.

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

Proof:
Let $\mathrm{O}(\mathrm{G})=\mathrm{p}$, where p is a prime number.
Let $a(\neq e) \in G$.
Consider a subgroup generated by a.
Let $H=a$
$\Rightarrow O(H) \quad 1\left[\begin{array}{lllll}\square H & a \in a & H \& a l \boxplus e=H & \theta(H) & 1\end{array}\right]$
Since H is a subgroup of G , then by Lagrange's theorem,
$\mathrm{O}(\mathrm{H}) / \mathrm{O}(\mathrm{G}) \quad \Rightarrow \mathrm{O}(\mathrm{H}) / \mathrm{p}$
$\Rightarrow O(H) \quad 1$ or $p[\square p$ 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, $\therefore \mathrm{G}$ is a cyclic group.

## COSETS:

If H is a sub group of $(\mathrm{G}, *)$ and $\mathrm{a} \in \mathrm{G}$ then the set
$H a=\{h * a \mid h \in H\}$ is called a right coset of $H$ in $G$.
Similarly $\quad \mathrm{aH}=\{\mathrm{a} * \mathrm{~h} \mid \mathrm{h} \in \mathrm{H}\}$ 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 $\left.G=Z_{12},{ }_{12}\right]$, Find the left cosets $\boldsymbol{f} \quad H=[0],[4],[8]$ and show that the distinct left cosets of $\mathbf{H}$ forms a partition of $\mathbf{G}$.

$$
\begin{aligned}
& Z_{12}=\{[0],[1],[2],[3],[4],[5],[6],[7],[8],[9],[10],[11]\} ; \quad H=\{[0],[4],[8]\} \\
& {[0]+H=\{[0],[4],[8]\}=H=[4]+H=[8]+H} \\
& {[1]+H=\{[1],[5],[9]\}=[5]+H=[9]+H} \\
& {[2]+H=\{[2],[6],[10]\}=[6]+H=[10]+H} \\
& {[3]+H=\{[3],[7],[11]\}=[7]+H=[11]+H} \\
& \therefore G=H \cup([1]+H) \cup([2]+H) \cup([3]+H)
\end{aligned}
$$

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 $h_{1}, h_{2}, h_{3}, \ldots, h_{m}$ are the m distinct elements of $H$
For $x \in G$, the right coset of $H$ is defined by $H x=\{h \underset{1}{x}, h \underset{2}{x}, \underset{3}{x}, \ldots \ldots . . h \underset{m}{x}\}$.
Since there is a one to one correspondence between $H$ and $H x$, the members of $H x$ are distinct.

Hence, each right coset of $H$ in $G$ has $m$ distinct members.
Wknow 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.) $G=H x_{1} \square H x_{2} \square H x_{3} \square \ldots \square x_{k}$

$$
\begin{aligned}
& O(G)=O\left(H x_{1}\right)+O\left(H x_{2}\right)+O\left(H x_{3}\right)+\ldots+O\left(H x_{k}\right) \\
& n=m+m+m+\ldots m \quad(k \text { times })
\end{aligned}
$$

$$
\begin{aligned}
& \qquad \frac{O(G)}{O(H)}=k \\
& \text { Hence } O(H) \text { divides } O(G)
\end{aligned}
$$

3. Let $G$ be a group subgroups $H$ and $K$. If $|G|=660,|K|=66$ and $K \subset H \subset G$, what are the possible values of $|\mathrm{H}|$ ?
$\mathrm{O}(\mathrm{K})<\mathrm{O}(\mathrm{H})<\mathrm{O}(\mathrm{G})$ and $\mathrm{O}(\mathrm{K})$ divides $\mathrm{O}(\mathrm{H})$ and $\mathrm{O}(\mathrm{H})$ divides $\mathrm{O}(\mathrm{G})$.
$\mathrm{O}(\mathrm{K})=|\mathrm{K}|=66=2 \cdot 3 \cdot 11$.
$\mathrm{O}(\mathrm{G})=|\mathrm{G}|=660=2^{2} \cdot 3 \cdot 5 \cdot 11$.
$|\mathrm{K}|$ divides $|\mathrm{H}|$ and $|\mathrm{K}|<|\mathrm{H}|$
$\Rightarrow|\mathrm{H}|=x|\mathrm{~K}|=x(2 \cdot 3 \cdot 11)$, with $x>1$
$|\mathrm{H}|$ divides $|\mathrm{G}|$ and $|\mathrm{H}|<|\mathrm{G}|$
$\Rightarrow|\mathrm{G}|=\mathrm{y}|\mathrm{H}|=y x$ (2.3.11), with $y>1$
$\Rightarrow 660=y x(2.3 .11)$
$2^{2} \cdot 3 \cdot 5 \cdot 11=y x(2.3 .11)$
$2.5=y x$, with $x>1, y>1$
$\Rightarrow x=2$ or $x=5$
Nen $\quad x=2 \quad \Rightarrow|\mathrm{H}|=2(2.3 .11)=132$
MEn $\quad x=5 \quad \Rightarrow|H|=5(2.3 .11)=330$.
Normal Subgroup :
A subgroup ( $\mathrm{N},{ }^{*}$ ) of a group ( $\mathrm{G},{ }^{*}$ ) is said to be a normal subgroup of G, If for every $\mathrm{g} \in \mathrm{G}$ and $\mathrm{n} \in \mathrm{N}$, $g * n * g^{-1} \in N$.
4. Prove that intersection of any two normal subgroups of a group ( $\mathrm{G},{ }^{*}$ ) is a normal subgroup of a group ( $\mathrm{G},{ }^{*}$ ).

## Solution:

Let G be the group and $H$ and $K$ are the normal subgroups of G .
Since $H$ and $K$ are normal subgroups of
$\Rightarrow H$ and $K$ are subgroups of G
$\Rightarrow H \square K$ is a subgroup of G .
Nowhave to prove $H \square K$ is normal
Since $e \in H$ and $e \in K \Rightarrow \in e H \square K$.
Thus $\mathrm{H} \cap \mathrm{K}$ is nonempty.
Let $x \in G$ and $h \in H \square K$
$x \in G$ and $h \in H, h \in K$
$x \in G, h \in H$ and $x \in G, h \in K$

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

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

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

Quotient group or Factor group:
If $\left(N,{ }^{*}\right)$ is a normal subgroup of $\left(G,{ }^{*}\right)$ then the group $(\mathrm{G} / \mathrm{N}, \oplus)$ is called the quotient group or factor group of G by N or quotient group modulo N .

Group Homomorphism:
Let ( $\mathrm{G}, *$ ) and $(S, \square$ ) be two groups. A mapping f : $\mathrm{G} \rightarrow \mathrm{S}$ is said to be a group homomorphism if for any $\mathrm{a}, \mathrm{b} \in \mathrm{G}$,

$$
f(\mathrm{a} * \mathrm{~b})=f(\mathrm{a}) \square f(\mathrm{~b}) .
$$

Example: Consider $f:\left(R^{+},.\right) \rightarrow(R, \quad)$ where $f(\mathrm{x})=\log _{10}(\mathrm{x})$
for any $\mathrm{a}, \mathrm{b} \in \mathrm{R}^{+}, f(\mathrm{a} \cdot \mathrm{b})=\log _{10}(\mathrm{ab})=\log _{10}(\mathrm{a})+\log _{10}(\mathrm{~b})=f(\mathrm{a})+f(\mathrm{~b})$.
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 $(\boldsymbol{G}, *) \rightarrow(\boldsymbol{G}+, \quad)$ be groups with e' as the identity eleemt of $\quad \mathrm{G}^{\prime}$. Let f : $\mathrm{G} \rightarrow \mathrm{G}^{\prime}$ be a homomorphism. The kernel of $f$ is the set of all elements of $G$ which are mapped onto $e^{\prime}$ and is denoted by $\operatorname{ker} f$.
$\operatorname{Ker} f=\left\{x \in G \notin(x)=e^{\prime}\right\}$

1. Consider two groups $G$ and $G^{\prime}$ where $G=\{Z,+\}$ and $G^{\prime}=\left\{z^{m} / m=0, \pm 1, \pm 2, \pm 3, \ldots, \square\right\}$. Let
 homomorphism.
? $(m)=2^{m}$ where $m \in \mathrm{Z}$
$\therefore$ ® $(m+r)=2^{m+r}=2^{m} \rrbracket 2^{r}=$ ( $m$ ) $(r)$
Hence ? is homomorphism.
2. Let $f:(G, *) \rightarrow\left(G+^{\prime}, \quad\right)$ be an isomorphism. If $G$ is an abelian group then prove that $G^{\prime}$ is also an abelian group.
Let $a^{\prime}, b^{\prime} \in G^{\prime}$.
Then there exists $a, b \in G$,suchthat $f(\mathrm{a})=a^{\prime} \& f(\mathrm{~b})=b^{\prime}$
$a^{\prime}+b^{\prime}=f(a)+f(\mathrm{~b})=f(a * \mathrm{~b})=f(\mathrm{~b} * a)=f(\mathrm{~b})+f(a)=b^{\prime}+a^{\prime}$
Hence $G^{\prime}$ is an abelian group.
3. Let $\mathrm{f}: \mathbf{G} \rightarrow \mathbf{H}$ be a homomorphism from the group ( $\mathbf{G}, *$ ) to the group ( $\mathbf{H}, \Delta$ ). Prove that the kernel of $f$ is a normal subgroup of $G$.
Proof:
Let K be the Kernel of the homomorphism g. That is $K=\left\{x \in G \mid g(x)=e^{\prime}\right\}$ here $\quad e^{\prime}$ the identity element of H. is
Let $x, y \in K$. Now
$g\left(x * y^{-1}\right)=g(x) \Delta g\left(y^{-1}\right)=g(x) \Delta[g(y)]^{-1}=e^{\prime} \Delta\left(e^{\prime}\right)^{-1}=e^{\prime} \Delta e^{\prime}=e^{\prime}$
$x * y^{-1} \in K$
Therefore K is a subgroup of G . Let
$x \in K, f \in G$
$g\left(f * x * f^{-1}\right)=g(f)^{*} g(x) * g\left(f^{-1}\right)=g(f) e^{\prime}[g(f)]^{-1}=g(f)[g(f)]^{-1}=e^{\prime}$
$\therefore \quad f^{*} x * f^{-1} \in K$
Thus K is a normal subgroup of G .
4. Let $(G, \square),\left(\mathbf{H},{ }^{*}\right)$ be groups with respective identities $\mathbf{e}_{\mathbf{G}}, \mathbf{e}_{\mathbf{H}}$.If $f: \mathbf{G} \rightarrow \mathbf{H}$ is a homomorphism, then show that
(a) ) $f\left(e_{G}\right)=e_{H}$
(b) $f\left(a^{-1}\right)=[f(a)]^{-1} \forall a \in G$
(c ) $f\left(a^{n}\right)=[f(a)]^{n} \forall a \in G$ and all $n \in Z$
(d) $f(\mathrm{~S})$ is a subgroup of H for each subgroup S of G .

## Proof:

(a) $\mathrm{e}_{\mathrm{H}} * \mathrm{f}\left(\mathrm{e}_{\mathrm{G}}\right)=\mathrm{f}\left(\mathrm{e}_{\mathrm{G}}\right)=\mathrm{f}\left(\mathrm{e}_{\mathrm{G}} \square \mathrm{e}_{\mathrm{G}}\right)=\mathrm{f}\left(\mathrm{e}_{\mathrm{G}}\right) * \mathrm{f}\left(\mathrm{e}_{\mathrm{G}}\right)$

$$
\therefore \mathrm{e}_{\mathrm{H}}=\mathrm{f}\left(\mathrm{e}_{\mathrm{G}}\right) \text {, by right cancellation law }
$$

(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 $f\left(a * a^{-1}\right)=f\left(e_{G}\right)$

$$
f(a) \square f\left(a^{-1}\right)=e_{H}
$$

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

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

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

Case(i): if $\mathrm{n}=0$ then $\begin{gathered}a^{n}=a^{0}=e_{G} \\ f\left(a^{0}\right)\end{gathered}=\underset{G}{=} f(e)=e \quad[f(a)]^{0}$

$$
\Rightarrow f\left(a^{n}=[f(a)]^{n}\right.
$$

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

$$
a^{n}=a \rrbracket a \rrbracket a \rrbracket \quad a \text { ( } n \text { times) }
$$

$$
\begin{aligned}
f\left(a^{n}\right) & =f(a \rrbracket a \square a \rrbracket \quad a) \text { (n times) } \\
& =f(a) * f(a) * f(a) * \square * f(a) \\
& =[f(a)]^{n}
\end{aligned}
$$


$\therefore f\left(a^{n}\right)=[f(a)]^{n} \forall a \in G$ and all $n \in Z$
(d) If $S$ is a subgroup of $G$, then $S \neq \phi$, so $f(S) \neq \phi . \quad$ 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
$\therefore a \square b \in S$,
$f(a) * f(b)=f(a \square b) \in f(S)$
$\Rightarrow * x \in y \quad f(S)$, so $f(S)$ is closed
Finally,

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

$\square a \in S \Rightarrow a \in \quad S \& f\left[a^{-1} \in\right] \quad f(S)$
$x^{-1} \in f(S)$
$\therefore f(\mathrm{~S})$ is a subgroup of H for each subgroup S of G .

## 5. State and prove Fundamental Theorem of Group Homomorphism.

## Statemt :

Let $\left(\mathrm{G},{ }^{*}\right)$ and $(\mathrm{H}, \Delta)$ be two groups. Let $g: G \rightarrow H$ be a honmrphiswith kernel K . Then $G / K$ is isomphic to $\mathrm{H}(\mathrm{g}(\mathrm{G}) \subseteq \mathrm{H})$.

## Proof:

Let $g: G \rightarrow H$ be a hoommphisfrime group
$(G, *)$ to the group $(H, \Delta)$
Then $K=\operatorname{ker}(\mathrm{g})=\left\{x \in G / g(x)=e^{1}\right\}$ is a norad sub-group of $\quad(G, *)$
Also we know that the quotient set $(G / K, \otimes)$ is a group.
Define ? : $G \not K \rightarrow H \quad$ is apping frorthe group $\quad(G / K, \otimes)$ to the group $(H, \Delta)$ given by
( $3(K a)=g(a), \quad$ for any $a \in G$.
Type your text
Since if $K a=K b$

$$
\begin{aligned}
& \Rightarrow a * b \stackrel{-1}{\epsilon} \quad K \\
& \Rightarrow g\left(a^{*} b=\frac{-1}{=}\right) \quad e^{\prime} \\
& \Rightarrow g(\mathbb{A}) \quad g\left(b^{-\frac{1}{=}}\right) \quad e^{\prime} \\
& \Rightarrow g(\Delta) \quad g(b \Delta) \quad g(\nexists) \Delta e^{\prime} \quad g(b) \\
& \Rightarrow g(a \Delta) \quad \mathrm{e}^{\prime} \quad g(b) \\
& \Rightarrow g(a)=g(b)
\end{aligned}
$$

? is well defined.
Clai:m is honmrphism
Let $K a, k b \in G$.
Now,
? $(K a \otimes K b)=$ ? $[K(a * b)]$
$=g(a * b)$
$=g(a) \Delta g(b)$

$$
=?(K a) \Delta \square(K b)
$$

$\therefore$ is a hommphism
Clai:m is one-to-one.
If $]^{2}(K a)=$ ( $K b$ )
then $g(a)=g(b)$

$$
\begin{aligned}
\Rightarrow & g(\mathbb{Z}) \quad g\left(b^{-1}\right) \quad g(\mathbb{Z}) \quad g\left(b^{-1}\right) \\
& g\left(a^{*} b^{-1}\right)=g\left(b^{*} b^{-1}\right)=g(e)=e^{\prime}
\end{aligned}
$$

$\therefore a * b^{-1} \in k \Rightarrow k=a \quad k b$
$\therefore$ ? is one-to-one.
Claim: ? is onto.
Let $y$ be any elemt of $H$.
Since $g: G \rightarrow H$ is hommphisfrora to H .
Therefore there exists an elemnt $\quad a \in G$ such that $g(a)=y$
$\therefore$ For every $a \in G, K a \in G \not K$
we get ? $(K a)=g(a)$ for all $g(a)=y \in H$
$\therefore$ ? is onto.

$$
\therefore \llbracket: G / K \rightarrow H \text { is an isomrphism } \quad G / K \cong H
$$

## 6. State and prove Cayley's theorem.

## Statemt :

Every finite group $\mathbf{G}$ of order $\mathbf{n}$ is isomphic to a perntation group of degree $\mathbf{n}$.

## Proof:

Let $O(G)$ be finite say $n$ and $a \in G$. Define $f_{a}: G \rightarrow G$ as $f_{a}(x)=a x \forall x \in G$
To prove $f_{a}$ is bijection
Consider $\mathrm{f}_{\mathrm{a}}(\mathrm{x})=\mathrm{f}_{\mathrm{a}}(\mathrm{y})$
$\Rightarrow \mathrm{ax}=\mathrm{ay} \Rightarrow \mathrm{x}=\mathrm{y} \Rightarrow \mathrm{f}_{\mathrm{a}}$ is one to one
For any $g \in G$, there exists an elemnt $a, x \quad \in G$ such that $g=a x=f_{a}(x)$
Thus for every iage in $G$, there is a pre-iage in $G \quad \Rightarrow f_{a}$ is onto
Since G has n elemts, $\mathrm{f} a$ is just the perntation of n -sybols
Define $\mathrm{G}^{\prime}=\left\{\mathrm{f}_{\mathrm{a}} / \mathrm{a} \in \mathrm{G}\right\}$
To prove $\mathrm{G}^{\prime}$ is a group under coposition

## (i) Closure property

$$
\begin{aligned}
\left(\mathrm{f}_{\mathrm{a}}{ }^{\circ} \mathrm{f}_{\mathrm{b}}\right)(\mathrm{x}) & =\mathrm{f}_{\mathrm{a}}\left[\mathrm{f}_{\mathrm{b}}(\mathrm{x})\right] \\
& =\mathrm{f}_{\mathrm{a}}(\mathrm{bx}) \\
& =\mathrm{abx}=\mathrm{f}_{\mathrm{ab}}(\mathrm{x})
\end{aligned}
$$

Since $a, b \in G, a b \in G \Rightarrow f_{a b} \in G^{\prime}$
Therefore it has the closure property.

## (ii) Associative property:

$$
\begin{aligned}
\left.\mathrm{f}_{\mathrm{a}}{ }^{\circ}\left(\mathrm{f}_{\mathrm{b}}{ }^{\circ} \mathrm{f}_{\mathrm{c}}\right)\right)(\mathrm{x}) & =\mathrm{f}_{\mathrm{a}}\left[\left(\mathrm{f}_{\mathrm{b}} \circ \mathrm{f}_{\mathrm{c}}\right)(\mathrm{x})\right] \\
& =\mathrm{f}_{\mathrm{a}}\left[\mathrm{f}_{\mathrm{b}}\left(\mathrm{f}_{\mathrm{c}}(\mathrm{x})\right)\right] \\
& =\mathrm{f}_{\mathrm{a}}\left[\mathrm{f}_{\mathrm{b}}(\mathrm{cx})\right] \\
& =\mathrm{f}_{\mathrm{a}}(\mathrm{bcx})
\end{aligned}
$$

$$
=\mathrm{abcx}
$$

Thus $\left(f_{a}{ }^{\circ} \mathrm{f}_{\mathrm{b}}\right)^{\circ} \mathrm{f}_{\mathrm{c}}=\mathrm{f}_{\mathrm{a}}{ }^{\circ}\left(\mathrm{f}_{\mathrm{b}}{ }^{\circ} \mathrm{f}_{\mathrm{c}}\right)$
Therefore it has the associative property.

## (iii)Identity elemt:

Consider $\left(\mathrm{f}_{\mathrm{a}}{ }^{\circ} \mathrm{f}_{\mathrm{e}}\right)(\mathrm{x})=\mathrm{f}_{\mathrm{a}}\left[\mathrm{f}_{\mathrm{e}}(\mathrm{x})\right]$

$$
=f_{a}(e x)=f_{a}(x)
$$

$\Rightarrow \mathrm{f}_{\mathrm{e}}$ is the identity elemt
(iv) Inverse elemt:

$$
\begin{aligned}
\left(f_{a} \square f_{a^{-1}}\right)(\mathrm{x}) & =f_{a}\left[f_{a^{-1}}(\mathrm{x})\right] \\
& =f_{a}\left(\mathrm{a}^{-1} \mathrm{x}\right) \\
& =a a^{-1} x=e x=f_{e}(x)
\end{aligned}
$$

$f_{a^{-1}}$ is the inverse of $f_{a}$
Thus $\left(\mathrm{G}^{\prime},{ }^{\circ}\right)$ is a group
Define $\varphi: G \rightarrow G^{\prime}$ by $\varphi(\mathrm{a})=\mathrm{f}_{\mathrm{a}}$ for all $\mathrm{a} \in \mathrm{G}$.
(i) $\varphi$ is one to one

Consider $\varphi(\mathrm{a})=\varphi(\mathrm{b})$
$\Rightarrow \mathrm{f}_{\mathrm{a}}=\mathrm{f}_{\mathrm{b}}$
$\Rightarrow \mathrm{f}_{\mathrm{a}}(\mathrm{x})=\mathrm{f}_{\mathrm{b}}(\mathrm{x})$
$\Rightarrow \mathrm{ax}=\mathrm{bx}$
$\Rightarrow \mathrm{a}=\mathrm{b}$
Thus $\varphi$ is one to one
ii) $\varphi$ is onto

For every $\mathrm{f}_{\mathrm{a}} \in \mathrm{G}^{\prime}$,
since f is onto, there exists $\mathrm{a} \in \mathrm{G}$
such that $\varphi(\mathrm{a})=\mathrm{f}_{\mathrm{a}}$
Thus $\varphi$ is onto
(iii) $\varphi$ is a honorphism

$$
\varphi\left(\mathrm{a}^{*} \mathrm{~b}\right)=\mathrm{f}_{\mathrm{a}^{*} \mathrm{~b}}=\mathrm{f}_{\mathrm{a}}{ }^{\circ} \mathrm{f}_{\mathrm{b}}
$$

$$
\begin{aligned}
\left(\mathrm{f}_{\mathrm{a}}{ }^{\circ} \mathrm{f}_{\mathrm{b}}\right)(\mathrm{x}) & =\mathrm{f}_{\mathrm{a}}\left[\mathrm{f}_{\mathrm{b}}(\mathrm{x})\right] \\
= & \mathrm{f}_{\mathrm{a}}(\mathrm{bx}) \\
= & \mathrm{abx}=\mathrm{f}_{\mathrm{a}} * \mathrm{~b}(\mathrm{x}) \\
= & \varphi(\mathrm{a})^{\circ} \varphi(\mathrm{b})
\end{aligned}
$$

Thus $\varphi$ is a honmrphism
$\Leftrightarrow$ is a isomphishetween G and G
$\Rightarrow \mathrm{G} \cong \mathrm{G}^{\prime}$.
7. Show that $(M, 0)$ is an abelian group where $\left.\mathbf{M} \mathbf{A}, \mathbf{A} \quad{ }^{2}, \mathbf{A}^{3}, \mathbf{A}^{4}\right\}$ with $A=\left[\begin{array}{cc}0 & 1 \\ - & ]\end{array}\right.$ and is the ordinary matrix multiplication. Further prove that $(M, \mathbb{0})$ is isomorphic to the abelian group $(G, \rrbracket)$ where $\mathbf{G}=\{1,-1, i,-i\}$ and $\rrbracket$ is the ordinary multiplication.

## Solution:

$$
A=\begin{array}{cc}
{\left[\begin{array}{cc}
0 & 1 \\
-1 & 0
\end{array}\right]} \\
\lfloor & \rfloor
\end{array} A^{2}=\underset{c c}{[-1} \begin{array}{cc}
0 \\
0 & -1 \\
& \rfloor
\end{array} ; A^{3}=\left[\begin{array}{cc}
0 & -1 \\
1 & 0 \\
\hline
\end{array}\right] ; A^{4}=\left[\begin{array}{ll}
1 & 0 \\
0 & 1 \\
\hline & \rfloor
\end{array}\right]=I
$$

For all $1 \leq \mathrm{m}, \mathrm{n} \leq 4, \quad \mathrm{~A}^{\mathrm{m}} . \mathrm{A}^{\mathrm{n}}=\mathrm{A}^{\mathrm{m}+\mathrm{n}}=\mathrm{A}^{\mathrm{r}}$ where $1<\mathrm{r}<4$ and $\mathrm{m}+\mathrm{n} \cong \mathrm{r}(\bmod 4)$.
Thus . is a closure. Thus . is a closure operation. Since matrix multiplication is associative so is $\because$
$A^{4}=\left[\begin{array}{ll}1 & 0 \\ 0 & 1\end{array}\right]=I$ is the identity.
$\left.A^{-1}=\begin{array}{l}1 \\ -\left\lfloor\begin{array}{cc}0 & -1 \\ 1\end{array}\right]=A^{3} \\ \left(A^{2}\right)^{-1} \\ =\frac{1}{1}\left[\begin{array}{cc}-1\end{array}\right] \\ 1 \\ 0\end{array}\right]=A^{2}$
$\left(A^{3}\right)^{-1}=\frac{1}{1}\left[\begin{array}{cc}0 & 1 \\ -1 & 0\end{array}\right]=A$
$\left(A^{4}\right)^{-1}=\frac{1}{1}\left[\begin{array}{ll}1 & 0 \\ 0 & 1\end{array}\right]=I=A^{4}$

For all $1 \leq m, n \leq 4, \quad A^{m} . A^{n}=A^{m+n}=A^{n+m}=A^{n} . A^{m}$, so ${ }^{\prime} .^{\prime}$ is commutative.
$\therefore(M, 0)$ is an abelian group .

Define $\mathrm{f}: \mathrm{M} G$ such that $\quad \mathrm{f}(\mathrm{A})=\mathrm{i}, \mathrm{f}\left(\mathrm{A}^{2}\right)=-1=\mathrm{i}^{2}, \mathrm{f}\left(\mathrm{A}^{3}\right)=-\mathrm{i}=\mathrm{i}^{3}, \mathrm{f}\left(\mathrm{A}^{4}\right)=1=\mathrm{i}^{4}$
$\therefore \mathrm{f}$ is $1-1$ and onto
Since $\left.i^{3}=-i=f\left(A^{3}\right)=f(A\urcorner A^{2}\right)=f(A) f\left(A^{2}\right)=i \| i^{2}=i^{3}=-i$
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) $<R,+\rangle$ is an abelian group
(ii) $\langle R, \cdot>$ 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 $a b=b a$ for all $a, b \in R$ (it is commutative under multiplication). Note that rings are always commutative under addition.
Subring:
Let $(R,+, \cdot)$ be a ring. A non - empty subset $S$ of $R$ is called a subring of $R$, if $(S,+, \cdot)$ is a ring.
Example: The ring of rational numbers is a subring of the ring of real numbers.

1. Prove that the set $\mathbf{R}$ of numbers of the form $a+b \sqrt{2}$, where $\mathbf{a}$ and $\mathbf{b}$ are integers, is a ring with respect to ordinary addition and multiplication.
Proof:
2. Closure : Let $x_{1}=a_{1}+b_{1} \quad \sqrt{2}, x_{2}=a_{2}+b_{2} \sqrt{2} \in R$ where $a_{1}, a_{2}, b_{1}, b_{2} \in Z$
$x_{1}+x_{2}=\left(a_{1}+b_{1} \sqrt{2}\right)+\left(a_{2}+b_{2} \sqrt{2}\right)=\left(a_{1}+a_{2}\right)+\left(b_{1}+b_{2}\right) \sqrt{2} \in R$
where $\left(a_{1}+a_{2}\right) \&\left(b_{1}+b_{2}\right) \in Z$.
$\therefore \mathrm{R}$ is closed under + .
3. 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

$$
\begin{aligned}
& \left.\left.a_{1}, a_{2}, \begin{array}{c}
a_{3}, b_{1}, b_{2}, b_{3} \in Z \\
\left(x_{1}+x_{2}\right)+x_{3}=\left[\left(a_{1}+b_{1} \mathcal{J}^{2}\right)+\left(a_{2}+b_{2}\right.\right. \\
z)
\end{array}\right)\right]+\left(a_{3}+b_{3} \mathcal{F}^{2}\right) \\
& =\left\lceil\left(a_{1}+a_{2}\right)+\left(b_{1}+b_{2}\right) \sqrt{ }\right\rceil+\left(a_{3}+b_{3} \sqrt{2}\right) \\
& =\left[\begin{array}{cc}
(a+a)+a \\
1 & 2
\end{array}\right]+\left[\begin{array}{c}
(b+b)+b \\
1
\end{array}\right] \sqrt{2} \\
& =\left[a_{1}+\left(a_{2}+a_{3}\right)\right]+\left[b_{1}+\left(b_{2}+b_{3}\right)\right] \sqrt{2} \\
& =\left(a_{1}+b_{1} \sqrt{2}\right)+\left[\left(a_{2}+a_{3}\right)+\left(b_{2}+b_{3}\right) \sqrt{2}\right] \\
& =\left(a_{1}+b_{1} \sqrt{z}\right)+\left\lceil\left(a_{2}+b_{2} \sqrt{ }^{z}\right)+\left(a_{3}+b_{3} \sqrt{ }\right)\right\rceil=x_{1}+\left(x_{2}+x_{3}\right)
\end{aligned}
$$

3. Identity: $0+0 \vartheta \in R$

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

4. Inverse: $a+b \nLeftarrow,-a-b \quad \sqrt{2} \in R$
$(a+b \sqrt{2})+(-a-b \sqrt{2})=(a-a)+(b-b) \sqrt{2}=0+0 \sqrt{2}$
$(-a)+(-b) \sqrt{2}$ is the identity inverse of $a+b \sqrt{2}$
5. Commutative law:

$$
\begin{aligned}
x_{1}+x_{2}=\left(a_{1}+b_{1} \sqrt{2}\right) & +\left(a_{2}+b_{2} \sqrt{2}\right)=\left(a_{1}+a_{2}\right)+\left(b_{1}+b_{2}\right) \sqrt{2} \\
=( & \left.a_{2}+a_{1}\right)+\left(b_{2}+b_{1}\right) \sqrt{2} \\
& =\left(a_{2}+b_{2} \sqrt{2}\right)+\left(a_{1}+b_{1} \sqrt{2}\right)=x_{2}+x_{1}
\end{aligned}
$$

Under Multiplication
6. Closure Axioms:

$$
\begin{aligned}
& x_{1} x_{2}=\left(a_{1}+b_{1} \sqrt{2}\right) \cdot\left(a_{2}+b_{2} \sqrt{2}\right)=\left(a_{1} a_{2}+2 b_{1} b_{2}\right)+\left(a_{2} b_{1}+a_{1} b_{2}\right) \sqrt{2} \\
& a_{1} a_{2}+2 b b_{12}, a b+a b_{12} \in Z \\
& \therefore x_{1} x_{2} \in R \\
& \text { 7. Associative: } \\
& \begin{aligned}
\left(x_{1} \cdot x_{2}\right) \cdot x_{3}= & {\left[\left(a_{1}+b_{1} \sqrt{2}\right) \cdot\left(a_{2}+b_{2} \sqrt{2}\right)\right] \cdot\left(a_{3}+b_{3} \sqrt{2}\right) } \\
& \quad\left[\left(a_{1} a_{2}+2 b_{1} b_{2}\right)+\left(a_{2} b_{1}+a_{1} b_{2}\right) \sqrt{2}\right] \cdot\left(a_{3}+b_{3} \sqrt{2}\right) \\
= & {\left[\left(a_{1} a_{2}+2 b_{1} b_{2}\right) a_{3}+2\left(a_{2} b_{1}+a_{1} b_{2}\right) b_{3}\right]+\left[\left(a_{1} a_{2}+2 b_{1} b_{2}\right) b_{3}+\left(a_{2} b_{1}+a_{1} b_{2}\right) a_{3}\right] . } \\
= & x_{1} \cdot\left(x_{2} \cdot x_{3}\right)
\end{aligned}
\end{aligned}
$$

$$
\begin{aligned}
& \text { 8. Distributive Laws : } \\
& \begin{array}{l}
\text { 8. Distributive Laws : } \\
x_{1} \cdot\left(x_{2}+x_{3}\right)=\left(a_{1}+b_{1} \sqrt{ }\right) \cdot\left[\left(a_{2}+b_{2} \sqrt{ }^{z}\right)+\left(a_{3}+b_{3} \mathcal{F}^{2}\right)\right]
\end{array} \\
& =\left(a_{1}+b_{1} \sqrt{ }\right) \cdot\left[\left(a_{2}+a_{3}\right)+\left(b_{2}+b_{3}\right) \sqrt{2}\right] \\
& =\left[a_{1}\left(a_{2}+a_{3}\right)+2\left(b_{2}+b_{3}\right) b_{1}\right]+\left[b_{1}\left(a_{2}+a_{3}\right)+\left(b_{2}+b_{3}\right) a_{1}\right] \sqrt{2} \\
& =\left(a_{1}+b_{1} \sqrt{2}\right) \cdot\left(a_{2}+b_{2} \sqrt{2}\right)+\left(a_{1}+b_{1} \sqrt{2}\right) \cdot\left(a_{3}+b_{3} \sqrt{2}\right) \\
& =a_{1} a_{2}+a_{1} a_{3}+2 b_{1} b_{2}+2 b_{1} b_{3}+\sqrt{2} a_{2} b_{1}+\sqrt{2} a_{3} b_{1}+\sqrt{2} a_{1} b_{2}+\sqrt{2} a_{1} b_{3} \\
& =\left\lceil\left(a_{1} a_{2}+2 b_{1} b_{2}\right)+\left(a_{1} b_{2}+a_{2} b_{1}\right) \sqrt{2}\right\rceil+\left[\left(a_{1} a_{3}+2 b_{1} b_{3}\right)+\left(a_{1} b_{3}+a_{3} b_{1}\right) \sqrt{ }\right] \\
& x_{1} \cdot\left(x_{2}+x_{3}\right)=x_{1} \cdot x_{2}+x_{1} \cdot x_{3} \\
& \left(x_{2}+x_{3}\right) \cdot x_{1}=x_{2} \cdot x_{1}+x_{3} \cdot x_{1}
\end{aligned}
$$

Hence the given set is a ring.
2. Prove that the set $Z_{4}=\mathbb{\pi}, 1,2,3$ is a commutative ring with respect to the binary operation $+_{4}$ and $\mathbf{X}_{4}$.

## 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.

| $\mathrm{x}_{4}$ | $[0]$ | $[1]$ | $[2]$ | $[3]$ |
| :---: | :---: | :---: | :---: | :---: |
| $[0]$ | 0 | 0 | 0 | 0 |
| $[1]$ | 0 | 1 | 2 | 3 |
| $[2]$ | 0 | 2 | 0 | 2 |
| $[3]$ | 0 | 3 | 2 | 1 |

From tables, evget
(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 rowis equal to entries in the first, second, third and fourth columns respectively.

Hence the operations are commutative.
(iii) Modular addition and Modular multiplications are alays associative.
(iv) 0 is the additive identity and 1 is the multiplicative identity.
(v) Aditive inverse of $0,1,2,3$ are respectively $0,3,2,1$. Multiplicative inverses of the nonzero 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 $\left(Z_{4},{ }_{4}, \times_{4}\right)$ is a commutative ring ith unity.
3.

Let $A=\left\{\left[\begin{array}{ll}a & 0 \\ 0 & a\end{array}\right] / a \in R\right\} \quad$ (a) Show that $\mathbf{A}$ is a ring under matrix addition and
multiplication (b) Prove that $R$ is isomorphic to $A$.
Proof:
(a) For any $B=\left[\begin{array}{ll}b & 0 \\ 0 & b\end{array}\right]$ and $C=\left[\begin{array}{ll}c & 0 \\ 0 & c\end{array}\right]$, we have
$B+C=\left[\begin{array}{ll}b & 0 \\ 0 & b\end{array}\right]+\left[\begin{array}{ll}c & 0 \\ 0 & c\end{array}\right]=\left[\begin{array}{cc}b+c & 0 \\ 0 & b+c\end{array}\right] \in A$ and
$\mathrm{B} \cdot \mathrm{C}=\left[\begin{array}{ll}\mathrm{b} & 0 \\ 0 & \mathrm{~b}\end{array}\right] \cdot\left[\begin{array}{cc}\mathrm{c} & 0 \\ \mathrm{fb} & 0\end{array}\right]=\left[\begin{array}{cc}\mathrm{bc} & 0\end{array}\right] \in \mathrm{A}$
Also for any $B=\left[\begin{array}{ll}\lceil b & 0 \\ 0 & b\end{array}\right]$, the additiveinverse $-B=\left[\begin{array}{cc}-b & 0 \\ 0 & -b\end{array}\right]$ exists such that
$B+(-B)=\left[\begin{array}{ll}\mathrm{b} & 0 \\ 0 & \mathrm{~b}\end{array}\right]+\left[\left.\begin{array}{cc}-\mathrm{b} & 0 \\ 0 & -\mathrm{b}\end{array} \right\rvert\,=\left[\begin{array}{ll}0 & 0 \\ 0 & 0\end{array}\right] \in \mathrm{A}\right.$.

$$
\begin{aligned}
& \text { Distributive Laws: }
\end{aligned}
$$

$$
\begin{aligned}
& A .(B+C)=\begin{array}{ll}
{\left[\begin{array}{ll}
a .(b+c) & 0 \\
0 & a .(b+c)
\end{array} \begin{array}{l}
\dagger \\
\lfloor
\end{array} \begin{array}{cc}
(a . b+a . c) & 0 \\
0 & (a . b+a . c)
\end{array}\right]}
\end{array}
\end{aligned}
$$

$$
\begin{aligned}
& =\left[\begin{array}{ll}
a & 0 \\
0 & a
\end{array}\right] \cdot\left[\begin{array}{ll}
b & 0 \\
0 & b
\end{array}\right]+\left[\begin{array}{ll}
a & 0 \\
0 & a
\end{array}\right] \cdot\left[\begin{array}{ll}
c & 0 \\
0 & c
\end{array}\right]=A \cdot B+A \cdot C
\end{aligned}
$$

Similarly, $\quad(B+C) . A=B . A+C . A$
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 $r \in R, f: R \rightarrow A$ where $f(\notin)\left[\begin{array}{ll}r & 0 \\ 0 & r\end{array}\right]$ i.e., for any real number we associate a $2^{\text {nd }}$ order scalar matrix.

$$
\begin{aligned}
& \text { Now for any } \underset{r}{r}, \underset{r}{s} \in \mathrm{~s} \\
& f(r+s)=\left[\begin{array}{cc}
\underset{r}{s+s} \in R & 0 \\
0 & r+s
\end{array} \left\lvert\,=\left[\begin{array}{ll}
r & 0 \\
0 & r
\end{array}\right]+\left[\begin{array}{ll}
s & 0 \\
0 & s
\end{array}\right]=f(r)+f(s)\right.\right. \\
& \mathrm{f}(\mathrm{r} \cdot \mathrm{~s})=\left[\begin{array}{ll}
\mathrm{rs} & 0 \\
0 & \mathrm{rs}
\end{array}\right]=\left[\begin{array}{ll}
\mathrm{r} & 0 \\
&
\end{array}\right] \cdot\left[\begin{array}{cc}
\mathrm{s} & 0 \\
& \mathrm{f}
\end{array}\right]=\mathrm{f}(\mathrm{r}) \cdot \mathrm{f}(\mathrm{~s})
\end{aligned}
$$

Thus two operations + , are preserved and f is $1-1$ and onto.
$\therefore \mathrm{f}$ is an isomorphism from R to A .

Integral domain:
A commutative ring $\mathbf{R}$ with a unit element is called an integral domain if $\mathbf{R}$ has no zero divisors.
Zero Divisors
A ring $(\mathrm{R},+, \cdot)$ is said to be ring with zero divisors, if there exists non zero elements
$a, b$ in $R$, such that $a b=0$.
Example:
$\left(\{0,1,2,3,4,5\},+_{6}, \times_{6}\right)$ 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 $\{\mathrm{D},+, \cdot\}$ be a finite integral domain.
Then $D$ has a finite number of distinct elements, say $\left\{a_{1}, a_{2}, a_{3}, \square a_{n}\right\}$.
Let $a(\neq 0)$ be any element of $D$.
Then the elements a $\cdot a_{1}, a \cdot a_{2}, a \cdot a_{3}, a \cdot a_{n} \in D$, since $D$ is closed under multiplication.
The elements a $\cdot a_{1}, a \cdot a_{2}, a \cdot a_{3}, \square a \cdot a_{n}$ are distinct, because fa
$\cdot \mathrm{a}_{\mathrm{i}}=\mathrm{a} \cdot \mathrm{a}_{\mathrm{j}} \in \mathrm{D}$, then $\mathrm{a} \cdot\left(\mathrm{a}_{\mathrm{i}}-\mathrm{a}_{\mathrm{j}}\right)=0$.
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 $\mathrm{a}_{1}, \mathrm{a}_{2}, \mathrm{a}_{3}, \square \mathrm{a}_{\mathrm{n}}$ are distinct elements of D .
Hence the sets $\left\{a \cdot a_{1}, a \cdot a_{2}, a \cdot a_{3}, \square a \cdot a_{n}\right\}$ and $\left\{a_{1}, a_{2}, a_{3}, \square a_{n}\right\}$ are the sameSince
$a \in D$ is in both sets,
let $\mathrm{a} \cdot \mathrm{a}_{\mathrm{k}}=\mathrm{a}$, for some $\mathrm{k} \quad(\mathbf{1})$
Then $a_{k}$ is the unity of $D$, detailed as follows:
Let $\mathrm{a}_{\mathrm{j}}=\mathrm{a} \cdot \mathrm{a}_{\mathrm{i}}, \mathrm{a}_{\mathrm{j}} \in \mathrm{D} \quad$ (2)

$$
\begin{aligned}
\text { Now } \mathrm{a}_{\mathrm{j}} \cdot \mathrm{a}_{\mathrm{k}} & =\mathrm{a}_{\mathrm{k}} \cdot \mathrm{a}_{\mathrm{j},} \text { bycommutative property } \\
& =a_{\mathrm{k}} \cdot\left(\mathrm{a} \cdot \mathrm{a}_{\mathrm{i}}\right), \text { by }(2) \\
& =\left(a_{k} \cdot a\right) \cdot a_{\mathrm{i}} \\
& =\left(\mathrm{a} \cdot a_{\mathrm{k}}\right) \cdot a_{\mathrm{i}}, \text { by commutative property } \\
& =a \cdot a_{\mathrm{i}}, \text { by }(1) \\
& =a_{\mathrm{j}}, \text { by }(2)
\end{aligned}
$$

Since $\mathrm{a}_{\mathrm{j}}$ is an arbitrary element of $\mathrm{D}, \mathrm{a}_{\mathrm{k}}$ 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 $\{\mathrm{D},+, \cdot\}$ be a finite integral domain.
Field:
A commutative ring $(\mathrm{F},+, \cdot)$ which has more than one element such that every nonzero element of F has a multiplicative inverse in F is called a field.
Example: ( $\mathrm{Q},+,.),(\mathrm{R},+,$.$) and (C,+, .) are all fields.$

## Note:

But $(\mathrm{Z},+$, . $)$ is an integral domain and not a field.

## 1. Every field is an integral domain. <br> Proof: <br> Let (F,,$+ \cdot$ ) 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 $\mathrm{a}^{-1}$ exists

$$
\begin{aligned}
& \therefore \mathrm{a}^{-1} \cdot(\mathrm{a} \cdot \mathrm{~b})=\mathrm{a}^{-1} \cdot 0 \\
& \Rightarrow\left(\mathrm{a}^{-1} \mathrm{a}\right) \Rightarrow 0 \\
& \Rightarrow 1 \Rightarrow \mathrm{~b} \quad 0 \\
& \Rightarrow=0
\end{aligned}
$$

Thus $a \cdot b=0, a \neq 0 \Rightarrow b=0$
$\therefore \mathrm{F}$ has no zero divisors.
Hence $F$ is an integral domain.

## 2. Prove that $Z_{n}$ is a field if and only if $\mathbf{n}$ is a prime.

## Proof:

Whave $Z_{n}=\{[0],[1],[2], \square[n-1]\}$
Bknow $\left(Z_{n},+\right.$ is $)$ a commutative ring with identity $1[$. $]$
Let n be a prime, and suppose that $0<\mathrm{a}<\mathrm{n}$ then $\operatorname{gcd}(\mathrm{a}, \mathrm{n})=1$
$\therefore$ there exists integers s , t such that as $+\mathrm{tn}=1 \Rightarrow \mathrm{sa}-1=(-\mathrm{t}) \mathrm{n}$
$\therefore \quad$ sa- 1 is divisible by $n$
$\Rightarrow \quad \mathrm{sa} \equiv 1(\operatorname{modn})$
$\Rightarrow \quad[\mathrm{s}][\mathrm{a}]=[1]$
$\therefore[\mathrm{s}]$ is the multiplicativeinverse of [a].
Thus [a]isa 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 $\mathrm{n}=\mathrm{n}_{1} \mathrm{n}_{2}$, where $1<\mathrm{n}_{1}, \mathrm{n}_{2}<\mathrm{n}$. So $\left[\mathrm{n}_{1}\right] \neq[0]$ and $\left[\mathrm{n}_{2}\right] \neq[0]$
But $\left[\mathrm{n}_{1}\right]\left[\mathrm{n}_{2}\right]=\left[\mathrm{n}_{1} \mathrm{n}_{2}\right]=[\mathrm{n}]=[0]$
$\therefore\left[\mathrm{n}_{1}\right],\left[\mathrm{n}_{2}\right]$ aredivisors of zero which contradicts thefact $\mathrm{Z}_{\mathrm{n}}$ 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 $\operatorname{gcd}(27,33)$. First, we have to divide the bigger one by the smaller one.

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

So, $33=1 \times 27+6$

Thus $\operatorname{gcd}(33,27)=\operatorname{gcd}(27,6)$. Repeating this (i.e., divide 27 by 6 , quotient is 4 and remainder is 3 )
So, $27=4 \times 6+3$
and we see $\operatorname{gcd}(27,6)=\operatorname{gcd}(6,3)$. Finally divide 6 by 3 , quotient is 2 and remainder is 0
so, $6=2 \times 3+0$
Since 6 is a perfect multiple of $3, \operatorname{gcd}(6,3)=3$, and thus we have found that $\operatorname{gcd}(33,27)=3$.

## 1. Find $[100]^{-1}$ in $\mathrm{Z}_{1009}$.

## SOLUTION:

$\operatorname{gcd}(100,1009)=1$,
By Euclidean Algorithm,

$$
\begin{align*}
& 1009=10(100)+9 \text {------------------------------------1)}  \tag{1}\\
& \begin{aligned}
100 & =11(9) \\
B y(2) \Rightarrow \quad 1 & =100-11(9) \\
& =100-11[1009-10(100)] \\
& =100+110(100)-11(1009) \\
& =111(100)-11(1009) \\
& =(111)(100)(\bmod 1009)
\end{aligned}  \tag{2}\\
& \therefore[1]=[111][100](\bmod 1009) \\
& \Rightarrow[100]^{-1} \text { is }[111] \text { in } Z_{1009} .
\end{align*}
$$

# MOHAMED SATHAK A .J .COLLEGE OF ENGINEEING <br> MA8551 Algebra and Number Theory <br> Unit II - Finite Fields and Polynomials <br> Notes 

## Introduction

You have studied in school polynomials with integer coefficients, rational coefficients and real coefficients. A polynomial is an expression of the form $a_{0}+a_{1} x+a_{2} x^{2}+\cdots+a_{n} x^{n}$, where $n$ is a non-negative integer and $a_{0}, a_{1}, a_{2} \because ; ; a_{n}$ 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,

$$
f(x)=\underset{0}{a}+a_{1} x+a_{2} x^{2}++a_{r} x^{r}+\quad+a_{n} x^{n},
$$

$a$ is called the coefficient of $x^{r}$ and $a x^{r}$ is a term of the polynomial $f(x)$.
Definition: Let $f(x)=\underset{0}{a}+a_{1} x+a_{2} x^{2}+\quad+a x_{n}^{n}$ 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 $\operatorname{deg} f(x)=n$ 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 $f(x)=\underset{0}{a}+\underset{1}{a} x+a_{2} x^{2}+\ldots+a_{n} x^{n}$, and $g(x)=\underset{0}{b}+\underset{1}{b} x+\underset{2}{b} x^{2}+\ldots+b_{n} x^{n}$, 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, $a+a \underset{1}{x}+a x_{2}^{2}+a x_{3}^{3}$ 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 $f(x)+g(x)=C_{0}+C_{1} x+C_{2} x_{2}+\ldots+C x_{s}$
Where $C_{i}=a_{i}+b_{i} \forall i$.

|  | And the product $\begin{aligned} & f(x) \cdot g(x)=\left(\underset{0}{a}+a_{1} x+a_{2} x^{2}+\cdots+a_{n} x^{n}\right) \cdot\left(b_{0}+b_{1} x+b_{2} x^{2}+\ldots+b_{m} x^{m}\right) \\ & =C_{0}+C_{1} x+C_{2} x^{2}+\cdots+C_{r} x^{r}+\cdots C_{k} x^{k} \end{aligned}$ <br> Where $\begin{aligned} & C_{0}=a_{0} b_{0} \\ & C_{1}=a_{0} b_{1}+a_{1} b_{0} \\ & C_{2}=a_{0} b_{2}+a_{1} b_{1}+a_{2} b_{0} \end{aligned}$ $C_{r}=a_{0} b_{r}+a_{1} b_{r-1}+\cdots+a_{r} b_{0}$ <br> Note: Though the definition of multiplication appear to be complicated, it is the familiar process of using distributive property and collecting like terms. <br> For example consider $f(x)=2+3 x+2 x^{2}+x^{3}$ and $g(x)=1+x+2 x^{2}$, in $Z[x]$ <br> Then $\begin{aligned} f(x)+g(x) & =(2+1)+(3+1) x+(2+2) x^{2}+(1+0) x^{3} \\ & =3+4 x+4 x^{2}+x^{3} \end{aligned}$ <br> And $\begin{aligned} & f(x) \cdot g(x)=\left(2+3 x+2 x^{2}+x^{3}\right) \cdot\left(1+x+2 x^{2}\right) \\ & =2 \cdot 1+(3 \cdot 1+2 \cdot 1) x+(2 \cdot 1+2 \cdot 2+3 \cdot 1) x^{2}+(1+2 \cdot 1+3 \cdot 2) x^{3}+(1+2 \cdot 2) x^{4}+1 \cdot 2 x^{5} \\ & \quad=2+5 x+9 x^{2}+9 x^{3}+5 x^{4}+2 x^{5} \end{aligned}$ |
| :---: | :---: |
| 1 | Theorem: Let $R$ be a ring, then ( $R[x],+, \cdot)$ is a ring. |
|  | Proof: <br> Given $R$ is a ring. <br> Let $f(x)$ and $g(x) \in R[x]$ <br> 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 $f(x)+g(x)=C_{0}+C_{1} x+C_{2} x_{2}+\ldots+C x_{s}$
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
$f(x) \cdot g(x)=C_{0}+C_{1} x+C_{2} x_{2}+\ldots+C_{r} x_{r}+\ldots x_{k}$
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 $\cdot$ 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 $+\mathrm{in} R[x]$. 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
$f(x)=a_{0}^{a}+a_{1} x+a_{2} x^{2}+\ldots+a_{n} x^{n}$
$g(x)=b_{0}+b_{1} x+b_{2} x^{2}+\ldots+b_{m} x^{m}$
$h(x)=C_{0}+C_{1} x+C_{2} x_{2}+\ldots+C_{p} x_{p}$
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 $\left(a_{r} b_{s}\right) c_{t}$, where $r, s, t$ are non-negative integers such that $r+s+t=i$.

|  | Again the coefficient of $x^{i}$ in the expansion of $f(x)(g(x) h(x))$ is sum of the products of the form $a_{r}\left(b_{s} c_{t}\right)$, where $r, s, t$ are non-negative integers such that $r+s+t=i .$ <br> Since multiplication is associative in $R$. $a_{r}\left(b_{s} c_{t}\right)=\left(a_{r} b_{s}\right) c_{t}$ <br> Coefficient of $x^{i}$ in $(f(x) g(x)) h(x)$ is equal to the coefficient of $x^{i}$ in $f(x)(g(x) h(x))$ <br> Multiplication of polynomials is associative. $(f(x) g(x)) h(x)=f(x)(g(x) h(x))$ <br> Now $f(x)[g(x)+h(x)]=f(x) g(x)+f(x) h(x)$, since the coefficient of $x^{i}$ in the L.H.S is $a_{r}\left(b_{s}+c_{t}\right)$ and the coefficient of $x$ in the R.H.S is $a_{r} b_{s}+a_{r} c_{t}=a_{r}\left(b_{s}+c_{t}\right)$ <br> Hence ( $R[x],+;$ ) is a ring under polynomial addition and multiplication. |
| :---: | :---: |
|  | Note: <br> 1. This ring $R[x]$ is called the ring of polynomials over $R$ or the ring of polynomials with coefficients in $R$. <br> 2 If $R$ is commutative, then $R[x]$ is also commutative. <br> For, if $f(x)=a_{0}+a_{1} x+a_{2} x^{2}+\ldots+a_{n} x^{n}$ and $g(x)=b_{0}+b_{1} x+b_{2} x^{2}+\ldots+b_{m} x^{m}$ Then coefficient of $x^{r}$ in $f(x) g(x)$ is $\begin{aligned} & =a_{0} b_{r}+a_{1} b_{r-1}+a_{2} b_{r-2}+\cdots+a_{r} b_{0} \\ & =b_{r} a_{0}+b_{r-1} a_{1}+b_{r-2} a_{2}+\cdots+b_{0} a_{r}[\because R \text { is commuative }] \\ & =b_{0} a_{r}+b_{1} a_{r-1}+b_{2} a_{r-2}+\cdots+b_{r} a_{0} \\ & =\text { Coefficient of } x^{r} \text { in } g(x) f(x) \end{aligned}$ $f(x) g(x)=g(\cdot x) f(x) \forall f(x), g(x) \in R[x]$ |


|  | $\therefore R[x]$ is commutative. <br> 3. If $R$ is a ring with identity 1 , then $R[x]$ is a ring with identity 1 , <br> Since $1=1+0 x+0 x^{2}+\cdots+0 x^{t} \in R[x]$ and $\begin{aligned} & f(x) \cdot 1=\left(\underset{0}{a}+a_{1} x+a_{2} x+\cdots+a_{n} x^{n}\right) \cdot\left(1+0 x+0 x^{2}+\cdots+0 x^{t}\right) \\ & =a_{0}+a_{1} x+a_{2} x+\cdots+a_{n} x^{n} \\ & =f(x) \end{aligned}$ <br> 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: <br> Let $R$ be an integral domain. <br> Then $R$ is a commutative ring with identity and without zero divisors. <br> Hence $R[x]$ is commutative ring with identity 1 , since $f(x) \cdot 1=f(x)$. <br> We have to prove $R[x]$ is without zero divisors. <br> To prove $f(x) \neq 0, g(x) \neq 0 \Rightarrow f(x) g(x) \neq 0$ <br> Let $f(x)=a_{0}+a_{1} x+a_{2} x^{2}+\ldots+a_{n} x^{n}, a \neq 0$ then <br> $g(x)=b_{0}+b_{1} x+b_{2} x^{2}+\ldots+\underset{m}{x^{m}}, \underset{m}{\neq 0}$. Then <br> $f(x) \cdot g(x)=c_{0}+c_{1} x+c_{2} x^{2}+\ldots+c_{n+m} x^{n+m}$, where $c_{r}=a \underset{0_{r}}{b}+a_{1 r} b_{r}+\ldots+a_{r 0} b_{0}$ and $c_{m+n}=a_{n} \cdot b_{m}$ <br> Since $R$ is without zero divisors $\begin{aligned} & a_{n} \neq 0, b_{m} \neq 0 \Rightarrow a_{n} b_{m} \neq 0 \Rightarrow c_{n+m} \neq 0 \\ & \therefore f(x) g(x) \neq 0 \end{aligned}$ <br> Hence $R[x]$ is an integral domain. <br> 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 $R[x]$. <br> 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. <br> $\therefore F[x]$ is an integral domain by above theorem. <br> Note that if $F$ is a field, the $F[x]$ is not afield. <br> Proof: We know if $F$ is a filed, then $F[x]$ is an integral domain by Corollary <br> 1. <br> Let $f(x)=x \in F[x]$. Suppose it has the multiplicative inverse <br> $g(x)=\underset{0}{a}+\underset{1}{a} x+a_{2} x^{2}+\ldots+a_{n} x^{n}$, then $x g(x)=1$ $\begin{aligned} & x\left(a_{0}+a_{1} x+\cdots+a_{n} x^{n}\right)=1+0 x+0 x^{2}+\cdots \\ & a_{0} x+a_{1} x^{2}+\cdots+a_{n} x^{n+1}=1+0 x+0 x^{2}+\cdots+0 x^{n+1} \end{aligned}$ <br> By definition of equality of polynomials, we find $1=0$ (equating constant terms). <br> Which is a contradiction <br> $\therefore f(x)=x$ has no multiplicative inverse. <br> Hence, $F[x]$ is not a field. |
| 4 | Theorem: If $R$ is an integral domain, then $\operatorname{deg}(f(x) \cdot g(x))=\operatorname{deg} f(x)+\operatorname{deg} g(x)$. |
|  | Proof: Let $R$ be an integral domain. <br> Then $R$ is a commutative ring with identity and without zero divisions. i.e., $a \neq 0, b \neq 0 \Rightarrow a b \neq 0$. <br> Let $f(x)=a_{0}+a_{1} x+a_{2} x^{2}+\ldots+a_{n} x^{n}, a \neq 0$ therefore $\operatorname{deg} f(x)=n$ and $g(x)=b_{0}+b_{1} x+b_{2} x^{2}+\ldots+b_{m} x^{m}, b \neq 0$ therefore $\operatorname{deg} g(x)=m$ |


|  | Since $R$ is an integral domain, $a_{n} \cdot b_{m} \neq 0$. <br> Now $f(x) g(x)=c_{0}+c_{1} x+c_{2} x^{2}+\ldots+c_{n+m} x^{n+m}$ where $c_{n+m}=a_{n m}^{b} \neq 0$ $\therefore \operatorname{deg}(f(x) g(x))=n+m=\operatorname{deg} f(x)+\operatorname{deg} g(x)$ <br> Note: <br> 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 $\operatorname{deg} f(x) g(x) \leq \operatorname{deg} f(x)+\operatorname{deg} g(x)$. <br> In the product, $f(x) g(x)=c_{0}+c_{1} x+c_{2} x^{2}+\ldots+c x_{s}^{s}$. <br> If $c_{i}=0 \forall i$, then $f(x) g(x)=0$ <br> Otherwise $f(x) g(x) \neq 0$ <br> If $a_{n} b_{m}=0$, then $\operatorname{deg} f(x) g(x)<\operatorname{deg} f(x)+\operatorname{deg} g(x)$. <br> If $a_{n} b_{m} \neq 0$, then $\operatorname{deg} f(x) g(x)=\operatorname{deg} f(x)+\operatorname{deg} g(x)$. <br> $\therefore \operatorname{deg} f(x) g(x) \leq \operatorname{deg} f(x)+\operatorname{deg} g(x)$ <br> $2 f(x)+g(x)=0$ or $\operatorname{deg}(f(x)+g(x)) \leq \max \{\operatorname{deg} f(x), \operatorname{deg} g(x)\}$ |
| :---: | :---: |
|  | Definition: Root of a polynomial <br> Let $R$ be a ring with identity 1 and let $f(x)=a_{0}+a_{1} x+a_{2} x^{2}+\cdots+a_{n} x^{n} \in R[x]$ <br> With $\operatorname{deg} f(x) \geq 1$. <br> An element $a \in R$ is called a root of $f(x)$ if $f(a)=a_{0}+a_{1} a+a_{2} a^{2}+\ldots+a a_{n}^{n}=0$ <br> If $f(a)=0$, then $a$ is root of $f(x)$. <br> Note: If $R=\left(Z_{6},+, \bullet\right)$, where $Z_{6}=\{0,1,2,3,4,5\}$ by writing [a] a s $a$. <br> A polynomial over $Z_{6}$ can be written differently. <br> $f(x)=2 x^{3}+5 x^{2}+3 x-2$ over $Z \underset{6}{\text { is a polynomial }}$ |


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


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


|  |
| :--- |
|  |
| $\therefore 6(6)=6^{2}+4 \cdot 6=36+24=60 \equiv 0(\bmod 12)$ |
| $f(7)=7^{2}+4 \cdot 7=49+28=77 \equiv 5(\bmod 12) \neq 0$ |
| $\therefore 7$ is not a root of $f(x)$ |
| $f(8)=8^{2}+4 \cdot 8=64+32=96 \equiv 0(\bmod 12)$ |
| $\therefore 8$ is a root of $f(x)$ |
| $f(9)=9^{2}+4 \cdot 9=81+36=117 \equiv 9(\bmod 12) \neq 0$ |
| $\therefore 9$ is not a root of $f(x)$ |
| $f(10)=10^{2}+4 \cdot 10=100+40=140 \equiv 8(\bmod 12) \neq 0$ |
| $\therefore 10$ is not a root of $f(x)$ |
| $f(11)=11^{2}+4 \cdot 11=121+44=165 \equiv 9(\bmod 12) \neq 0$ |
| $\therefore 11$ is not a root of $f(x)$ |
| $\therefore x=0,2,6,8$ are the roots of $f(x)$ over $Z_{12}$. |


|  | $\begin{aligned} & \therefore 2 \text { is not a root of } f(x) \\ & f(3)=3^{3}+5 \cdot 3^{2}+2 \cdot 3+6=27+45+6+6=84 \equiv 0(\bmod 7) \\ & \therefore 3 \text { is a root of } f(x) \\ & f(4)=4^{3}+5 \cdot 4^{2}+2 \cdot 4+6=64+80+8+6=128 \equiv 2(\bmod 7) \neq 0 \\ & \therefore 4 \text { is not a root of } f(x) \\ & f(5)=5^{3}+5 \cdot 5^{2}+2 \cdot 5+6=125+125+10+6=266 \equiv 0(\bmod 7) \\ & \therefore 5 \text { is a root of } f(x) \\ & f(6)=6^{3}+5 \cdot 6^{2}+2 \cdot 6+6=216+180+12+6=434 \equiv 0(\bmod 7) \\ & \therefore 6 \text { is a root of } f(x) \end{aligned}$ <br> Therefore the roots of $f(x)$ are $1,3,5,6$ in $Z_{7}$. |
| :---: | :---: |
| 10 | Example: Determine all the roots of $\left.f(x)=x^{2}+3 x+2 \in\right]_{6}[x]$. |
|  | Solution: Given $f(x)=x^{2}+3 x+2 \in Z_{6}[x]$ and $Z_{6}=\{0,1,2,3,4,5\}$. <br> We verify and find the roots. <br> Now $f(0)=2 \neq 0$ <br> $\therefore 0$ is not a root of $f(x)$ $f(1)=1^{2}+3 \cdot 1+2=1+3+2=6 \equiv 0(\bmod 6)$ <br> $\therefore 1$ is a root of $f(x)$ $f(2)=2^{2}+3 \cdot 2+2=4+6+2=12 \equiv 0(\bmod 6)$ <br> $\therefore 2$ is a root of $f(x)$ $f(3)=3^{2}+3 \cdot 3+2=9+9+2=20 \equiv 2(\bmod 6) \neq 0$ <br> $\therefore 3$ is not a root of $f(x)$ $f(4)=4^{2}+3 \cdot 4+2=16+12+2=30 \equiv 0(\bmod 6)$ <br> $\therefore 4$ is a root of $f(x)$ |


|  | $f(5)=5^{2}+3 \cdot 5+2=25+15+2=42 \equiv 0(\bmod 6)$ <br> $\therefore 5$ is a root of $f(x)$ <br> 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 $Z_{2}=\{0,1\}$ <br> Let the general polynomial of degree 2 is $f(x)=a+a \underset{1}{x}+a x_{2}^{2}, a \neq 0$ <br> The possible coefficients are from $Z_{2}$, where $a_{2} \neq 0$, so $a_{2}=1$ $f(x)=a_{0}^{a}+a_{1} x+x^{2}$ <br> If $\underset{0}{a}=0, a=1$ then $f(x)=x^{2}$ <br> If $\underset{0}{a=0, a=1}=1$ then $f(x)=x+x^{2}$ <br> If $\underset{0}{a=1, a=0} 10$ then $f(x)=1+x^{2}$ <br> If $\underset{0}{a=1, a=1} \operatorname{l}_{1}$ then $f(x)=1+x+x^{2}$ <br> Therefore, there are four possible polynomials of degree 2, $2, x^{2}, x+x^{2}, 1+x^{2}, 1+x+x^{2} \in Z[x] .$ |
|  | Definition: Divisor of a polynomial <br> 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 $g(x)=f(x) h(x)$ <br> We also say that $f(x)$ divides $g(x)$ or $g(x)$ is a multiple of $f(x)$. <br> We have division algorithm for an integer $a$ and positive integer $n$, $a=n q+r, 0 \leq r<n$ <br> We are familiar with division of polynomials with real coefficients. <br> For example, divide $g(x)=x^{3}-3 x^{2}+4 x+5$ by $f(x)=x-2$ <br> The division is shown here |

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

Here quotient $q(x)=x^{2}-x+2$ and the remainder $r(x)=9$
$\therefore x^{3}-3 x^{2}+4 x+5=(x-2)\left(x^{2}-x+2\right)+9$
$\Rightarrow g(x)=q(x) f(x)+r(x)$.
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 $\operatorname{deg} r(x)<\operatorname{deg} f(x)$.
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 $\operatorname{deg} r(x)<\operatorname{deg} f(x)$

If not, let $\operatorname{deg} r(x) \geq \operatorname{deg} f(x)$
Let $r(x)=\underset{0}{a}+\underset{1}{a} x+a_{2} x^{2}+\ldots+a x_{n}^{n}, \underset{n}{a \neq 0}$ and
$f(x)=\underset{0}{b}+b_{1} x+b_{2} x^{2}+\ldots+b_{m} x^{m}, b_{m} \neq 0$
$\therefore \quad n \geq m$
Define

$$
\begin{gathered}
h(x)=r(x)-a_{n} b_{m}^{-1} x^{n-m} f(x) \quad\left[\because b_{m} \neq 0, b_{m}^{-1} \text { exist in } F\right] \\
=a_{0}+a_{1} x+a_{2} x^{2}+\cdots+a_{n} x^{n}-a b_{n m}^{-1} x^{n-m}\left(b_{0}+b_{1} x+b_{2} x^{2}+\cdots+b_{m} x^{m}\right) \\
=a_{0}+a_{1} x+a_{2} x^{2}+\cdots+a_{n} x^{n}-a a_{n} b_{m}^{-1} b x^{n-m}-a b_{n} b_{m}^{-1} b x_{1}^{n-m+1}-a b_{n}^{-1} b x_{2}^{n-m+2}-. .-a_{n m m}^{b^{-1} b x^{m}} \\
\therefore \operatorname{deg} h(x)<n=\operatorname{deg} r(x) \\
\text { Since } r(x) \in S, r(x)=g(x)-q(x) r(x) \\
\qquad h(x)=g(x)-q(x) f(x)-a b_{n} b^{-1} x^{n-m} f(x) \\
=g(x)-\left[q(x)-a b_{n m}^{-1} x^{n-m}\right] f(x) \\
=g(x)-p(x) f(x)
\end{gathered}
$$

Where $p(x)=q(x)_{n m} a b^{-1} x^{n-m} \in F[x]$
$\therefore h(x) \in S$ and $\operatorname{deg} h(x)<\operatorname{deg} r(x)$
Which is contradiction to the fact that $\operatorname{deg} r(x)$ is minimum.
$\therefore \operatorname{deg} r(x)<\operatorname{deg} f(x)=n$
Where $r(x)=0$ or $\operatorname{deg} r(x)<\operatorname{deg} f(x)$

|  | We now prove the uniqueness <br> Suppose we also have $g(x)=q_{1}(x) f(x)+r_{1}(x)$ <br> Where $r_{1}(x)=0$ or $\operatorname{deg} r_{1}(x)<\operatorname{deg} f(x)$ <br> Then $q(x) f(x)+r(x)=q_{1}(x) f(x)+r_{1}(x)$ <br> $\left[q(x)-q_{1}(x)\right] f(x)=r_{1}(x)-r(x)$ <br> If $\quad q(x)-q_{1}(x) \neq 0, \quad$ then $\quad \operatorname{deg}\left[q(x)-q_{1}(x)\right] f(x) \geq \operatorname{deg} f(x)$ <br> $\Rightarrow \operatorname{deg}\left[r_{1}(x)-r(x)\right] \geq \operatorname{deg} f(x)$, which is a contradiction <br> $\therefore q(x)-q_{1}(x)=0 \Rightarrow q(x)=q_{1}(x)$ <br> Then (3) $r_{1}(x)-r(x)=0 \Rightarrow r_{1}(x)=r(x)$ <br> 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 $f(x)$. <br> 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 $f(x)=3 x^{4}+x^{3}+2 x^{2}+1$ and $g(x)=x^{2}+4 x+2$ in $Z[x]$. <br> Find $q(x)$ and $r(x)$ when $f(x)$ is divided by $g(x)$. |
|  | Solution: Given $f(x)=3 x^{4}+x^{3}+2 x^{2}+1$ and $g(x)=x^{2}+4 x+2$ <br> 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 |  |
| :---: | :---: |
| $3 x^{2}+4 x$ | $\lceil 12 \equiv 2(\bmod 5)]$ |
| $x ^ { 2 } + 4 x + 2 \longdiv { 3 x ^ { 4 } + x ^ { 3 } + 2 x ^ { 2 } + 0 x + 1 }$ | $\|6 \equiv 1(\bmod 5)\|$ |
| $3 x^{4}+2 x^{3}+x^{2}$ | $-1 \equiv 4(\bmod 5)$ |
| $4 x^{3}+x^{2}+0 x+1$ | $16 \equiv 1(\bmod 5)$ |
| $4 x^{3}+x^{2}+3 x$ | $8 \equiv 3(\bmod 5)$ |
| $2 x+1$ | $\lfloor-3 \equiv 2(\bmod 5)\rfloor$ |

Therefore, the quotient $q(x)=3 x^{2}+4 x$ and the remainder $r(x)=2 x+1$
$\therefore 3 x^{4}+x^{3}+2 x^{2}+1=\left(x^{2}+4 x+2\right)\left(3 x^{2}+4 x\right)+(2 x+1)$

## 14

Example: If $f(x)=2 x^{4}+5 x^{2}+2, g(x)=6 x^{2}+4$, then determine $q(x)$ and $r(x)$ in $Z_{7}[x]$, when $f(x)$ is divided by $g(x)$.

Solution: Given $f(x)=2 x^{4}+5 x^{2}+2$, and $g(x)=6 x^{2}+4$,
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
$\left.\begin{array}{|c|c|}\hline 5 x^{2}+1 & \lceil 30 \equiv 2(\bmod 7) \\ \left.6 x^{2}+0 x+4\right) \\ \frac{2 x^{4}+0 x^{3}+5 x^{2}+0 x+2}{2 x^{4}+6 x^{2}} & \left\lvert\, \begin{array}{l}20 \equiv 6(\bmod 7) \\ -1 \equiv 6(\bmod 7) \\ 6 x^{2}+0 x+2 \\ 6 x^{2}+0 x+4 \\ 5\end{array}\right. \\ \hline-2 \equiv 5(\bmod 7)\end{array}\right]$

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

|  | $\therefore 2 x^{4}+5 x^{2}+2=\left(5 x^{2}+1\right)\left(6 x^{2}+4\right)+5$ |
| :---: | :---: |
| 15 | Example: If $f(x)=3 x^{2}+4 x+2$ and $g(x)=6 x^{4}+4 x^{3}+5 x^{2}+3 x+1$, are polynomials in $Z_{7}[x]$, then find $q(x)$ and $r(x)$ in when $g(x)$ is divided by $f(x)$. |
|  | Solution: Given $f(x)=3 x^{2}+4 x+2$ and $g(x)=6 x^{4}+4 x^{3}+5 x^{2}+3 x+1$, <br> 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 . <br> The division is shown here |
|  | $\left.3 x^{2}+4 x+2\right) \frac{2 x^{2}+x+6}{6 x^{4}+4 x^{3}+5 x^{2}+3 x+1}$ <br> $\frac{6 x^{4}+x^{3}+3 x^{2}}{3 x^{3}+x^{2}+3 x}$ <br> $\frac{3 x^{3}+4 x^{2}+2 x}{4 x^{2}+4 x+1}$ <br> $\frac{4 x^{2}+4 x+1}{5 x+3}$$\|$$8 \equiv 1(\bmod 7)$ <br> $\|-3 \equiv 4(\bmod 7)\|$ <br> $8 \equiv 4(\bmod 7)$ <br> $\left\|\begin{array}{l}1 \\ 24 \equiv 3(\bmod 7) \\ 12 \equiv 5(\bmod 7) \\ \|-2 \equiv 5(\bmod 7)\| \\ -4 \equiv 3(\bmod 7)\end{array}\right\|$ |

Therefore, the quotient $q(x)=2 x^{2}+x+6$ and the remainder $r(x)=5 x+3$
$\therefore 6 x^{4}+4 x^{3}+5 x^{2}+3 x+1=\left(2 x^{2}+x+6\right)\left(3 x^{2}+4 x+2\right)+(5 x+3)$
16 Example: If $f(x)=x^{5}+3 x^{4}+x^{3}+x^{2}+2 x+2 \in Z[x]$ is divided by $(x-1)$, find the quotient and remainder.
Solution: Given $f(x)=x^{5}+3 x^{4}+x^{3}+x^{2}+2 x+2$ 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 <br> divided by $g(x)$, we use long division method keeping in mind addition and <br> multiplication are done under modulo 7. <br> The division is shown here <br> $\frac{x^{4}+4 x^{3}+x+3}{x^{5}+3 x^{4}+x^{3}+x^{2}+2 x+2}$ <br> $\frac{x^{5}-x^{4}}{4 x^{4}+x^{3}}$ <br> $\frac{4 x^{4}-4 x^{3}}{x^{2}+2 x}$ <br> $\frac{x^{2}-x}{3 x+2}$ <br> $\frac{3 x-3}{0}$ | $[5 \equiv 0(\bmod 5)]$ |
| :--- | :--- |$\quad$|  |
| :--- |

Therefore, the quotient $q(x)=x^{4}+4 x^{3}+x+3$ and the remainder $r(x)=0$
$(x-1)$ is a factor of $f(x)$
$f(x)=\left(x^{4}+4 x^{3}+x+3\right)(x-1)$

17
Example: $f(x)=x^{3}+5 x^{2}+2 x+6 \in Z[, x]$, 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 $f(x)=x^{3}+5 x^{2}+2 x+6$

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

## Solution:

Given $f(x)=\left(2 x^{3}+1\right)\left(5 x^{3}+5 x+3\right)(4 x-3) \in Z_{7}[x]$,

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 $2 x^{2}+1$

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

4 from $4 x-3$

Now
$1 \equiv 8(\bmod 7)$
$3 \equiv 10(\bmod 7)$
$-3 \equiv 4(\bmod 7)$
$f(x)=\left(2 x^{3}+8\right)\left(5 x^{3}+5 x+10\right)(4 x+4)$
$=2\left(x^{2}+4\right) 5\left(x^{3}+x+2\right) 4(x+1)$
$=40\left(x^{2}+4\right)\left(x^{3}+x+2\right)(x+1)$
$=5\left(x^{2}+4\right)\left(x^{3}+x+2\right)(x+1) \quad[\because 40 \equiv 5(\bmod 7)]$

Note: Instead of $-3 \equiv 4(\bmod 7)$ in the $3^{\text {rd }}$ factor.

|  | We may write $3 \equiv 24(\bmod 7)$ <br> Then we get $f(x)=2\left(x^{2}+4\right) 5\left(x^{3}+x+2\right) 4(x-6)$ $\begin{aligned} & =40\left(x^{2}+4\right)\left(x^{3}+x+2\right)(x-6) \\ & =5\left(x^{2}+4\right)\left(x^{3}+x+2\right)(x-6) \end{aligned}$ |
| :---: | :---: |
|  | As corollaries of the division algorithm, we get the remainder theorem and factor theorem. |
| 19 | Corollary: The remainder theorem <br> 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, $(x-a) \in F[x]$ <br> By division algorithm, $f(x)=q(x)(x-a)+r(x)$ <br> Where $r(x)=0$ or $\operatorname{deg} r(x)<\operatorname{deg}(x-a)=1$ $\therefore \operatorname{deg} r(x)=0$ <br> $\Rightarrow r(x)=r($ a constant $)$, an element is $F$. $f(x)=q(x)(x-a)+r$ <br> Put $x=a$ |



|  | $(x-a)$ is a factor of $f(x)$. |
| :---: | :---: |
| 21 | Example: What is the remainder when $f(x)=x^{5}+2 x^{3}+x^{2}+2 x+3 \in Z\left[\begin{array}{c}x \\ 5\end{array}\right]$ is divided by $(x-1)$ ? |
|  | Solution: Given $f(x)=x^{5}+2 x^{3}+x^{2}+2 x+3$. <br> When $f(x)$ is divided by $(x-1)$, the remainder is $f(1)$. <br> $f(1)=1+2+1+2+3=9 \equiv 4(\bmod 5)$ the remainder is 4 in $Z_{5}$. |
| 22 | Example: What is the remainder when $f(x)=2 x^{3}+x^{2}+2 x+3 \in Z\left[{ }_{5}^{x}\right]$ is divided by $(x-2)$ ? |
|  | Solution: Given $f(x)=2 x^{3}+x^{2}+2 x+3$ and $Z=\{0,1,2,3,4\}$. <br> When $f(x)$ is divided by $(x-2)$, the remainder is $f(2)$. <br> $f(2)=2 \cdot 2^{3}+2^{2}+2 \cdot 2+3=27 \equiv 2(\bmod 5)$ the remainder is 2 in $Z$. |
| 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 $g(x)=x-1$ <br> The remainder when $f(x)$ is divided by $g(x)$ is $f(1)$. $f(1)=1+1+1+1+1+1=6 \equiv 0(\bmod 2)$ <br> 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 $f(x)=a x+b, a, b \in F, a \neq 0$. <br> Clearly $-\frac{b}{a}$ or $-a^{-1} b \in F$ and $f\left(-a^{-1} b\right)=a\left(-a^{-1} b\right)+b=-b+b=0$. <br> $\therefore f(x)$ has (at least) one root in $F$. <br> If $c_{1}, c_{2}$ in $F$ are two roots of $f(x)$, then $f\left(c_{1}\right)=0 \Rightarrow a c_{1}+b=0$ <br> And $f\left(c_{2}\right)=0 \Rightarrow a c_{2}+b=0$ $a c_{1}+b=a c_{2}+b \Rightarrow a c_{1}=a c_{2}$ <br> Since $F$ is a field, it is an integral domain and so cancellation laws hold. $a c_{1}=a c_{2} \Rightarrow c_{1}=c_{2}$ <br> Therefore there is exactly one root of $F$ for $f(x)=a x+b, a \neq 0$ |



| 25 | Test whether the polynomial $f(x)=2 x^{2}+4$ is irreducible over $Z, Q, R$ and $C$. |
| :---: | :---: |
|  | Solution: <br> Given $f(x)=2 x^{2}+4=2\left(x^{2}+2\right)$ <br> Since 2 is constant polynomial in $\mathrm{Z}[\mathrm{x}]$ whose degree is 0 and $x^{2}+2 \in \mathrm{Z}[\mathrm{x}]$. <br> Now $2 x^{2}+4=0 \Rightarrow x^{2}+2=0 \Rightarrow x^{2}=-2 \Rightarrow x= \pm i \sqrt{ } 2$ <br> The roots do not belong to $\mathrm{Z}, \mathrm{Q}$ and R. But $i \sqrt{ } 2$ and $-i \sqrt{ } 2$ belong to C . <br> Hence $f(x)=2 x^{2}+4$ is reducible over C. |
| 26 | Is $f(x)=x^{2}+1$ in $Z[x]$ irreducible over $Z$ ? |
|  | Solution: <br> Given $f(x)=x^{2}+1$ in $\mathrm{Z}[x]$. <br> Now $x^{2}+1=0 \Rightarrow x^{2}=-1 \Rightarrow x= \pm i$ <br> $\therefore$ 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: <br> Given $f(x)=x^{3}+x^{2}+x+1 \in \mathrm{Z}_{2}[x]$ and $\mathrm{Z}_{2}=\{0,1\}$ <br> $f(0)=0+0+0+1=1 \neq 0 \quad \therefore 0$ is not a root in $\mathrm{Z}_{2}$. <br> $f(1)=1+1+1+1=4 \equiv 0(\bmod 2) \therefore 1$ is a root in $\mathrm{Z}_{2}$. |


|  | Hence $(x-1)$ is a factor of $f(x)$ in $\mathrm{Z}_{2}[x] . \therefore f(x)$ is reducible. $\begin{aligned} & x-1) \frac{x^{2}+1}{x^{3}+x^{2}+x+1} \\ & \begin{array}{r} x+1 \\ x-1 \end{array} \end{aligned}$ $\therefore f(x)=\left(x^{2}+1\right)(x-1)$ |
| :---: | :---: |
| 28 | Test the polynomial $x^{2}+x+4 \in \mathrm{Z}_{11}[x]$ is irreducible over $\mathrm{Z}_{11}$. |
|  | Solution: <br> Let $f(x)=x^{2}+x+4 \in \mathrm{Z}_{11}[x]$ and $\mathrm{Z}_{11}=\{0,1,2,3,4,5,6,7,8,9,10\}$ is a field, since 11 is a prime. $f(x)=x^{2}+x+4$ is a polynomial of degree 2 in $\mathrm{Z}_{11}[x]$. <br> We search for an element $a \in \mathrm{Z}_{11}$ such that $f(a)=0$. We have $\begin{aligned} & f(0)=0+0+4=4 \neq 0(\bmod 11) \\ & f(1)=1+1+4=6 \equiv-5(\bmod 11) \neq 0 \\ & f(2)=2^{2}+2+4=10 \equiv-1(\bmod 11) \neq 0 \\ & f(3)=3^{2}+3+4=16 \equiv 5(\bmod 11) \neq 0 \\ & f(4)=4^{2}+4+4=24 \equiv 2(\bmod 11) \neq 0 \end{aligned}$ $f(5)=5^{2}+5+4=34 \equiv 1(\bmod 11) \neq 0$ $f(6)=6^{2}+6+4=46 \equiv 2(\bmod 11) \neq 0$ $f(7)=7^{2}+7+4=60 \equiv 5(\bmod 11) \neq 0$ |


|  | $\begin{aligned} & f(8)=8^{2}+8+4=76 \equiv 10(\bmod 11) \neq 0 \\ & f(9)=9^{2}+9+4=94 \equiv 6(\bmod 11) \neq 0 \\ & f(10)=10^{2}+10+4=114 \equiv 4(\bmod 11) \neq 0 \end{aligned}$ <br> $\therefore$ there is no root in $\mathrm{Z}_{11}$. Hence $f(x)$ is irreducible over $\mathrm{Z}_{11}$. |
| :---: | :---: |
| 29 | Find two non-zero polynomials $f(x)$ and $g(x)$ in $Z_{12}[x]$ such that $f(x) g(x)$ $=0$. |
|  | Solution: <br> We know $\mathrm{Z}_{12}=\{0,1,2,3,4,5,6,7,8,9,10,11\}$ <br> Consider $f(x)=3 x^{2} \in Z_{12}[x]$ and $g(x)=4 x+8 \in \mathrm{Z}_{12}[x]$. <br> We know $f(x)$ and $g(x)$ are non-zero polynomials. But $f(x) g(x)=3 x^{2}(4 x+8)=12 x^{3}+24 x^{2}=0+0=0$ <br> $f(x) g(x)$ is a zero polynomial in $\mathrm{Z}_{12}[x]$. |
| 30 | Find two non-zero polynomials $f(x), g(x)$ in $\mathrm{Z}_{7}[x]$ such that $f(x) g(x) \neq 0$. |
|  | Solution: <br> We know $\mathrm{Z}_{7}=\{0,1,2,3,4,5,6\}$. Let $f(x)=2 x^{2}+4 x+1$ and $g(x)=6 x^{3}$ be two non-zero polynomials in $\mathrm{Z}_{7}[x]$. $\begin{array}{rlr} f(x) g(x) & =\left(2 x^{2}+4 x+1\right) 6 x^{3} \\ & =12 x^{5}+24 x^{4}+6 x^{3} \quad \text { Since } 12 \equiv 5(\bmod 7) \text { and } 24 \equiv 3(\bmod 7) \\ & =5 x^{5}+3 x^{4}+6 x^{3} \neq 0 . \end{array}$ |


| 31 | Reducibility Test <br> Let $F$ be a field and $f(x) \in F(x)$. Then <br> (i) If $f(x)$ is of degree 1 , then $f(x)$ is irreducible. <br> (ii) If $f(x)$ is of degree 2 or 3 , then $f(x)$ is reducible iff $f(x)$ has a root in $F$. |
| :---: | :---: |
|  | Proof: <br> (i) Let $f(x)=a x+b, a \neq 0$ in $F[x]$. <br> Suppose $f(x)$ is reducible, then there exist $g(x), h(x) \in F[x]$ such that $f(x)=g(x) h(x)$, where $1 \leq \operatorname{deg} g(x)<\operatorname{deg} f(x)$ and $1 \leq \operatorname{deg} h(x)<\operatorname{deg}$ <br> $f(x)$ $\begin{aligned} & \therefore a x+b=g(x) h(x) \\ & \therefore \operatorname{deg}(a x+b)=\operatorname{deg} g(x)+\operatorname{deg} h(x) \\ & \Rightarrow 1=\operatorname{deg} g(x)+\operatorname{deg} h(x) \end{aligned}$ <br> This is impossible, since $\operatorname{deg} g(x)+\operatorname{deg} h(x) \geq 2$ <br> $\therefore f(x)$ is irreducible over $F$. <br> (ii) Let $f(x) \in F[x]$ be of degree 2 or 3 . <br> Suppose $f(x)$ is reducible over $F$, then $f(x)=g(x) h(x)$ for some $g(x)$, $h(x) \in F[x]$, where $1 \leq \operatorname{deg} g(x)<\operatorname{deg} f(x)$ and $1 \leq \operatorname{deg} h(x)<\operatorname{deg} f(x)$. <br> Since $\operatorname{deg} f(x)=\operatorname{deg} g(x)+\operatorname{deg} h(x)$ and $\operatorname{deg} f(x)=2$ or 3 , we have $\operatorname{deg}$ $g(x)+\operatorname{deg} h(x)=2$ or 3 . <br> $\therefore$ at least one of $g(x)$ and $h(x)$ has degree 1 . <br> Let $\operatorname{deg} g(x)=1 \Rightarrow g(x)=a x+b, a \neq 0$. <br> Now $-a^{-1} b \in F$ and $g\left(-\alpha^{-1} b\right)=a\left(-a^{-1} b\right)+b$ $\begin{aligned} & =-\left(a \cdot a^{-1}\right) b+b \\ & =-b+b=0 \end{aligned}$ |


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


| $\begin{aligned} & \begin{array}{r} \left.2 x^{2}+2 x+2\right) \\ \frac{\frac{1}{2} x-\frac{1}{2}}{x^{3}-1} \\ \frac{x^{3}+x^{2}+x}{-x^{2}-x-1} \\ x^{3}-1 \end{array} \\ & =\left(\begin{array}{ll} x-\frac{1}{2}-x-1 \\ 2 & - \\ 2 \end{array}\right)\left(2 x^{2}+2 x+2\right)+0 \\ & \\ & =(x-1)\left(x^{2}+x+1\right) \end{aligned}$ <br> $\therefore$ The last non-zero remainder is $x^{2}+x+1$, which is the g.c.d |
| :---: |
| Characteristic of a Ring <br> Characteristic of a ring R is the least positive integer n such that na $=0 \forall \mathrm{a}$ $\in R$ and we write $\operatorname{char}(R)=n$. If no such positive integer exists, then $R$ is said to have characteristic 0 . <br> For example, <br> 1. The ring $(\mathrm{Z} 3,+, \bullet)$ has characteristic 3 . <br> In $\mathrm{Z} 3=\{0,1,2\}$, $\begin{aligned} & 1+1+1=3(1) \equiv 0(\bmod 3) \\ & 2+2+2=3(2) \equiv 0(\bmod 3) \\ & 3(\mathrm{a})=0 \forall \mathrm{a} \in \mathrm{Z}_{3} \end{aligned}$ <br> $\therefore$ Characteristic is 3 . That is $\operatorname{Char}\left(\mathrm{Z}_{3}\right)=3$. <br> More generally, characteristic of the ring $\left(\mathrm{Z}_{\mathrm{n}},+, \bullet\right)$ is n . <br> 2. $(\mathrm{Z},+, \bullet)$ and $(\mathrm{Q},+, \bullet)$ are rings. <br> For any $\mathrm{a} \in \mathrm{Z}$ (or Q ), there is no positive integer n such that na $=0$. <br> $\therefore \operatorname{chat}(Z)=0$ and $\operatorname{char}(Q)=0$ |


| 33 | Theorem: The characteristic of a field $(F,+, \bullet)$ is either 0 or a prime number. |
| :---: | :---: |
|  | Proof: |
|  | Let $(F,+, \bullet)$ be a field. |
|  | If $\operatorname{char}(F)=0$, then there is nothing to prove. |
|  | If $\operatorname{char}(F) \neq 0$, then let $\operatorname{char}(F)=n$. |
|  | To prove $n$ is a prime. |
|  | Suppose $n$ is not prime, then $n=p q$, where $1<p<n, 1<q<n$. |
|  | i.e., $p$ and $q$ are proper factors of $n$. |
|  | Since $\operatorname{char}(F)=n$, we have $n \alpha=0 \forall a \in F$. |
|  | Take $a=1$, then $n \bullet 1=0(1$ is identity of $F)$ |
|  | $\Rightarrow(p q) \mathbf{d}=0 \Rightarrow(p \mathbf{b})(q \mathbf{r})=0$ |
|  | $[\because(p q) \cdot 1=\underbrace{1+1+1+\ldots+1}_{p q \text { terms }}=\underbrace{(1+1+1+\ldots+1)}_{p \text { terms }} \underbrace{(1+1+1+\ldots+1)}_{q \text { terms }}]$ |
|  | 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: <br> We know for a prime $p, Z p$ is a field having $p$ elements and $\operatorname{char}(Z p)=p$, since $p a=0 \forall a \in Z p$. <br> Consider the polynomial $f(x)=x^{p}{ }^{n}-x$ in $Z[x]$. <br> Now $f^{\prime}(x)=p^{n} x^{p^{n}-1}-1$ <br> Since $\operatorname{char}\left(Z_{p}\right)=p, \operatorname{char}\left(Z_{p}[x]\right)=p$ and $p g(x)=0 \forall g(x) \in Z_{p}[x]$. <br> Hence $p x^{n-1}=0 \Rightarrow p^{n} x^{n}{ }^{n-1}=0$ <br> $\therefore \quad f^{\prime}(x)=-1$, a constant polynomial. <br> Hence $f(x)$ and $f^{\prime}(x)$ have no common root. <br> Hence $f(x)$ has no multiple roots. . the roots of $f(x)$ are all distinct. <br> If $K$ is the smallest extendsion field containing all the roots of $f(x)$. <br> i.e., $K$ is the splitting field of $f(x)$. Then $f(x)$ has $p^{n}$ distinct roots in $K$. <br> In $K$, let $F$ be the set of all elements satisfying $f(x)$. <br> ie. $\mathrm{F}=\left\{a \in K: a^{p^{n}}=a\right\}$ <br> Hence $F$ has only $p^{n}$ elements. <br> We now prove F is a field. <br> Let $a, b \in F$. Then $a^{p}=a$ and $b^{p}=b^{n}$. $\begin{aligned} & (a b)^{p^{n}}=a^{p^{n}} \cdot b^{p^{n}}=\boldsymbol{c} b \in F \\ & (a+b)^{p^{n}}=a^{p^{n}}+p^{n} C_{1} a^{p^{n}-1} b+p^{n} C_{2} a^{p}-2 b^{2}+\ldots+b^{n} p \end{aligned}$ <br> Since $\operatorname{char}(K)=p, p^{n} C a_{r}{ }^{{ }^{n}-r} b^{r}=0, r=1,2,3 \ldots$ $\therefore(a+b)^{p^{n}}=a^{p^{n}}+b^{p^{n}}=a+b \in F$ <br> 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 $\mathrm{F}[\mathrm{x}$ ] <br> 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 $\mathrm{g}(\mathrm{x})$ modulo $\mathrm{s}(\mathrm{x})$ and write $\mathrm{f}(\mathrm{x}) \equiv \mathrm{g}(\mathrm{x})(\bmod \mathrm{s}(\mathrm{x}))$ if $\mathrm{s}(\mathrm{x})$ divides $f(x)-g(x)$. <br> i.e., $f(x)-g(x)=q(x) s(x)$ for some $q(x) \in F[x]$. |
| Definition: Ideal of a ring <br> Let $(\mathrm{R},+, \bullet)$ be a ring. A non-empty subset $I$ of a ring is called an ideal of $R$, if <br> (i) for all $a, b \in I$, we have $a-b \in I$ <br> (ii) for all $r \in R$ and $a \in I$, we have ar, $r a \in I$. <br> Example: For any positive integer $n$, the subset $n Z=\{0, \pm n, \pm 2 n, \ldots\}$ is the ring $(Z,+, \bullet)$ is an ideal of $Z$. <br> Note: An ideal is always a subring, but a subring is not an ideal. Ideal is something more than a subring. <br> For example, $(\mathrm{Z},+, \bullet)$ is a subring of $(\mathrm{Q},+, \bullet)$, but is not an ideal, because if we take $2 \in \mathrm{Z}$ and $\frac{1}{3} \in \mathrm{Q}$, then $\frac{1}{3} .2=\frac{2}{3} \notin \mathrm{Z}$. |
| Definition: Factor ring <br> 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 $(a+I)+(b+I)=a+b+I \quad \text { and } \quad(a+I) \cdot(b+I)=a b+I \quad \forall a, b \in R$ <br> This ring is called factor ring or quotient ring and is denoted by $\mathrm{R} / \mathrm{I}$. |


|  | Definition: Principal ideal <br> An ideal generated by single element a is called a principal ideal and is denoted by $<a>$. Thus $<a>=\{r a: r \in R\}$. <br> Then quotient ring is $\mathrm{R} /<\mathrm{a}>$ <br> 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. <br> [Hint: Using the irreducible binary polynomial $x^{2}+x+1$ ] |
|  | Solution: <br> Consider $Z_{2}=\{0,1\}$ $f(x)=x^{2}+x+1 \in Z_{2}[x]$ $f(0)=0+0+1=1 \neq 0$ $f(1)=1+1+1=3 \equiv 1(\bmod 2) \neq 0$ <br> $\therefore f(x)$ is irreducible over $Z_{2}$. <br> $\therefore \frac{Z_{2}[x]}{\langle f(x)\rangle}=\frac{Z_{2}[x]}{\left\langle x^{2}+x+1\right\rangle}$ is a field having $2^{2}=4$ elements. <br> To find the four elements <br> Consider $g(x) \in Z_{2}[x]$ and $x_{2}+x+1 \in Z[x]$. |

By division algorithm,

$$
g(x)=q(x)\left(x^{2}+x+1\right)+r(x)
$$

whereeither $r(x)=0$ or $\operatorname{deg} r(x)<\operatorname{deg}\left(x^{2}+x+1\right)=2$

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

Hence $r(x)=a x+b$, where $a, b \in Z_{2}$

Since

$$
\begin{aligned}
g(x) & =q(x)\left(x^{2}+x+1\right)+r(x) \\
g(x)-r(x) & =q(x)\left(x^{2}+x+1\right) \\
g(x) & \equiv r(x) \bmod \left(x^{2}+x+1\right) \\
{[g(x)] } & =[r(x)]
\end{aligned}
$$

So, to find the equivalence classes $\bmod \left(x^{2}+x+1\right)$,
it is enough to find the possible values of $r(x)=a x+b$

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

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

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

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 $\frac{Z_{2}[x]}{\left\langle x^{2}+x+1\right\rangle}$ are $[0],[1],[x],[x+1]$.


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 $Z\left[{ }_{3} x\right], s(x)=x^{2}+x+2$. Show that $\mathbf{s}(\mathbf{x})$ is irreducible over $Z$ and construct that the field $\frac{Z_{3}[x]}{\langle s(x)\rangle}$. What is the order of this field? |  |
| :---: | :---: | :---: |
|  | Solution: <br> Consider $Z_{3}=\{0,1,2\}$ $s(x)=x^{2}+x+2 \in Z_{3}[x]$ $s(0)=0+0+2=2 \neq 0$ $s(1)=1+1+2=4 \equiv 1(\bmod 3) \neq 0$ $s(2)=4+2+2=8 \equiv 2(\bmod 3) \neq 0$ <br> $\therefore s(x)$ is irreducible over $Z_{3}$. <br> $\therefore \frac{Z_{3}[x]}{\langle s(x)\rangle}=\frac{Z_{3}[x]}{\left\langle x^{2}+x+2\right\rangle}$ is a field having $3^{2}=9$ elements. <br> To find the nine elements <br> Consider $g(x) \in Z_{3}[x]$ and $x_{2}+x+2 \in Z_{3}[x]$. <br> By division algorithm, $g(x)=q(x)\left(x^{2}+x+2\right)+r(x)$ <br> whereeither $r(x)=0$ or $\operatorname{deg} r(x)<\operatorname{deg}\left(x^{2}+x+1\right)=2$ $\therefore \quad \operatorname{deg} r(x)=0 \text { or } 1 .$ <br> Hence $r(x)=a x+b$, where $a, b \in Z_{3}$ <br> Since $\begin{aligned} g(x) & =q(x)\left(x^{2}+x+2\right)+r(x) \\ g(x)-r(x) & =q(x)\left(x^{2}+x+2\right) \end{aligned}$ |  |

$$
\begin{aligned}
& g(x) \equiv r(x) \bmod \left(x^{2}+x+2\right) \\
& {[g(x)]=[r(x)]}
\end{aligned}
$$

So, to find the equivalence classes $\bmod \left(x^{2}+x+2\right)$,
it is enough to find the possible values of $r(x)=a x+b$

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

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

If $a=2, b=2 \Rightarrow r(x)=2 x+2$
$\therefore$ the equivalence classes are $[0],[1],[2],[x],[x+1],[x+2],[2 x],[2 x+1],[2 x+2]$
$\therefore$ the 9 elements of the field $\frac{Z_{3}[x]}{\langle s(x)\rangle}$ are[0],[1],[2], $[x],[x+1],[x+2],[2 x],[2 x+1],[2 x+2]$.
Hence the number of elements $=9$.

# MOHAMED SATHAK A.J.COLLEGE OF ENGINEERING <br> MA8551-Algebra and Number Theory <br> NOTES <br> <br> UNIT-III DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS 

 <br> <br> 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 $b=a x$ and we write it as $a \mid b$. If $b$ is not divisible by $a$, then we write it $a s a \not a$.

## Theorem:

## 1. Prove the following:

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

Proof:
Given $\mathrm{a} \mid \mathrm{b}$ by definition $\mathrm{b}=\mathrm{ax}$.....(1) for some integer x
Multiply (1) by c
$\Rightarrow \mathrm{bc}=\mathrm{acx}$
$\Rightarrow \mathrm{bc}=\mathrm{a}(\mathrm{cx})$, where $z=\mathrm{cx}$ an integer
$\mathrm{bc}=\mathrm{az} \Rightarrow \mathrm{a} \mid \mathrm{bc}$
(2). $\mathrm{a} \mid \mathrm{b}$ and $\mathrm{b}|\mathrm{c} \Rightarrow \mathrm{a}| \mathrm{c}$ for any integer

Proof:
Assume that $\mathrm{a} / \mathrm{b}$ and $\mathrm{b} / \mathrm{c}$
$\mathrm{a} \mid \mathrm{b} \Rightarrow \mathrm{b}=\mathrm{ax} \cdots$ (1)for some integer x
$b \mid c \Rightarrow c=b y \cdots$ (2)for some integer $y$
Substitute (1) in (2),
$c=(a x) y=a(x y)=a z$, where $z=x y$ is an integer
$\Rightarrow \mathrm{a} \mid \mathrm{c}$
(3). $\mathrm{a} \mid \mathrm{b}$ and $a|\mathrm{c} \Rightarrow \mathrm{a}|(b x+c y)$ for any integer $\mathrm{x} \& \mathrm{y}$

Proof:

By definition, $b=a x_{1}$, where $x_{1}$ is an integer.
Multiply both side by x , $\mathrm{bx}=\mathrm{a} \mathrm{x}_{1} \ldots .$. (1)
Assume that a|c then $c=a y_{1}$, for someinteger $y_{1}$
cy $=$ ayy $_{1}$
Adding (1) and (2)
$b x+c y=a x x_{1}+a y y_{1}=a\left(x x_{1}+y y_{1}\right)=a z$, where $z=x x_{1}+y y_{1}$ is an integer
$\Rightarrow \mathrm{a} \mid(\mathrm{bx}+\mathrm{cy})$
(4). $\mathrm{a} \mid \mathrm{b}$ and $b \mid \mathrm{a} \Rightarrow \mathrm{a}= \pm \mathrm{b}$

## Proof:

Given $a \mid b$ by definition $b=a x$.....(1) for some integer $x$
$b \mid a \Rightarrow a=b y \cdots(2)$ for some integer $y$
Multiply (1) and (2),

$$
\begin{aligned}
& a b=(a x)(b y) \\
& \Rightarrow 1=x y \\
& \Rightarrow x=1 \& y=1 \text { or } x=-1 y=-1 \\
& \Rightarrow a= \pm b
\end{aligned}
$$

(5). If $\mathrm{m} \neq 0, \mathrm{a}|\mathrm{b} \Leftrightarrow m a| \mathrm{m} b$

## Proof:

Given $a \mid b$ by definition $b=a x$.....(1) for some integer $x$.
Multiply (1) both sides by $\mathrm{m}, \mathrm{m} \neq 0$
$\mathrm{mb}=\mathrm{max} \Rightarrow \mathrm{ma} \mid \mathrm{mb}$
Assume that ma|mb
by definition, $m b=m a x$ for some integer $x$
$b=a x$
$\Rightarrow \mathrm{a} \mid \mathrm{b}$

## THE DIVISION ALGORITHM:

Let $a$ be any integer and $b$ be a positive integer. Then there exist unique $q$ and $r$ such that $\mathrm{a}=\mathrm{b} \cdot \mathrm{q}+\mathrm{r}$, where $0 \leq \mathrm{r}<\mathrm{b}$, and where a is dividend, b is divisor, q is quotient and r is remainder.

## Proof:

## Existence Part

Let $S=\{a-b n: n \in Z$ and $a-b n \geq 0\}$
Then, first we prove that $S$ is non-empty.
Case(i): Let $a \geq 0$ Then $a-b(0)=\mathrm{a} \geq 0$ with $0 \in \mathrm{Z}$. By the definition $\mathrm{S}, a \in S$. Hence S is non-empty.
Case(ii):
Let $a<0 \sin c e b$ is a positive integer $b \geq 1$
Hence $a b \leq a$, sin ce $a<0$
$\Rightarrow a-b \cdot a \geq 0$, with $a \in Z$.
By the definition of $S, a-b \cdot a \in S$.
Thus in both cases Scontains atleast one element. So Sis 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 $r=b q$, where $r \geq 0$
To show that $r<b$ :
We will prove by contradiction.
Assume $\mathrm{r} \geq \mathrm{b}$. Then $\mathrm{r}-\mathrm{b} \geq 0$. But $\mathrm{r}-\mathrm{b}=(a-b q)-b=a-b(q+1)$.
Since $a-b(q+1)$ is of the form $a-b n$ and is $\geq 0, a-b(q+1) \in S$
$\Rightarrow r-b \in S$. 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 $0 \leq r<b$.

## Uniqueness Proof:

Let there be two sets of integers $q, \mathrm{r}$ and $q^{\prime}, r^{\prime}$ such that
$a=b q+r----$ (1)
and $a=b q^{\prime}+r^{\prime}-----(2)$

Assume that $q \geq q^{\prime}$, from (1) and (2)
$b q+r=b q^{\prime}+r^{\prime} \Rightarrow b\left(q-q^{\prime}\right)=r^{\prime}-r$
with $r^{\prime}-r<b \quad-----(4)$
$\sin c e r^{\prime}<b$ and $r<b$
Assume that $q>q^{\prime}$. Then $q-q^{\prime} \geq 1$. Since $b>0 . b\left(q-q^{\prime}\right) \geq b$.
Hence from (3) $r^{\prime}-r \geq b$, contradicts (4).
$\therefore q \ngtr q^{\prime}$. hence $\mathrm{q}=\mathrm{q}^{\prime}$, Therefore, from (3) $0=\mathrm{r}^{\prime}-\mathrm{r} \Rightarrow \mathrm{r}=\mathrm{r}^{\prime}$
Thus, the integers $q$ and $r$ are unique.
i.e., There exist unique integers $q$ and $r$ such that
$\mathrm{a}=\mathrm{b} \cdot \mathrm{q}+\mathrm{r}$, where $0 \leq \mathrm{r}<\mathrm{b}$

## 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 $\geq 2$. 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 $0,1,2 \ldots b-1$. 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., $x=b q_{1}+r$ and $y=b q_{2}+r$
$\Rightarrow x-y=b\left(q_{1}-q_{2}\right) \Rightarrow b \mid(x-y)$.
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 $\mathrm{A}_{1}, \mathrm{~A}_{2}, \ldots \mathrm{~A}_{n}$ are finite sets, then $\left|\bigcup_{i=1}^{n} A_{i}\right|=\sum_{1 \leq i \leq n}\left|A_{i}\right|-\sum_{1 \leq i<j \leq n}\left|A_{i} \cap A_{j}\right|+\sum_{1 \leq i<j<k \leq n}\left|A_{i} \cap A_{j} \cap A_{k}\right|-\ldots \ldots+(-1)^{n+1}\left|\bigcap_{i=1}^{n} A_{i}\right|$

## Problem:

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

## Soln:

Let $A=\{x \in N / x \leq 2076$ and divisible by 4$\}, B=\{x \in N / x \leq 2076$ and divisible by 5$\}$ then $|A \cup B|=|A|+|B|-|A \cap B|$

$$
\begin{aligned}
& =\lfloor 2076 / 4\rfloor+\lfloor 2076 / 5\rfloor-\lfloor 2076 / 20\rfloor \\
& =519+415-103=831
\end{aligned}
$$

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 positiveintegers $\leq 1976$ that are divisible by $13=\left[\frac{1976}{13}\right]=[152]=152$
The number of positive integers $\leq 3776$ 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

$$
\begin{aligned}
& =290-152+1 \\
& =139[\because 1976 \text { is included in the list of numbers divisible by } 13]
\end{aligned}
$$

3. Find the number of positive integer's $\leq \mathbf{3 0 0 0}$ and divisible by 3,5 , or 7 .

Soln:
Let $\mathrm{A}, \mathrm{B}, \mathrm{C}$ be the set of numbers $\leq 3000$ and divisible by $3,5,7$ respectively.
Required $|A \cup B \cup C|$
By inclusion and exclusion principle, we get
$|\mathrm{A} \cup \mathrm{B} \cup \mathrm{C}|=S_{1}-S_{2}+S_{3}$
Now

$$
\begin{aligned}
& |\mathrm{A}|=\left[\frac{3000}{3}\right]=[1000]=1000 \\
& |B|=\left[\frac{3000}{5}\right]=[600]=600 \\
& |C|=\left[\frac{3000}{7}\right]=[428.57]=428 \\
& S_{1}=|\mathrm{A}|+|B|+|C|=1000+600+428=2028 \\
& |\mathrm{~A} \cap \mathrm{~B}|=\left[\frac{3000}{3 \times 5}\right]=[200]=200 \\
& |\mathrm{~A} \cap C|=\left[\frac{3000}{3 \times 7}\right]=[142.85]=142 \\
& |B \cap C|=\left[\frac{3000}{5 \times 7}\right]=[85.71]=85 \\
& S_{2}=|\mathrm{A} \cap \mathrm{~B}|+|\mathrm{A} \cap C|+|B \cap C|=200+142+85=427 \\
& \mathrm{Now} S_{3}=|\mathrm{A} \cap \mathrm{~B} \cap \mathrm{C}|=\left[\frac{3000}{3 \times 5 \times 7}\right]=[28.57]=28 \\
& |\mathrm{~A} \cup \mathrm{~B} \cup \mathrm{C}|=S_{1}-S_{2}+S_{3}=2028-427+28=1629
\end{aligned}
$$

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

## To prove:

$\mathrm{p}(\mathrm{n})=n^{2}+n$ is an even integer
$p(1)=1^{2}+1=2$ is an even number
We assume that the result is true for all $\mathrm{k}, \mathrm{k}$ be the arbitrary number. $\Rightarrow \mathrm{p}(\mathrm{k})=k^{2}+k$ is an even integer consider $\mathrm{p}(\mathrm{k}+1)=(k+1)^{2}+(k+1)$

$$
=k^{2}+2 k+1+k+1=\left(k^{2}+k\right)+(2 k+2)=\text { Even number }
$$

hence $\mathrm{p}(\mathrm{n})=\mathrm{n}^{2}+n$ is even integer $\forall \mathrm{n}$.
5. Show that for any integer $n, n^{2}-n$ is divisible by 2 and $n^{5}-n$ is divisible by 6

## Soln:

$\mathrm{n}^{2}-\mathrm{n}=\mathrm{n}(\mathrm{n}-1)$ It is two consecutive number. So it is divisible by 2
To Prove: $\mathrm{n}^{5}-\mathrm{n}$ is divisible by 6

$$
\mathrm{n}^{5}-\mathrm{n}=n\left(n^{4}-1\right)=n\left(n^{2}-1\right)\left(n^{2}+1\right)=n(n-1)(n+1)\left(n^{2}+1\right)=(n-1) n(n+1)\left(n^{2}+1\right)
$$

Now, as we know that product of 3 consecutive natural numbers is always divisible by 3 and that of 2 consecutive natural numbers is always divisible by 2 so this expression is always divisible by 6 .

## 6. Show that $30 \mid n^{5}-n$, where $n$ is an arbitrary integer

Soln:

First we prove $\mathrm{n}^{5}-\mathrm{n}$ isdivisible by 6

$$
\mathrm{n}^{5}-\mathrm{n}=n\left(n^{4}-1\right)=n\left(n^{2}-1\right)\left(n^{2}+1\right)=n(n-1)(n+1)\left(n^{2}+1\right)=(n-1) n(n+1)\left(n^{2}+1\right)
$$

Now, as we know that product of 3consecutive natural numbers is always divisible by 3 and that of 2 consecutive natural numbers is always divisible by 2 so this expression is always divisible by6.
Now to prove divisibility by5,First we write the factorisation as under

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

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

Hence the proof.
7. If the sum of the cubes of three consecutive integers is a cube $\boldsymbol{k}^{3}$, prove that $3 \mid \mathrm{k}$

## Soln:

Let $\mathrm{n}, \mathrm{n}+1, \mathrm{n}+2$ be the three consecutive integers.
Given $\mathrm{n}^{3}+(\mathrm{n}+1)^{3}+(\mathrm{n}+2)^{3}$ is a cube $\mathrm{k}^{3}$
$\Rightarrow \mathrm{n}^{3}+\mathrm{n}^{3}+3 \mathrm{n}^{2}+3 \mathrm{n}+1+\mathrm{n}^{3}+3 \mathrm{n}^{2} \cdot 2+3 \mathrm{n} \cdot 2^{2}+2^{3}=\mathrm{k}^{3}$
$\Rightarrow 3 \mathrm{n}^{3}+9 \mathrm{n}^{2}+15 \mathrm{n}+9=\mathrm{k}^{3}$
$\Rightarrow 3\left(\mathrm{n}^{3}+3 \mathrm{n}^{2}+5 \mathrm{n}+3\right)=\mathrm{k}^{3}$
$\Rightarrow 3\left|\mathrm{k}^{3} \Rightarrow 3\right| \mathrm{k} \cdot \mathrm{k} \cdot \mathrm{k}$
Since 3 is a prime, $3 \mid k$

## Base-b representation:

The expression $a_{k} b^{k}+a_{k-1} b^{k-1}+\ldots . .+a_{1} b+a_{0}$ is the base-b representation of the integer N .
Accordingly, we write $N=\left(a_{k} a_{k-1} \ldots . . a_{1} a_{0}\right)_{b}$ 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 $0,1,2,3, \ldots 9, A, B, C, D, E$, 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:

$$
\begin{aligned}
(101011111)_{2} & =1\left(2^{8}\right)+0\left(2^{7}\right)+1\left(2^{6}\right)+0\left(2^{5}\right)+1\left(2^{4}\right)+1\left(2^{3}\right)+1\left(2^{2}\right)+1\left(2^{1}\right)+1\left(2^{0}\right) \\
& =256+64+16+8+4+2+1=351
\end{aligned}
$$

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

## Soln:

We know $\mathrm{A}=10, \mathrm{~B}=11, \mathrm{E}=14$

$$
\begin{aligned}
(3 \mathrm{AB} 0 \mathrm{E})_{16} & =3\left(16^{4}\right)+A\left(16^{3}\right)+\mathrm{B}\left(16^{2}\right)+0\left(16^{1}\right)+E\left(16^{0}\right) \\
& =3\left(16^{4}\right)+10\left(16^{3}\right)+11\left(16^{2}\right)+0\left(16^{1}\right)+14\left(16^{0}\right) \\
& =196608+40960+2816+14=240398
\end{aligned}
$$

## 3. Express 1776 in the octal system.

## Soln:

1776=222(8)+0
$222=27(8)+6$
$27=3(8)+3$
$3=0(8)+\mathbf{3}$
$1776=(3360)_{8}$
4. Find the value of the base $b$ so that $144_{b}=49$.

## Soln:

$144_{b}=49 \Rightarrow 1 \times b^{2}+4 \times b^{1}+4 \times b^{0}=49$
$\Rightarrow b^{2}+4 b+4=49$
$\Rightarrow b^{2}+4 b-45=0$
$\Rightarrow(b+9)(b-5)=0$
$\sin c e b \neq-9$,
$\therefore b=5$

## Number Patterns:

Consider the following number patter,

$$
\begin{aligned}
1 \cdot 9+2 & =11 \\
12 \cdot 9+3 & =111 \\
123 \cdot 9+4 & =1111 \\
1234 \cdot 9+5 & =11111
\end{aligned}
$$

In general,
$123 \ldots(\mathbf{n}) \cdot 9+(\mathbf{n}+\mathbf{1})=\underbrace{\mathbf{1 1 1} \ldots \mathbf{1 1}}_{\mathrm{n}+1 \text { ones }}$

1. Add two more rows to the following pattern, and write conjecture formula for the $\mathbf{n}^{\text {th }} \mathbf{r o w}$ :

$$
9 \cdot 9+7=88
$$

$98 \cdot 9+6=888$
$\mathbf{9 8 7} \cdot 9+5=8888$
$9876 \cdot 9+4=88888$
$98765 \cdot 9+3=888888$
Soln:
The next two rows of the given patterns are,
$987654 \cdot 9+2=8888888$
$9876543 \cdot 9+1=88888888$
The general pattern is
$98765 \ldots . .(10-n) \cdot 9+(8-n)=\underbrace{888 \ldots . .88}_{(n+1) \text { Eighs }}$
2. Consider the number pattern
$10^{2}-10+1=91$
$10^{4}-10^{2}+1=9901$
$10^{6}-10^{3}+1=999001$
$10^{8}-10^{4}+1=99990001$
Conjecture a formula for the ${ }^{\text {th }}$ row of thispattern and establish the validity of the formula.
Soln:
$n^{\text {th }}$ row is : $10^{2 n}-10^{n}+1=\underbrace{999 \cdots 9}_{\mathrm{n} \text { times }} \underbrace{000 \cdots 0}_{(\mathrm{n}-1)} 1$
LHS : $10^{2 n}-10^{n}+1=10^{n}\left(10^{n}-1\right)+1$
$=10^{n}(\underbrace{999 \cdots 9}_{\mathrm{n} \text { times }})+1$

$$
\begin{aligned}
& =\underbrace{999 \cdots 9}_{n \text { times }} \underbrace{000 \cdots 0}_{n \text { zeros }}+1 \\
& =\underbrace{999 \cdots 9}_{n \text { times }} \underbrace{000 \cdots 0}_{(n-1) \text { zeros }} 1
\end{aligned}
$$

## Prime and Composite Numbers:

A positive integer $\mathrm{p}>1$ is called a prime number if its only positive factors are a and p . If $\mathrm{P}>1$ is not a prime, then it is called a composite number.

## 1. Theorem (Euclid): There are infinitely many primes. <br> Proof:

We prove by contradiction method.
Assume that there are only n primes $p_{1}, p_{2}, \ldots, p_{n}$ where n is prime.
Now consider the integer
$m=p_{1} \cdot p_{2} \cdot \mathrm{p}_{3} \ldots, p_{n}$
Since $m>1$, by theorem, every integer $n \geq 2$ has a prime factor..$\therefore \mathrm{m}$ has a prime factor p .
But none of the primes $p_{1}, p_{2}, \mathrm{p}_{3}, \ldots, p_{n}$ divide m
For, if $\mathrm{p}_{i} \mid \mathrm{m}$ and since $p_{i} \mid p_{1} \cdot p_{2} \cdot \mathrm{p}_{3} \ldots, p_{n}$
we get $p_{i}\left|\mathrm{~m}-p_{1} \cdot p_{2} \cdot \mathrm{p}_{3} \ldots, p_{n} \Rightarrow p_{i}\right| 1$, which is not true and hence a contradiction.

$$
\therefore \mathrm{p}_{i}+m
$$

So, we have a prime p which is not in the list of n primes. Thus, we have $\mathrm{n}+1$ primes $p_{1}, p_{2}, \mathrm{p}_{3}, \ldots, p_{n}, p_{n+1}$ 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 $\mathrm{n}=2$, 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 $\mathrm{k}+1$ :
If $k+1$ is a prime, then $k+1$ is a prime factor of $k+1$.
If $\mathrm{k}+1$ is not a prime, then $\mathrm{k}+1$ must be a composite number.
So, it must have factor d , where $\mathrm{d} \leq k$. Then by the induction hypothesis, d has a prime factor p .
Since $\mathrm{p} \mid \mathrm{d}$ and $\mathrm{d} \mid \mathrm{k}+1$, we have $\mathrm{p} \mid \mathrm{k}+1$. So p is a factor of $\mathrm{k}+1$.

Hence by second principle of induction the statement is true for every integer >1
$\therefore$ Every integer $\mathrm{n} \geq 2$ has a prime factor.
3. Every composite number $\mathbf{n}$ has a prime factor $\leq\lfloor\sqrt{\mathrm{n}}\rfloor$.

## Proof:

Given n is a composite number.
Then there exist positive integer a and b such that $\mathrm{n}=\mathrm{ab}$, where $1<\mathrm{a}<\mathrm{n}, 1<\mathrm{b}<\mathrm{n}$.
We will prove $a \leq \sqrt{\mathrm{n}}$ or $\mathrm{b} \leq \sqrt{\mathrm{n}}$.
Suppose $a>\sqrt{\mathrm{n}}$ and $b>\sqrt{\mathrm{n}}$
Then $\mathrm{a} \cdot \mathrm{b}>\sqrt{\mathrm{n}} \cdot \sqrt{\mathrm{n}}=\mathrm{n}$
$\Rightarrow \mathrm{a} \cdot \mathrm{b}>\mathrm{n}$
which is impossible, either $\mathrm{a} \leq\lfloor\sqrt{\mathrm{n}}\rfloor$. or $b \leq\lfloor\sqrt{\mathrm{n}}\rfloor$.
we know that every positive integer $\geq 2$ 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 $\leq\lfloor\sqrt{\mathrm{n}}\rfloor$.

## Theorem:

Let $\mathrm{p}_{1}, \mathrm{p}_{2}, \ldots, \mathrm{p}_{\mathrm{r}}$ be the primes $\leq\lfloor\sqrt{\mathrm{n}}\rfloor$. Then the number of prime $\leq \mathrm{n}$ is $\pi(\mathrm{n})=n-1+\pi(\sqrt{\mathrm{n}})-\sum_{i}\left\lfloor\frac{\mathrm{n}}{\mathrm{p}_{\mathrm{i}}}\right\rfloor+\sum_{i<j}\left\lfloor\frac{\mathrm{n}}{\mathrm{p}_{\mathrm{i}} \mathrm{p}_{\mathrm{j}}}\right\rfloor-\sum_{i<j<k}\left\lfloor\frac{\mathrm{n}}{\mathrm{p}_{\mathrm{i}} \mathrm{p}_{\mathrm{j}} \mathrm{p}_{\mathrm{k}}}\right\rfloor+\ldots+(-1)^{n} \sum_{i<j<k \times r}\left\lfloor\frac{\mathrm{n}}{\mathrm{p}_{\mathrm{i}} \mathrm{p}_{\mathrm{j}} \mathrm{p}_{\mathrm{k}} \ldots \mathrm{p}_{r}}\right\rfloor$

## 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 $\leq\lfloor\sqrt{n}\rfloor$, then n is a prime consider prime number $\leq\lfloor\sqrt{1601}\rfloor \Rightarrow$ prime number $\leq 40$ (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 $\leq 100$

## Soln:

Here $\mathrm{n}=100$, and $\sqrt{100}=10$
Primes which are less than or equal to 10 are:2,3,5,7.
Then the number of prime $\leq 100$ is

$$
\begin{aligned}
& \pi(\mathrm{n})=n-1+\pi(\sqrt{\mathrm{n}})-\sum_{i}\left\lfloor\frac{\mathrm{n}}{\mathrm{p}_{\mathrm{i}}}\right\rfloor+\sum_{i<j}\left\lfloor\frac{\mathrm{n}}{\mathrm{p}_{\mathrm{i}} \mathrm{p}_{\mathrm{j}}}\right\rfloor-\sum_{i<j<k}\left\lfloor\frac{\mathrm{n}}{\mathrm{p}_{\mathrm{i}} \mathrm{p}_{\mathrm{j}} \mathrm{p}_{\mathrm{k}}}\right\rfloor+\ldots+(-1)^{n} \sum_{i<j<k \ldots r r}\left\lfloor\frac{\mathrm{n}}{\mathrm{p}_{\mathrm{i}} \mathrm{p}_{\mathrm{j}} \mathrm{p}_{\mathrm{k}} \ldots \mathrm{p}_{r}}\right\rfloor \\
& \pi(100)=100-1+\pi(\sqrt{100})-\left\{\left\lfloor\frac{100}{2}\right\rfloor+\left\lfloor\frac{100}{3}\right\rfloor+\left\lfloor\frac{100}{5}\right\rfloor+\left\lfloor\frac{100}{7}\right\rfloor\right\} \\
& +\left\{\left\lfloor\frac{100}{2 \times 3}\right\rfloor+\left\lfloor\frac{100}{2 \times 5}\right\rfloor+\left\lfloor\frac{100}{2 \times 7}\right\rfloor+\left\lfloor\frac{100}{3 \times 5}\right\rfloor+\left\lfloor\frac{100}{3 \times 7}\right\rfloor+\left\lfloor\frac{100}{5 \times 7}\right\rfloor\right\} \\
& -\left\{\left\lfloor\frac{100}{2 \times 3 \times 5}\right\rfloor+\left\lfloor\frac{100}{2 \times 3 \times 7}\right\rfloor+\left\lfloor\frac{100}{2 \times 5 \times 7}\right\rfloor+\left\lfloor\frac{100}{3 \times 5 \times 7}\right\rfloor\right\}+\left\lfloor\frac{100}{2 \times 3 \times 5 \times 7}\right\rfloor \\
& =99+4-\{50+33+20+14\}+\{16+10+7+6+4+2\}-\{3+2+1+0\}+0 \\
& =103-117+45-6 \\
& =25
\end{aligned}
$$

## 4. Find the smallest prime factor of 129 .

## Solution:

Here $\mathrm{n}=129$, and $\lfloor\sqrt{129}\rfloor=11$
Primes which are less than or equal to 11 are: 2,3,5,7,11.
$2 \dagger 129$ 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
$(n+1)!+2,(n+1)!+3, \ldots \ldots,(n+1)!+(n+1)$ Where $\mathrm{n} \geq 1$.
Let $2 \leq k \leq n+1$
Then $k \mid(n+1)$ ! and always $k \mid k$
$\Rightarrow k \mid[(n+1)!+k]$, for every $k=2,3, \ldots(n+1)$
$\Rightarrow 2|[(n+1)!+2], 3|[(n+1)!+3], \ldots \ldots,(n+1) \mid[(n+1)!+(n+1)]$
$\Rightarrow(n+1)!+2,(n+1)!+3, \ldots .,(n+1)!+(n+1)$ 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 $\mathrm{n}=6$
$\therefore$ The six consecutive composite numbers are $5042,5043,5044,5045,5046$, and 5047

## 3. Prove that any prime of the form $3 k+1$ is of the form $6 k+1$.

## Soln.:

Let the prime $\mathrm{p}=3 \mathrm{k}+1$, then k must be even.
[if k is odd, then 3 k is odd $\Rightarrow 3 \mathrm{k}+1$ is even $\Rightarrow 3 \mathrm{k}+1$ is not prime]
$\therefore \mathrm{k}=2 \mathrm{k}^{\prime}$, then $\mathrm{p}=3\left(2 \mathrm{k}^{\prime}\right)+1=6 \mathrm{k}^{\prime}+1$.
Hence any prime of the form $3 \mathrm{k}+1$ is of the form $6 \mathrm{k}+1$.
4. Show that product of $k$ consecutive integers is divisible by $k$ !

## Proof:

Let $(n+1),(n+2), \cdots \cdots,(n+k)$ be the ' k ' consecutive integer.
Product of ' k ' consecutive integer $=(n+1)(n+2) \cdots \cdots(n+k)$

$$
\begin{aligned}
& =\frac{n!}{n!}(n+1)(n+2) \cdots \cdots(n+k) \\
& =\frac{(n+k)!}{n!}
\end{aligned}
$$

Product of ' k ' consecutive integer $=\frac{\mathrm{k}!(n+k)!}{\mathrm{k}!n!}=\mathrm{k}!n+r C_{r}=$ 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 $\operatorname{gcd}(a, b)$ 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 $g c d$ to positive integers.

## Definition:

A positive integer $d$ is the $\mathbf{g c d}$ of integers $a$ and $b$ if
(i). $d \mid a$ and $d \mid b$
(ii).If $c \mid a$ and $c \mid b$, then $c \mid d$, 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 $\mathbf{a} \& b$. Proof:

LetS be the set of positive linear combination of a and b ; that is $S=\{m a+n b / m a+n b>0, m, n \in Z\}$
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 $\mathrm{S}, \mathrm{d}=\alpha a+\beta b$ for some integer $\alpha$ and $\beta$.
(1). First we will show that $d / a$ and $d / b$ :

By the division algorithm, there exist integers q and r such that $a=d q+r$,
where $0 \leq r<d$. Substituting for $d$.

$$
\begin{aligned}
\mathrm{r} & =\mathrm{a}-\mathrm{dq} \\
& =\mathrm{a}-(\alpha a+\beta b) q \\
& =(1-\alpha q) a+(-\beta q) b
\end{aligned}
$$

This shows $r$ is a linear combination of a and $b$.
If $r>0$, then $\mathrm{r} \in S$. Since $r<d$, r is less than the smallest element in S .
Which is a contrdiction. So $r=0$; thus, $\mathrm{a}=\mathrm{dq}$, so $\mathrm{d} \mid \mathrm{a}$.
Similarly, d|b. Thus d is common divisor of a and b .
(2).To show that any positive common divisior $d^{\prime}$ of a and $b$ is $\leq d$ :

Since $d^{\prime} \mid \mathrm{a}$, and $d^{\prime}\left|b \Rightarrow d^{\prime}\right|(\alpha a+\beta b)$
that is $d^{\prime} \mid d$. So $d^{\prime} \leq d$.
Thus, by parts (1) and (2), $\mathrm{d}=(a, b)$
2.Two positive integer $a$ and $b$ are relatively prime if and only iff there are integers $\alpha$ and $\beta$ such that $\alpha \mathrm{a}+\beta \mathrm{b}=1$.

## Proof:

Assume that a and b are relatively prime, then $(\mathrm{a}, \mathrm{b})=1$
We know that, there exist integer $\alpha$ and $\beta$ such that

$$
\begin{aligned}
& (a, b)=\alpha \mathrm{a}+\beta \mathrm{b} \\
& \Rightarrow 1=\alpha \mathrm{a}+\beta \mathrm{b}
\end{aligned}
$$

Conversely, assume that there exist integers $\alpha$ and $\beta$ such that $\alpha \mathrm{a}+\beta \mathrm{b}=1$.
Let $\mathrm{d}=(\mathrm{a}, \mathrm{b})$. Then $\mathrm{d} \mid \mathrm{a}$ and $\mathrm{d} \mid \mathrm{b}$.
$\Rightarrow d|(\alpha \mathrm{a}+\beta \mathrm{b}) \Rightarrow \mathrm{d}| 1 \Rightarrow \mathrm{~d}=1$
$\Rightarrow(\mathrm{a}, \mathrm{b})=1 \Rightarrow \mathrm{a}$ and b are relatively prime.
3. If $\mathrm{d}=(\mathrm{a}, \mathrm{b})$, then $\left(\frac{a}{d}, \frac{b}{d}\right)=1$

## Proof:

Since $d$ is gcd of $a$ and $b \Rightarrow d$ is positive integer
$\mathrm{d}=(\mathrm{a}, \mathrm{b}) \Rightarrow$ there exist integers $\alpha$ and $\beta$ such that $\mathrm{d}=\alpha \mathrm{a}+\beta \mathrm{b}$
$\Rightarrow 1=\alpha\left(\frac{a}{d}\right)+\beta\left(\frac{b}{d}\right)$
$\Rightarrow$ by the above theorem $\frac{\mathrm{a}}{\mathrm{d}}$ and $\frac{\mathrm{b}}{\mathrm{d}}$ are relatively prime
$\Rightarrow\left(\frac{a}{d}, \frac{b}{d}\right)=1$
4. If $(a, b)=1=(a, c)$ then $(a, b c)=1$

## Proof:

$(\mathrm{a}, \mathrm{b})=1 \Rightarrow$ there exist integers $\alpha$ and $\beta$ such that $\alpha \mathrm{a}+\beta \mathrm{b}=1----(1)$
$(\mathrm{a}, \mathrm{c})=1 \Rightarrow$ there exist integers $\gamma$ and $\delta$ such that $\gamma \mathrm{a}+\delta \mathrm{c}=1-----(2)$
Using (2) in (1),
$\alpha a+\beta b(1)=1$
$\alpha a+\beta b(\gamma \mathrm{a}+\delta \mathrm{c})=1$
$\alpha a+\beta \gamma \mathrm{ab}+\beta \delta b \mathrm{c}=1$
$(\alpha+\beta \gamma \mathrm{b}) \mathrm{a}+(\beta \delta) b \mathrm{c}=1 \Rightarrow(\mathrm{a}, \mathrm{bc})=1$
5. Prove that $(a, a-b)=1$ if and only if $(a, b)=1$

## Proof:

$\operatorname{Let}(a, b)=1$
Then there exist integer 1 and m such that
$l a+m b=1$
$l a+m a+m b-m a=1$
$(l+m) a-m(a-b)=1$
$(l+m) a+(-m)(a-b)=1 \Rightarrow(a, a-b)=1$
Conversely, let $(a, a-b)=1$. To prove: $(a, b)=1$
Then there exist integer $\alpha$ and $\beta$ 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 $d^{\prime}$ is any common divisor of $a$ and $b$, then $d^{\prime} \mid d$.

## Proof:

Since $\mathrm{d}=(\mathrm{a}, \mathrm{b}), \exists, \alpha$ and $\beta$ such that $\mathrm{d}=\alpha a+\beta b$.
also since $\mathrm{d}^{\prime}$ is common divisor of $\mathrm{a} \& \mathrm{~b} . \therefore \mathrm{d}^{\prime}\left|\mathrm{a} \& \mathrm{~d}^{\prime}\right| \mathrm{b}$
$\Rightarrow \mathrm{d}^{\prime} \mid(\alpha \mathrm{a}+\beta \mathrm{b})$; so $\mathrm{d}^{\prime} \mid \mathrm{d}$.

## Problem:

## 1. Find the GCD of $1819 \& 3587$.

Soln:

$$
\begin{aligned}
& (3587,1819)=1 \times 1819+1768 \\
& (1819,1768)=1 \times 1768+51 \\
& (1768,51)=34 \times 51+34 \\
& (51,34)=1 \times 34+17 \\
& (34,17)=2 \times 17+0
\end{aligned}
$$

$\therefore$ gcd of 1819,3587 is 17
2. Find the GCD of $a+b, a^{2}-b^{2}$.

$$
G C D\left(a+b, a^{2}-b^{2}\right)=G C D(a+b,(a-b)(a+b))=a+b
$$

3. If $(a, 4)=2 \&(b, 4)=2$ show that $(a+b, 4)=2$

Soln.:
$(a, 4)=2 \Rightarrow \operatorname{gcd}$ of $(a, 4)=2 \Rightarrow 2 / a$ but $4+a \therefore a=2 k$, and k is odd
$(\mathrm{b}, 4)=2 \Rightarrow \operatorname{gcd}$ of $(\mathrm{b}, 4)=2 \Rightarrow 2 / \mathrm{b}$ but $4+\mathrm{b} \therefore b=2 l$, and $l$ is odd
$a+b=2 k+2 l=2(k+l)=2($ even $)=2(2 m)=4 m$
$\therefore 4 / a+b \Rightarrow \operatorname{gcd}(a+b, 4)=4$

## 3. Evaluate by apply Euclidean Algorithm $(2076,1776)$

## Solu.:

By successive application of division algorithm, we get:

$$
\begin{aligned}
& 2076=1 \cdot 1776+300 \\
& 1776=5 \cdot 300+276 \\
& 300=1 \cdot 276+24 \\
& 276=11 \cdot 24+12 \\
& 24=2 \cdot 12+1
\end{aligned}
$$

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:

$$
\begin{aligned}
4076 & =3 \cdot 1024+1004 \\
1024 & =1 \cdot 1004+20 \\
1004 & =50 \cdot 20+4 \\
20 & =5 \cdot 4+0
\end{aligned}
$$

Since the last nonzero remainder is $(4076,1024)=4$

$$
\begin{aligned}
&(4076,1024)= 4 \\
&=1004-50 \cdot 20 \\
&=1004-50(1024-1 \cdot 1004) \\
&=51 \cdot 1004-50 \cdot 1024 \\
&=51(4076-3 \cdot 1024)-50 \cdot 1024 \\
&=51 \cdot 4076+(-203) \cdot 1024
\end{aligned}
$$

5. Apply Euclidean Algorithm to express the gcd of $(1976,1776)$ as a linear combination of $\mathbf{1 9 7 6}, 1776$.

## Soln.:

By successive application of division algorithm, we get:

$$
\begin{gathered}
1976=1 \cdot 1776+200 \\
1776=8 \cdot 200+176 \\
200=1 \cdot 176+24 \\
176=7.24+8 \\
24=3 \cdot 8+0
\end{gathered}
$$

Since the last nonzero remainder is $(1976,1776)=8$

$$
\begin{aligned}
(1976,1776)=8 & =176-7 \cdot 24 \\
& =176-7(200-1 \cdot 176) \\
& =8 \cdot 176-7 \cdot 200 \\
& =8(1776-8 \cdot 200)-7 \cdot 200 \\
& =8 \cdot 1776-71 \cdot 200 \\
& =8 \cdot 1776-71(1976-1.1776) \\
& =79.1776-71.1976 \\
& =79.1776+(-71) .1976
\end{aligned}
$$

Hence the gcd is a linear combination of numbers 1976,1776 .

## 6. Using recursion, evaluate ( $\mathbf{1 5 , 2 8 , 5 0 )}$.

## Soln.:

$$
\begin{aligned}
(15,28,50) & =(15,50,28) \\
& =((15,50), 28) \\
& =(5,28)=1
\end{aligned}
$$

1 is the $\operatorname{GCD}(15,28,50)$

## 7. Using recursion, evaluate ( $18,30,60,75,132$ ).

Soln:

$$
\begin{aligned}
(18,30,60,75,132) & =((18,30,60,75), 132) \\
& =(((18,30,60), 75), 132) \\
& =((((18,30), 60), 75), 132) \\
& =(((6,60), 75), 132) \\
& =((6,75), 132)=(3,132)=3
\end{aligned}
$$

## 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 $\mathrm{P}(\mathrm{n})$ denote the statement that n is a prime or can be expressed as a product of primes.

## (i) To show that $\mathbf{P}(\mathbf{n})$ is true for every integer $\mathbf{n} \geq \underline{2}$ :

Since 2 is a prime, clearly $\mathrm{P}(2)$ is true.
Now assume $\mathrm{P}(2), \mathrm{P}(3), \ldots . \mathrm{P}(\mathrm{k})$ 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 $k+1=a b$ for some integers $a$ and $b$, where $1<\mathrm{a}, \mathrm{b}<\mathrm{k}+1$. By the inductive hypothesis, a and b either are primes or can be expressed as products of primes; in any event, $\mathrm{k}+1=\mathrm{ab}$ can be expressed as products of primes. Thus, $\mathrm{P}(\mathrm{k}+1)$ 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 $\mathrm{r}=\mathrm{s}$ and every $\mathrm{p}_{i}$ 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 $p_{1} p_{2} \cdots \cdots p_{r}=q_{1} q_{2} \cdots \cdots q_{s}, p_{1} / q_{1} q_{2} \cdots q_{s}, \Rightarrow \mathrm{p}_{1}=q_{i}$ 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:
$p_{3} \ldots . . p_{r}=q_{1} q_{2} \ldots q_{i-1} q_{i} q_{i+1} \ldots q_{j-1} q_{j} q_{j+1} q_{s}$
Since $r \leq s$, continuing like this, we can cancel $p_{t}$ with some $q_{k} \cdot$ 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, $\mathrm{r}=\mathrm{s}$ and hence the primes $q_{1}, q_{2}, \ldots . . q_{s}$ are the same as the primes $p_{1} p_{2} \cdots p_{r}$ 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.
$168=2^{3} \cdot 3 \cdot 7 \quad 180=2^{2} \cdot 3^{2} \cdot 5$
$G C D=(168,280)=2^{2} \cdot 3=12$

## 2. Find the canonical decomposition of $\mathbf{2}^{\boldsymbol{9}} \mathbf{- 1}$

$$
\begin{aligned}
2^{9}-1=\left(2^{3}\right)^{3}-1^{3} & =\left(2^{3}-1\right)\left(2^{6}+2^{3}+1\right) \quad \because a^{3}-b^{3}=(a-b)\left(a^{2}+a b+b^{2}\right) \\
& =(7)(73)
\end{aligned}
$$

## 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 $[\mathrm{a}, \mathrm{b}]$.

## 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. <br> Soln.:

$$
168=2^{3} \cdot 3 \cdot 7 \quad 180=2^{2} \cdot 3^{2} \cdot 5
$$

$G C D=(168,280)=2^{2} \cdot 3=12$
$L C M=[168,280]=2^{3} \cdot 3^{2} \cdot 5 \cdot 7=2520$

## 3. Find the canonical decomposition of 23!

## Soln.:

The prime dividing 23 ! are 2,3,5.7,11,17,19,23
The power of 2 dividing 23 ! are $=\left[\frac{23}{2}\right]+\left[\frac{23}{2^{2}}\right]+\left[\frac{23}{2^{3}}\right]+\left[\frac{23}{2^{4}}\right]$

$$
\begin{aligned}
& =11+5+2+1 \\
& =19
\end{aligned}
$$

The power of 3 dividing 23! are $=\left[\frac{23}{3}\right]+\left[\frac{23}{3^{2}}\right]$

$$
\begin{aligned}
& =7+2 \\
& =9
\end{aligned}
$$

The power of 5 dividing 23! are $=\left[\frac{23}{5}\right]+\left[\frac{23}{5^{2}}\right]$

$$
=4+0=4
$$

The power of 7 dividing 23! are $=\left[\frac{23}{7}\right]=3$
The power of 11 dividing 23 ! are $=\left[\frac{23}{11}\right]=2$
The power of 13 dividing 23! are $=\left[\frac{23}{13}\right]=1$
The power of 17 dividing 23! are $=\left[\frac{23}{17}\right]=1$
The power of 19 dividing 23! are $=\left[\frac{23}{19}\right]=1$
The power of 23 dividing 23! 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 $[a, b]=\frac{a b}{(a, b)} \quad$ (or)
Prove that the product of ged and $\mathbf{l c m}$ of any two positive integers a and $\mathbf{b}$ is equal to their products.

## Proof:

Let $\mathrm{a}=\mathrm{p}_{1}^{a_{1}} \mathrm{p}_{2}^{a_{2}} \ldots . \mathrm{p}_{\mathrm{n}}^{a_{\mathrm{n}}}, \mathrm{b}=\mathrm{p}_{1}^{b_{1}} \mathrm{p}_{2}^{b_{2}} \ldots . . \mathrm{p}_{\mathrm{n}}^{b_{\mathrm{n}}}$ be the canonical decomposition of a and b . Then

$$
\begin{aligned}
& {[a, b]=\mathrm{p}_{1}^{\max \left\{a_{1}, b_{1}\right\}} \mathrm{p}_{2}^{\max \left\{a_{2}, b_{2}\right\}} \ldots . . \mathrm{p}_{\mathrm{n}}^{\max \left\{a_{\mathrm{n}}, b_{n}\right\}}} \\
& \begin{aligned}
&(a, b)=\mathrm{p}_{1}^{\min \left\{a_{1}, b_{1}\right\}} \mathrm{p}_{2}^{\min \left\{a_{2}, b_{2}\right\}} \ldots \ldots \mathrm{p}_{\mathrm{n}}^{\min \left\{a_{\mathrm{n}}, b_{n}\right\}} \\
& \Rightarrow[a, b](a, b)=\mathrm{p}_{1}^{\max \left\{a_{1}, b_{1}\right\}+\min \left\{a_{1}, b_{1}\right\}} \mathrm{p}_{2}^{\max \left\{a_{2}, b_{2}\right\}+\min \left\{a_{2}, b_{2}\right\}} \ldots \ldots \mathrm{p}_{\mathrm{n}}^{\max \left\{a_{\mathrm{n}}, b_{n}\right\}+\min \left\{a_{\mathrm{n}}, b_{n}\right\}} \\
&=\mathrm{p}_{1}^{a_{1}+b_{1}} \mathrm{p}_{2}^{a_{2}+b_{2}} \ldots . . \mathrm{p}_{\mathrm{n}}^{a_{\mathrm{n}}+b_{n}} \\
&=\left(\mathrm{p}_{1}^{a_{1}} \mathrm{p}_{2}^{a_{2}} \ldots \ldots \mathrm{p}_{\mathrm{n}}^{a_{\mathrm{n}}}\right)\left(\mathrm{p}_{1}^{b_{1}} \mathrm{p}_{2}^{b_{2}} \ldots . . \mathrm{p}_{\mathrm{n}}^{b_{\mathrm{n}}}\right) \\
&=\mathbf{a b}
\end{aligned}
\end{aligned}
$$

Hence $[a, b]=\frac{a b}{(a, b)}$

## Problem:

1. Using (252, 360) compute [252, 360].

Since GCD of $(252,360)=36$
$[a, b]=\frac{a b}{(a, b)} \Rightarrow[252,360]=\frac{252 \times 360}{36}=2520$

## 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 $(\mathrm{n}, \mathrm{n}+1)=1$.

By formula, $[a, b]=\frac{a b}{(a, b)}=\frac{\mathrm{n}(\mathrm{n}+1)}{1}=\mathrm{n}^{2}+\mathrm{n}$

## 3. Find a positive integer $\mathbf{a}$, if $[a, a+1]=132$.

## Soln.:

We know that $[a, b]=\frac{a b}{(a, b)}-----(1)$
Since LCM of $[a, a+1]=132 \&$ GCD of $(a, a+1)=1$
$(1) \Rightarrow 132=\frac{a \times a+1}{1} \Rightarrow a^{2}+a-132=0 \Rightarrow a=-12,11 \quad$ Since $a$ is positive integer, $a=11$

# MOHAMED SATHAK A.J.COLLEGE OF ENGINEERING <br> MA8551- ALGEBRA \& NUMBER THEORY <br> NOTES 

## 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 $a x+b y=c$, where $a, b, c$ areintegers.

## Theorem

The linear Diophantine equation $a x+b y=c$ 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 $x=x_{0}+\left(\frac{b}{d}\right) t \quad$ and $\quad y=y_{0}-\left(\frac{a}{d}\right) t, \quad t \in Z$

## Proof:

Assume the linear Diophantine equation $a x+b y=c$ is solvable.
To prove $d \mid c$
If $x=\alpha, y=\beta$ is a solution, then $\alpha a+\beta b=c$

$$
\begin{aligned}
& \text { Since } d=(a, b), d \mid a \text { and } d \mid b \\
& \Rightarrow d \mid \alpha a+\beta b \\
& \Rightarrow d \mid c
\end{aligned}
$$

1. Determine whether the $\operatorname{LDE} 2 x+3 y+4 z=5$ is solvable?

## Solution:

The $\operatorname{gcd}(2,3,4)=1$
i.e., $(2,3,4)=1$ and $1 / 5$

The given LDE is Solvable.
2. Find the general solution of the LDE $15 x+21 y=39$

## Solution:

$15 x+21 y=39 \Rightarrow a=15, b=21, c=39$.
$d=(15,21)$ and $d / 39 \Rightarrow d=3$
So, the given LDE is solvable.

$$
\begin{aligned}
& 15 x+21 y=39 \\
& \Rightarrow 5 x+7 y=13------(1) \\
& \text { then }(5,7)=d=1 \\
& \therefore d / 13 \\
& a=5, b=7, d=1
\end{aligned}
$$

We find $x_{0}=-3, y_{0}=4$ is a solution of (1) is
$x=x_{0}+\frac{b}{d} t \quad$ and $\quad y=y_{0}-\frac{a}{d} t, \quad t \in Z$
$x=-3+\frac{7}{1} t \quad$ and $\quad y=4-\frac{5}{1} t, \quad t \in Z$
$x=-3+7 t \quad$ and $\quad y=4-5 t, \quad t \in Z$
3. Find the general solution of the LDE $6 x+8 y+12 z=10$

## Solution:

Given the LDE is $6 x+8 y+12 z=10$
Here $a_{1}=6, a_{2}=8, a_{3}=12, c=10$
$\therefore\left(a_{1} \cdot a_{2}, a_{3}\right)=(6,8,12)=2$ and $c=10$
$\therefore \quad d=\left(a_{1} \cdot a_{2}, a_{3}\right)=2$
Since $2|10, d| c$
So, the given LDE is solvable.
Since $8 y+12 z$ is a linear combination of 8 and 12 , it must be a multiple of $(8,12)=4$

$$
\begin{aligned}
& \therefore \quad 8 y+12 z=4 u-------(2) \\
& \therefore(1) \Rightarrow \quad 6 x+4 u=10------(3)
\end{aligned}
$$

First we solve the LDE (3) in two variables $x$ and $u$
Here $\quad a=6, b=4, c=10$

$$
\begin{aligned}
& (a, b)=(6,4)=2 \\
& d=(a, b)=2 \text { and } c=10
\end{aligned}
$$

Since $2|10, d| c$
So, the given LDE (3) is solvable.
We find $x_{0}=1, u_{0}=1$ is a solution of (3) is

$$
\begin{array}{ll}
x=x_{0}+\frac{b}{d} t & \text { and } \quad u=u_{0}-\frac{a}{d} t, \quad t \in Z \\
x=1+\frac{4}{2} t & \text { and } \quad u=1-\frac{6}{2} t, \quad t \in Z \\
x=1+2 t & \text { and } \quad u=1-3 t, \quad t \in Z
\end{array}
$$

Substituting for $u$ in (2), we get

$$
\therefore \quad 8 y+12 z=4(1-3 t)
$$

Since $\mathrm{d}=\left(\begin{array}{ll}a & b \\ 8, & 12\end{array}\right)=4$ and $4=2.8+(-1) .12$ is a linear combination of 8 and 12 .
Multiplying by $(1-3 t)$, we get

$$
\begin{aligned}
4(1-3 t) & =2(1-3 t) \cdot 8+(-1)(1-3 t) \cdot 12 \\
& =(2-6 t) \cdot 8+(-1+3 t) \cdot 12
\end{aligned}
$$

$\therefore$ a solution of (2) is
$y_{0}=2-6 t \quad$ and $\quad z_{0}=-1+3 t, \quad t \in Z$
So, the general solution of (2) is
$y=y_{0}+\frac{b}{d} t^{\prime} \quad$ and $\quad z=z_{0}-\frac{a}{d} t^{\prime}, \quad t^{\prime} \in Z$
$y=2-6 t+\frac{12}{4} t^{\prime} \quad$ and $\quad z=-1+3 t-\frac{8}{4} t^{\prime}, \quad t^{\prime} \in Z$
$y=2-6 t+3 t^{\prime} \quad$ and $z=-1+3 t-2 t^{\prime}, \quad t^{\prime} \in Z$
Thus the general solution of (1) is

$$
x=1+2 t, y=2-6 t+3 t^{\prime}, \quad z=-1+3 t-2 t^{\prime}, \quad t^{\prime} \in Z
$$

## Congruence modulo m

If an integer $\mathrm{m}(\neq 0)$ divides the difference $a-b$, we say that $a$ is congruent to $b$ modulo $m$. (i.e) $a \equiv b(\bmod m)$.
4. Solve the congruence $4 x \equiv 5(\bmod 6)$.

## Solution:

$4 x \equiv 5(\bmod 6)$
Here $a=4, b=5, m=6$
$(a, m)=(4,6)=2$
$\Rightarrow 2+5 \quad$ (i.e) $(a, m)+b$
$\therefore$ The congruence has no solution.
5. Show that $\mathrm{n}^{2}+\mathrm{n} \equiv 0(\bmod 2)$ for any positive integer n .

## Proof:

$$
\begin{aligned}
& a \equiv b(\bmod k) \Rightarrow a-b \equiv k m, \quad m \in z \\
& a-b \text { is divisible by } k \\
& n=\text { even }=2 m \\
& n^{2}+n=(2 m)^{2}+(2 m) \\
& =4 m^{2}+2 m \\
& =2\left(2 m^{2}+m\right) \\
& \begin{aligned}
& n^{2}+n \text { is divisible by } 2 \\
& n=\text { odd }=2 m+1
\end{aligned} \\
& \begin{array}{r}
n^{2}+n=(2 m+1)^{2}+(2 m+1) \\
\quad=4 m^{2}+4 m+1+2 m+1 \\
\quad=4 m^{2}+6 m+2 \\
=
\end{array} \\
& =2\left(2 m^{2}+3 m+1\right)
\end{aligned}
$$

$n^{2}+n$ is divisible by 2
$\Rightarrow n^{2}+n \equiv 0(\bmod 2)$
6. Let $a \equiv b(\bmod m)$ and $c \equiv d(\bmod m)$, then prove that $a c \equiv b d(\bmod m)$.

## Solution:

Since $a \equiv b(\bmod m)$ and $c \equiv d(\bmod m)$,
$a=b+l m$ and $c=d+k m$ for some inegers $l$ and $m$.
Then $a c-b d=(a c-b c)+(b c-b d)$

$$
\begin{aligned}
& =c(a-b)+b(c-d) \\
& =c l m+b k m \\
& =(c l+b k) m
\end{aligned}
$$

So $a c \equiv b d(\bmod m)$
7. Let $a \equiv b(\bmod m)$ and $c \equiv d(\bmod m)$, then prove that $a+c \equiv b+d(\bmod m)$.

## Solution:

Since $a \equiv b(\bmod m)$ and $c \equiv d(\bmod m)$,
$a=b+l m$ and $c=d+k m$ for some inegers $l$ and $m$.
Then $a+c=(b+l m)+(d+k m)$

$$
\begin{aligned}
& =(b+d)+(l+k) m \\
& =b+d(\bmod m)
\end{aligned}
$$

8.If $a c=b c(\bmod m)$ and $(c, m)=1$, then prove that $a \equiv b(\bmod m)$.

## Solution:

Suppose $a c \equiv b c(\bmod m)$, where $(c, m)=1$.
Then $m|(a c-b c)=m| c(a-b)$.
we know that: If $a$ and $b$ are relatively prime, and if $a \mid b c$, then $a \mid c$.
$\operatorname{But}(m, c)=1, m \mid(a-b),($ i.e $) a \equiv b(\bmod m)$

## Complete residue system.

A set $x_{1}, x_{2}, \ldots, x_{m}$ is a complete residue system mod $m$ if for integer $y$, there is one and only one $x_{j}$ such that $y \equiv x_{j}(\bmod m)$.
9. Solve $x^{7}+1 \equiv 0(\bmod 7)$

## Solution:

The complete residue system (CRS) is $\{0,1,2,3,4,5,6\}$
But $4 \equiv-3(\bmod 7)$

$$
5 \equiv-2(\bmod 7)
$$

$$
6 \equiv-1(\bmod 7)
$$

The CRS is $\{0, \pm 1, \pm 2, \pm 3\}$
The CRS does not satisfy the congruence $x^{2}+1 \equiv 0(\bmod 7)$
$\therefore$ 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
$16 \equiv 2(\bmod 7)$.
We know that If $\mathrm{a} \equiv b(\bmod m)$, then $\mathrm{a}^{n} \equiv b^{n}(\bmod m)$ for any positiveinteger $n$ $16^{53} \equiv 2^{53}(\bmod 7)$.
Now express a suitable power of 2 congruent mod ulo 7 to a number lessthan 7 ,

$$
\begin{aligned}
& 2^{3} \equiv 1(\bmod 7) \\
& \therefore 2^{53} \equiv 2^{3(17)+2} \\
& \\
& \equiv\left(2^{3}\right)^{17} \cdot 2^{2} \\
& \\
& \equiv 1^{17} \cdot 4(\bmod 7) \\
& \\
& \equiv 4(\bmod 7)
\end{aligned}
$$

So $16^{53} \equiv 4(\bmod 7)$, by the transitive property.
Thus, when $16^{53}$ is divided by 7 , the remainder is 4 .
11. Find the remainder when $1!+2!+3!+\ldots .+300$ ! is divided by 13 .

## Solution:

For divisibility by 13 , we consider mod 13 .
For $r \geq 13$, $r$ ! will contain 13 as a facor.

$$
\left.\begin{array}{l}
\therefore r!\equiv 0(\bmod 13) \\
1!+2!+3!+4!+\ldots \ldots+12!+\ldots .+300! \\
\equiv 1!+2!+3!+4!+\ldots \ldots+12!+0+0+(\bmod 13) \\
\equiv 1!+2!+3!+4!+\ldots .+12!(\bmod 13) \\
\equiv 1+2+6+24+120+\ldots .+12!(\bmod 13) \\
\text { But } 2+24=26 \equiv 0(\bmod 13) \\
5!=120 \equiv 3(\bmod 13) \\
6!=5!6=3.6(\bmod 13) \\
\quad \equiv 18(\bmod 13) \\
\quad \equiv 5(\bmod 13) \\
7!=6!7
\end{array}\right)=5.7(\bmod 13)
$$

$$
\begin{aligned}
& 9!=8!9=7.9(\bmod 13) \\
& \equiv 63(\bmod 13) \\
& \equiv 11(\bmod 13) \\
& 10!=9!10=11.10(\bmod 13) \\
& \equiv 110(\bmod 13) \\
& \equiv 6(\bmod 13) \\
& 11!=10!11=6.11(\bmod 13) \\
& \equiv 66(\bmod 13) \\
& \equiv 1(\bmod 13) \\
& 12!=11!12=1.12(\bmod 13) \\
& \equiv 12(\bmod 13) \\
& 1!+2!+3!+4!+\ldots . . .+12!+\ldots . .+300!\equiv 1+6+0+3+5+9+7+11+6+1+12(\bmod 13) \\
& \equiv 61(\bmod 13) \equiv 9(\bmod 13)
\end{aligned}
$$

$\therefore$ the remainder is 9 when $1!+2!+3!+4!+\ldots . .+12!+\ldots . .+300$ ! is divided by 13 .
12. Find the remainder when $3^{181}$ is divided by 17 using modular exponentitation.

Solution:

$$
\left.\begin{array}{l}
3^{2} \equiv 9(\bmod 17) ; 3^{4} \equiv-4(\bmod 17) ; 3^{8} \equiv-1(\bmod 17) ; 3^{16} \equiv 1(\bmod 17) \\
3^{32} \equiv 1(\bmod 17) ; 3^{64} \equiv 1(\bmod 17) ; \\
3^{128} \equiv 1(\bmod 17) \\
\therefore 3^{181}
\end{array} \quad=3^{128} \cdot 3^{32} \cdot 3^{16} \cdot 3^{4} \cdot 3^{1}\right)
$$

Thus the desired remainder is 5 .
13 . Find the remainder when $3^{31}$ is divided by 7 .

$$
\begin{aligned}
& 3^{2} \equiv 2(\bmod 7) \\
& \left(3^{2}\right)^{3} \equiv 2^{3}(\bmod 7)=1(\bmod 7) \\
& 3^{6}=1(\bmod 7) \\
& \therefore 3^{31}=\left(3^{6}\right)^{5} \cdot 3 \\
& \quad \equiv 1^{5} .3(\bmod 7) \\
& \quad \equiv 3(\bmod 7)
\end{aligned}
$$

Thus the remainder is 3 .
14. Prove that $4^{2 n}+10 n \equiv 1(\bmod 25)$.

## Solution:

$$
4^{2 n}+10 n \equiv 1(\bmod 25)
$$

proof by mathematical induction
$\Rightarrow n=0$
$\left(4^{0}+0\right)-1=1-1=0$
$\Rightarrow 0$ is divisible by 25
statement is true for $n=0$.
$n=1,\left(4^{2}+10\right)-1=25$
$\Rightarrow 25$ is divisible by 25
statement is true for $n=1$.
Assume that the statement is true for $n=k$
(ie), $4^{2 k}+10 k-1=25 l$
Consider $\quad 4^{2 k+2}+10(k+1)-1$

$$
\begin{aligned}
& =4^{2 k} \cdot 16+10 k+10-1 \\
& =16(25 l-10 k+1)+10 k+9 \\
& =16(25 l)-160 k+16+10 k+9 \\
& =16(25 l)-150 k+25 \\
& =25(16 l-6 k+1) \\
& =25(y)
\end{aligned}
$$

$4^{2 k+2}+10(k+1)-1$ 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 $\left(n^{2}+n+41\right)^{2}$ is divisible by 12 .

## Solution:

First notice that product of four consecutive integers is divisible by 12 ,

$$
\begin{aligned}
& (i e),(n-1) n(n+1)(n+2) \equiv 0(\bmod 12) \\
& \left(n^{2}+n+41\right)^{2} \equiv\left(n^{2}+n+5\right)^{2}(\bmod 12)
\end{aligned}
$$

$$
\begin{aligned}
& \equiv\left(n^{4}+2 n^{3}+11 n^{2}+10 n+25\right)(\bmod 12) \\
& \equiv n\left(n^{3}+2 n^{2}-n-2\right)+1(\bmod 12) \\
& \equiv n\left[n^{2}(n+2)-(n+2)\right]+1(\bmod 12) \\
& \equiv n\left((n+2)\left(n^{2}-1\right)+1(\bmod 12)\right. \\
& \equiv(n-1) n(n+1)(n+2)+1(\bmod 12) \\
& \equiv 1(\bmod 12)
\end{aligned}
$$

Thus when $\left(n^{2}+n+41\right)^{2}$ 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 $3^{2} \equiv 9(\bmod 25)$

$$
\begin{aligned}
3^{4} & \equiv 9^{2}=81 \equiv 6(\bmod 25) \\
3^{8} & \equiv 6^{2}=36 \equiv 11(\bmod 25) \\
3^{16} & \equiv 11^{2}=121 \equiv 21(\bmod 25) \\
3^{32} & \equiv 21^{2} \equiv 16(\bmod 25) \\
3^{64} & \equiv 16^{2} \equiv 6(\bmod 25) \\
3^{128} & \equiv 6^{2} \equiv 11(\bmod 25) \\
3^{247} & =3^{128+64+32+16+4+2+1} \\
& =3^{128} \cdot 3^{64} \cdot 3^{32} \cdot 3^{16} \cdot 3^{4} \cdot 3^{2} \cdot 3 \\
3^{247} & \equiv 11.6 \cdot 16.21 \cdot 6 \cdot 9 \cdot 3(\bmod 25) \\
& \equiv 11(96)(21)(54) 3(\bmod 25) \\
& \equiv 11(-4)(-4)(4) 3(\bmod 25) \\
& \equiv 44.48(\bmod 25)
\end{aligned}
$$

$$
\begin{aligned}
& \equiv(-6)(-2)(\bmod 25) \\
& \equiv 12(\bmod 25)
\end{aligned}
$$

$\therefore$ 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:

$$
\begin{aligned}
& 3^{2} \equiv 9(\bmod 17) ; 3^{4} \equiv-4(\bmod 17) ; 3^{8} \equiv-1(\bmod 17) ; 3^{16} \equiv 1(\bmod 17) \\
& 3^{32} \equiv 1(\bmod 17) ; 3^{64} \equiv 1(\bmod 17) ; 3^{128} \equiv 1(\bmod 17) \\
& \begin{aligned}
\therefore 3^{181} & =3^{128} \cdot 3^{32} \cdot 3^{16} \cdot 3^{4} \cdot 3^{1} \\
& \equiv 1.1 .1 .13 .3(\bmod 17) \\
& \equiv 5(\bmod 17)
\end{aligned}
\end{aligned}
$$

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
$16 \equiv 2(\bmod 7)$.
We know that If $\mathrm{a} \equiv b(\bmod \mathrm{~m})$, then $\mathrm{a}^{n} \equiv b^{n}(\bmod m)$ for any positiveinteger $n$
$16^{53} \equiv 2^{53}(\bmod 7)$.
Now express a suitable power of 2 congruent $\bmod$ ulo 7 to a number lessthan 7 ,

$$
\begin{aligned}
2^{3} \equiv & \equiv(\bmod 7) \\
\therefore 2^{53} & \equiv 2^{3(17)+2} \\
& \equiv\left(2^{3}\right)^{17} \cdot 2^{2} \\
& \equiv 1^{17} \cdot 4(\bmod 7) \\
& \equiv 4(\bmod 7)
\end{aligned}
$$

So $16^{53} \equiv 4(\bmod 7)$, by the transitive property.
Thus, when $16^{53}$ is divided by 7 , the remainder is 4 .
19.Prove that p is a prime $\operatorname{iff}(\mathrm{p}-1)!+1 \equiv 0(\bmod \mathrm{p})$.

## 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) $\quad p_{1} /(p-1)$ ! Also $p_{1} / p$
we are given $(p-1)!+1 \equiv 0(\bmod p)$
$\therefore p /(p-1)!+1$
$\therefore p_{1} /(p-1)!+1$
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 $\quad \because p_{1}>1$
Hence $p$ must be prime.

## Linear Congruence

A congruence of the form $a x \equiv b(\bmod m)$, where m is a positive integer and $\mathrm{a}, \mathrm{b}$ are integers and x is a variable, is called a linear congruence.

## Chinese remainder theorem.

Let $m_{1}, m_{2}, \ldots, m_{r}$ denote $r$ positive integers that are relatively prime in pairs and let $a_{1}, a_{2}, \ldots ., a_{r}$ be any $r$ integers. Then the congruence $x \equiv a_{i}\left(\bmod m_{i}\right), \mathrm{i}=1,2, \ldots, \mathrm{r}$ have common solution.

## State and prove Chinese remainder theorem.

Let $m_{1}, m_{2}, \ldots, m_{r}$ denote $r$ positive integers that are relatively prime in pairs and let $a_{1}, a_{2}, \ldots, a_{r}$ be any $r$ integers. Then the congruence $x \equiv a_{i}\left(\bmod m_{i}\right), \mathrm{i}=1,2, \ldots, \mathrm{r}$ have common solution.

## Proof:

First we prove the existence of the solution
Let $n=m_{1} \cdot m_{2} \cdot m_{3}, \ldots m_{k}$
Let $n_{i}=\frac{n}{m_{i}}, i=1,2,3, \ldots, k$.
Since $m_{1} \cdot m_{2} \cdot m_{3} \cdot \ldots m_{k}$ are pairwise relatively prime

$$
\left(n_{i}, m_{i}\right)=1, \quad i=1,2,3, \ldots ., k
$$

Also $\quad n_{i} \equiv 0\left(\bmod m_{j}\right), i \neq j$

1. First we construct a solution to the linear system.

Since $\left(n_{i}, m_{i}\right)=1$, the congruence $n_{i} y_{i} \equiv 1\left(\bmod m_{i}\right)$ has a unique solution $y_{i}, i=1,2,3, \ldots, k$

Let $\quad x=a_{1} n_{1} y_{1}+a_{2} n_{2} y_{2}+\ldots \ldots .+a_{k} n_{k} y_{k}$
Now, we will show that x is a solution of the system of congrunces.
Since $n_{i} \equiv 0\left(\bmod m_{k}\right)$ for $i \neq k$, all terms except the $k^{\text {th }}$ term in this are congruent to 0 modulo $m_{k}$

Since $n_{k} y_{k} \equiv 1\left(\bmod m_{k}\right)$, we see that $x=a_{k} n_{k} y_{k} \equiv a_{k}\left(\bmod m_{k}\right)$, for $k=1,2,3, \ldots, n$
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 $n=m_{1} \cdot m_{2} \ldots . . m_{k}$.

Let $\quad x_{1}, x_{2}$ be two solutions of the system
To prove $x_{1} \equiv x_{2}(\bmod n)$
Since $\quad x_{1} \equiv a_{j}\left(\bmod m_{j}\right)$ and $x_{2} \equiv a_{j}\left(\bmod m_{j}\right), j=1,2,3, \ldots, k$
we have $x_{1}-x_{2} \equiv 0\left(\bmod m_{j}\right)$
$\Rightarrow \quad m_{j} \mid x_{1}-x_{2}$ for every $j$
Since $m_{1}, m_{2}, \ldots, m_{k}$ are pairwise ralatively prime,

$$
\begin{aligned}
& L C M\left[m_{1}, m_{2}, \ldots, m_{k}\right]=m_{1}, m_{2}, \ldots, m_{k} \mid x_{1}-x_{2} \\
\Rightarrow \quad & n \mid x_{1}-x_{2} \Rightarrow x_{1} \equiv x_{2}(\bmod n)
\end{aligned}
$$

Hence the solution is unique $\bmod m_{1}, m_{2}, \ldots, m_{k}$.
20. Use the Chinese remainder theorem to solve $x \equiv 1(\bmod 3), x \equiv 2(\bmod 4), x \equiv 3(\bmod 5)$.
(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 $x \equiv 1(\bmod 3)$

$$
\begin{aligned}
& x \equiv 2(\bmod 4) \\
& x \equiv 3(\bmod 5)
\end{aligned}
$$

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 $n_{1}=\frac{n}{m_{1}}=\frac{3.4 .5}{3}=20$

$$
\begin{aligned}
& n_{2}=\frac{n}{m_{2}}=\frac{3.4 .5}{4}=15 \\
& n_{3}=\frac{n}{m_{3}}=\frac{3.4 .5}{5}=12
\end{aligned}
$$

1. Wefind $y_{1}, y_{2}, y_{3}$ from the congrunces

$$
\begin{aligned}
& n_{1} y_{1} \equiv 1\left(\bmod m_{1}\right) \\
& n_{2} y_{2} \equiv 1\left(\bmod m_{2}\right) \\
& n_{3} y_{3} \equiv 1\left(\bmod m_{3}\right)
\end{aligned}
$$

We have $n_{1} y_{1} \equiv 1\left(\bmod m_{1}\right)$,

$$
20 y_{1} \equiv 1(\bmod 3),
$$

Since $20.2 \equiv 40 \equiv 1(\bmod 3)$, we see $y_{1}=2$ is a solution
We have $n_{2} y_{2} \equiv 1\left(\bmod m_{2}\right)$,

$$
15 y_{2} \equiv 1(\bmod 4),
$$

Since $15.3 \equiv 45 \equiv 1(\bmod 4)$, we see $y_{2}=3$ is a solution
We have $n_{3} y_{3} \equiv 1\left(\bmod m_{3}\right)$,

$$
12 y_{3} \equiv 1(\bmod 5),
$$

Since $12.3 \equiv 36 \equiv 1(\bmod 5)$, we see $y_{3}=3$ is a solution
2. Then solution is $\quad x \equiv a_{1} n_{1} y_{1}+a_{2} n_{2} y_{2}+a_{3} n_{3} y_{3}(\bmod n)$

$$
\begin{array}{ll}
\therefore & x \equiv 1.20 .2+2.15 .3+3.12 .3(\bmod 60) \\
\Rightarrow & x \equiv 40+90+72(\bmod 60) \\
\Rightarrow & x \equiv 238(\bmod 60) \\
\Rightarrow & x \equiv 58(\bmod 60)
\end{array}
$$

$\therefore 58$ is the unique solution $(\bmod 60)$
$\therefore$ the solution of the systemis $x \equiv 58(\bmod 60)$ and it is the unique solution.
21. Solve the congruence $x \equiv 1(\bmod 4), x \equiv 0(\bmod 3), x \equiv 5(\bmod 7)$.

## Solution:

$$
\text { Here } \begin{aligned}
a_{1} & =1, \quad a_{2}=0, \quad a_{3}=5 \\
m_{1} & =4, m_{2}=3, \quad m_{3}=7 \\
m & =m_{1} \cdot m_{2} \cdot m_{3} \\
& =4.8 .7 \\
& =84
\end{aligned}
$$

$$
\begin{aligned}
& \frac{m}{m_{1}}=\frac{84}{4}=21, \frac{m}{m_{2}}=\frac{84}{3}=28, \frac{m}{m_{3}}=\frac{84}{7}=12 \\
& \left(\frac{m}{m_{1}}, m_{1}\right)=(21,4)=1 \\
& \left(\frac{m}{m_{2}}, m_{2}\right)=(28,3)=1 \\
& \left(\frac{m}{m_{3}}, m_{3}\right)=(12,7)=1 \\
& w e k n o w t h a t \\
& \left(\frac{m}{m_{j}}\right) b_{j}=1\left(\bmod m_{j}\right) \\
& \text { For } m_{1} \Rightarrow\left(\frac{m}{m_{1}}\right) b_{1} \equiv 1\left(\bmod m_{1}\right) \\
& (21) b_{1} \equiv 1(\bmod 4) \Rightarrow 4 / 21 b_{1}-1 \\
& 21 b_{1}-1=4 k, \quad k \text { is an integer } \\
& 21 \mathrm{~b}_{1}=1+4 k \\
& b_{1}=\frac{1+4 k}{21}
\end{aligned}
$$

$$
\text { put } k=5, \quad b_{1}=1
$$

For $m_{2} \Rightarrow\left(\frac{m}{m_{2}}\right) b_{2} \equiv 1\left(\bmod m_{2}\right)$

$$
(28) b_{2} \equiv 1(\bmod 3) \Rightarrow 3 / 28 b_{2}-1
$$

$$
\Rightarrow \quad 28 b_{2}-1=3 k, \quad k \text { is an integer }
$$

$$
28 \mathrm{~b}_{2}=1+3 k
$$

$$
b_{2}=\frac{1+3 k}{28}
$$

$$
\text { put } k=9, \quad b_{2}=1
$$

For $m_{3} \Rightarrow\left(\frac{m}{m_{3}}\right) b_{3} \equiv 1\left(\bmod m_{3}\right)$

$$
(12) b_{3} \equiv 1(\bmod 7) \Rightarrow 7 / 12 b_{3}-1
$$

$$
\text { put } k_{2}=5, \quad b_{3}=3
$$

By chinese remainder theorem,

$$
\begin{aligned}
x= & \sum_{i=1}^{3}\left(\frac{m}{m_{i}}\right) a_{i} b_{i}(\bmod m) \\
& =\left(\frac{m}{m_{1}} a_{1} b_{1}+\frac{m}{m_{2}} a_{2} b_{2}+\frac{m}{m_{3}} a_{3} b_{3}\right)(\bmod m) \\
& =[(21 \times 1 \times 1)+(28 \times 0 \times 1)+(12 \times 5 \times 3)](\bmod 84) \\
& =(21+180)(\bmod 84) \\
& =201(\bmod 84)
\end{aligned}
$$

22. Determine whether the system
$x \equiv 3(\bmod 10) ; x \equiv 8(\bmod 15) ; x \equiv 5(\bmod 84)$ has a solution and find themall if it exists.

## Solution:

The first congruence $x \equiv 3(\bmod 10)$ is equivalent to the simultaneous congruences

$$
\begin{align*}
& x \equiv 3(\bmod 2)  \tag{1}\\
& x \equiv 3(\bmod 5) \tag{2}
\end{align*}
$$

The congruence $x \equiv 8(\bmod 15)$ is equivalent to,

$$
\begin{aligned}
& x \equiv 8(\bmod 3)-----(3) \\
& x \equiv 8(\bmod 5)-----(4)
\end{aligned}
$$

The congruence $x \equiv 5(\bmod 84)$ is equivalent to,
$x \equiv 5(\bmod 3)-----(5)$
$x \equiv 5(\bmod 4)-----(6)$
$x \equiv 5(\bmod 7)-----(7)$
The congruence (1) \& (6)

$$
x \equiv 3(\bmod 2)
$$

$x \equiv 5(\bmod 4)$ reduces to $x \equiv 1(\bmod 4)-----(8)$

$$
\begin{aligned}
& \Rightarrow \quad 12 b_{3}-1=7 k_{2}, \quad k_{2} \text { is an integer } \\
& 12 \mathrm{~b}_{3}=1+7 k_{2} \\
& b_{3}=\frac{1+7 k_{2}}{12}
\end{aligned}
$$

The congruence (3) \& (5)
$x \equiv 8(\bmod 3)$
$x \equiv 5(\bmod 3)$ reduces to $x \equiv 2(\bmod 3)-----(9)$
The congruence (2) \& (4)

$$
x \equiv 3(\bmod 5)
$$

$x \equiv 8(\bmod 5)$ reduces to $x \equiv 3(\bmod 5)-----(10)$
From $(7) \Rightarrow x \equiv 2(\bmod 7)-----(11)$
we have solve the congruence of (8),(9),(10) \& (11)
Here $a_{1}=1, a_{2}=2, a_{3}=3, a_{4}=5$

$$
m_{1}=4, m_{2}=3, \quad m_{3}=5, \quad m_{4}=7
$$

$$
\begin{aligned}
m & =m_{1} \cdot m_{2} \cdot m_{3} \cdot m_{4} \\
& =4.3 \cdot 5 \cdot 7 \\
& =420
\end{aligned}
$$

$\frac{m}{m_{1}}=105, \frac{m}{m_{2}}=140, \frac{m}{m_{3}}=84, \frac{m}{m_{4}}=60$

> we knowthat
$\left(\frac{m}{m_{j}}\right) b_{j}=1\left(\bmod m_{j}\right)$
For $m_{1} \Rightarrow\left(\frac{m}{m_{1}}\right) b_{1} \equiv 1\left(\bmod m_{1}\right)$

$$
\Rightarrow \quad \begin{aligned}
& (105) b_{1} \equiv 1(\bmod 4) \Rightarrow 4 / 105 b_{1}-1 \\
& 105 b_{1}-1=4 k_{1}, \quad k_{1} \text { is an integer } \\
& 105 \mathrm{~b}_{1}=1+4 k_{1} \\
& b_{1}=\frac{1+4 k_{1}}{105}
\end{aligned}
$$

$$
\text { put } k_{1}=26, \quad b_{1}=1
$$

For $m_{2} \Rightarrow\left(\frac{m}{m_{2}}\right) b_{2} \equiv 1\left(\bmod m_{2}\right)$

$$
\Rightarrow \quad \begin{aligned}
& (140) b_{2} \equiv 1(\bmod 3) \Rightarrow 3 / 140 b_{2}-1 \\
& 140 b_{2}-1=3 k_{2}, \quad k_{2} \text { is an integer } \\
& 140 \mathrm{~b}_{2}=1+3 k_{2}
\end{aligned}
$$

$$
b_{2}=\frac{1+3 k_{2}}{140}
$$

put $k_{2}=93, \quad b_{2}=2$
For $m_{3} \Rightarrow\left(\frac{m}{m_{3}}\right) b_{3} \equiv 1\left(\bmod m_{3}\right)$

$$
(84) b_{3} \equiv 1(\bmod 5) \Rightarrow 5 / 84 b_{3}-1
$$

$\Rightarrow \quad 84 b_{3}-1=5 k_{3}, \quad k_{3}$ is an integer

$$
84 \mathrm{~b}_{3}=1+5 k_{3}
$$

$$
b_{3}=\frac{1+5 k_{3}}{84}
$$

For $m_{4} \Rightarrow\left(\frac{m}{m_{4}}\right) b_{4} \equiv 1\left(\bmod m_{4}\right)$

$$
(60) b_{4} \equiv 1(\bmod 7) \Rightarrow 7 / 60 b_{4}-1
$$

$\Rightarrow \quad 60 b_{4}-1=7 k_{4}, \quad k_{4}$ is an integer

$$
\begin{aligned}
84 \mathrm{~b}_{4} & =1+7 k_{4} \\
b_{4} & =\frac{1+7 k_{4}}{84}
\end{aligned}
$$

put $k_{4}=17, \quad b_{3}=2$
By chinese remainder theorem,

$$
\begin{aligned}
x & =\sum_{i=1}^{4}\left(\frac{m}{m_{i}}\right) a_{i} b_{i}(\bmod m) \\
& =\left(\frac{m}{m_{1}} a_{1} b_{1}+\frac{m}{m_{2}} a_{2} b_{2}+\frac{m}{m_{3}} a_{3} b_{3}+\frac{m}{m_{4}} a_{4} b_{4}\right)(\bmod m) \\
& =[(105 \times 1 \times 1)+(140 \times 2 \times 2)+(84 \times 3 \times 4)+(60 \times 5 \times 2)](\bmod 420) \\
& =(105+560+1008+600)(\bmod 420) \\
& =2273(\bmod 420)=173(\bmod 420)
\end{aligned}
$$

## $\mathbf{2 x} 2$ linear system

A $2 \times 2$ linear system is a system of linear congruences of the form,
$a x+b y \equiv e(\bmod m)$
$c x+d y \equiv f(\bmod m)$
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 $a x+b y \equiv e(\bmod m)$ and $c x+d y \equiv f(\bmod m)$ has a unique solution if and only if $(\Delta, m)=1$, where $\Delta \equiv a d-b c(\bmod m)$.
23. Verify that the linear system $2 x+3 y \equiv 4(\bmod 13)$ and $3 x+4 y \equiv 5(\bmod 13)$ has a unique solution modulo 13.

## Solution:

We know that the system has a unique solution modulo $m$ if and only if $(\Delta, m)=1$
$\Delta=a d-b c=\left|\begin{array}{ll}2 & 3 \\ 3 & 4\end{array}\right|=-1 \equiv 12(\bmod 13)$.
Since $(12,13)=1$
Therefore the system has a unique solution modulo 13.
24.Solve the linear system
$5 x+6 y \equiv 10(\bmod 13)$
$6 x-7 y \equiv 2(\bmod 13)$.

## Solution:

$5 x+6 y \equiv 10(\bmod 13)$
$6 x-7 y \equiv 2(\bmod 13)$
$\Rightarrow \mathrm{a}=5, \mathrm{~b}=6, \mathrm{c}=6, \mathrm{~d}=-7, \mathrm{e}=10, \mathrm{f}=2$.
$m=13, \Delta=a d-b c$

$$
\begin{aligned}
& =-35-36 \\
& =-71(\bmod 13)=7(\bmod 13)
\end{aligned}
$$

$(\Delta, m)=(13,1)=1$.
Hence unique solution.

$$
\begin{aligned}
& x_{0}=\Delta^{-1}\left|\begin{array}{cc}
10 & 6 \\
2 & -7
\end{array}\right|(\bmod 13)-----(1) \\
& y_{0}=\Delta^{-1}\left|\begin{array}{cc}
5 & 10 \\
6 & 2
\end{array}\right|(\bmod 13)------(2) \\
& \Delta \Delta^{-1} \equiv 1(\bmod 13) \\
& 7 \Delta^{-1} \equiv 1(\bmod 13) \\
& \Rightarrow \Delta^{-1} \equiv 2(\bmod 13) \\
& (1) \Rightarrow \\
& \begin{aligned}
& x_{0} \equiv \Delta^{-1}(-70-12)(\bmod 13) \equiv 2(-70-12)(\bmod 13) \\
& \equiv-8(\bmod 13) \\
& \equiv 5(\bmod 13) \\
&(2) \Rightarrow \\
& \begin{aligned}
y_{0} & \equiv \Delta^{-1}(10-60)(\bmod 13)
\end{aligned} \\
& \equiv 2(-50)(\bmod 13) \\
& \therefore x \equiv 5(\bmod 13) \equiv 2.2(\bmod 13) \\
& y \equiv 4(\bmod 13) .
\end{aligned}
\end{aligned}
$$

## Wilson Theorem:

## 1. State and prove Wilson's Theorem

Statement:
If $p$ is prime, then $(p-1)!\equiv-1(\bmod p)$.
Proof:
We have to prove $(p-1)!\equiv-1(\bmod p)$
When $p=2,(p-1)!=(2-1)!=1 \equiv-1(\bmod 2)$.
So, the theorem is true when $p=2$.
Now let $p>2$ and let $a$ be a positive integer such that $1 \leq a \leq p-1$.
Since $p$ is a prime and $a<p,(a, p)=1$.
Then the congruence $a x \equiv 1(\bmod p)$ has a solution $a^{\prime}$ congruence modulo $p$.
$\therefore \quad a a^{\prime} \equiv 1(\bmod p)$, where $1 \leq a^{\prime}<p-1$
$\therefore \quad a, a^{\prime}$ are inverses of each other modulo p .
If $a^{\prime}=a$, then $a \cdot a \equiv 1(\bmod p)$
$\Rightarrow a^{2}-1 \equiv 0 \cdot(\bmod p)$
$\therefore p\left|a^{2}-1 \Rightarrow p\right|(a-1)(a+1)$

$$
\Rightarrow p \mid a-1 \quad \text { or } \quad p \mid a+1
$$

Since $a<p$, if $p \mid a+1$ then $a=p-1$.
If $p \mid a-1$, then $a-1=0 \Rightarrow a=1$.

$$
\Rightarrow a=1 \text { or } p-1 \quad \text { if } \quad a=a^{\prime}
$$

i.e., $\quad 1$ and $p-1$ are their own inverses.

If $a^{\prime} \neq a$, excluding 1 and $p-1$, the remaining $p-3$ residues $2,3,4, \ldots,(p-3),(p-2)$ can be grouped into $\frac{p-3}{2}$ pairs of the type $a, a^{\prime}$ such that $a a^{\prime} \equiv 1(\bmod p)$
Multiplying all these pairs together we get, $\quad 2 \cdot 3 \cdot 4 \ldots(\mathrm{p}-3)(\mathrm{p}-2) \equiv 1(\bmod \mathrm{p})$

$$
\begin{aligned}
\Rightarrow 1.2 \cdot 3 \cdot 4 \ldots & (p-2)(p-1) \equiv p-1 \bmod p) \\
& (p-1)!\equiv-1(\bmod \mathrm{p}) \quad(\text { Since } p-1 \equiv-1(\bmod \mathrm{p}))
\end{aligned}
$$

Hence the theorem.
This can be rewritten as $(p-1)!+1 \equiv 0(\bmod p)$

$$
\Rightarrow \quad \mathrm{p} \mid(\mathrm{p}-1)!+1,
$$

which is the result suggested by Wilson.

## 2. Let $p$ be a prime and $n$ any positive integer. Prove that $\frac{(n p)!}{n!p^{n}} \equiv(-1)^{n}(\bmod p)$

## Proof:

First, we can make an observation. Let a be any positive integer congruent to 1 modulo p .
Then by Wilson's theorem, $a(a+1) \ldots(a+(p-2)) \equiv(p-1)!\equiv-1(\bmod p)$
In other words, the product of the $\mathrm{p}-1$ integers between any two consecutive multiples of p is congruent to $-1 \bmod \mathrm{p}$.
Then $\frac{(n p)!}{n!p^{n}}=\frac{(n p)!}{p .2 p .3 p \ldots(n p)}$

$$
\begin{aligned}
& =\prod_{\mathrm{r}=1}^{\mathrm{n}}[(\mathrm{r}-1) \mathrm{p}+1] \ldots[(\mathrm{r}-1) \mathrm{p}+(\mathrm{p}-1)] \\
& \equiv \prod_{\mathrm{r}=1}^{\mathrm{n}}(\mathrm{p}-1)!(\bmod \mathrm{p}) \\
\equiv & \prod_{\mathrm{r}=1}^{\mathrm{n}}(-1)(\bmod p) \equiv(-1)^{\mathrm{n}}(\bmod \mathrm{p})
\end{aligned}
$$

## 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 $a^{p-1} \equiv 1(\bmod p)$
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 $0,1,2,3, \ldots, p-1$
Consider the set of integers $1 \cdot a, 2 \cdot a, 3 \cdot a, \ldots .(p-1) \cdot a$--------------(1)
Suppose $i a \equiv 0(\bmod p)$, then $p / i a$.
But $p+a \therefore p / i$, which is impossible, since $i<p$.

$$
i a \not \equiv 0(\bmod p) \text { for } i=1,2, \ldots, p-1 .
$$

So, no term of (1) is zero.
Next we prove they are all distinct
Suppose $i a \equiv j a(\bmod p)$, where $1 \leq i, j \leq p-1$.
Then $(i-j) a \equiv 0(\bmod p) \Rightarrow p /(i-j) a$
Since $p+a, p / i-j$ and $i, j<p \Rightarrow / i-j /<p$.

$$
\begin{aligned}
& \therefore i-j=0 \Rightarrow i \equiv j(\bmod p) \\
& \therefore \quad i \neq j \Rightarrow i a \neq j a .
\end{aligned}
$$

This means, no two of the integers in (1) are congruent modulo p .
$\therefore$ The least residues (or remainders) of the integers $a, 2 a, 3 a, \ldots,(p-l) a$ modulo p are the same as the integers $1,2,3, \ldots, p-1$ in some order.

So, their products are congruent modulo p .

$$
\begin{array}{ll} 
& a \cdot 2 a \cdot 3 a \ldots(p-l) a \equiv 1 \cdot 2 \cdot 3 \ldots(p-1)(\bmod p) \\
\Rightarrow & l \cdot 2 \cdot 3 \ldots(p-l) \cdot a P-1 \equiv(p-l)!(\bmod p) \\
\Rightarrow & (p-l)!a P-1 \equiv(p-l)!(\bmod p) \\
\Rightarrow & a P-1 \equiv l(\bmod p)(\operatorname{since} p+(p-l))
\end{array}
$$

The result $a^{p-1} \equiv l(\bmod p)$ is equivalent to $a^{p} \equiv a(\bmod p)$.

## 2. Find the remainder when $24^{1947}$ is divided by 17

## Solution.

We have to find the remainder when 241947 is divided by 17.

$$
\text { Here } \quad a=24, \quad p=17
$$

We know 17 is a prime \& 17|24
$\therefore$ By Fermats theorem, $2417-1 \equiv 1(\bmod 17)$

$$
\begin{gathered}
\left.\Rightarrow \quad \begin{array}{c}
2416 \equiv 1(\bmod 17) \\
\quad \therefore \quad(2416)^{121} \equiv 121(\bmod 17) \\
\quad \Rightarrow \quad 241936 \equiv 1(\bmod 17)
\end{array}\right) .
\end{gathered}
$$

$$
\text { Now } \quad 241947=241936+11=241936.2411
$$

$$
\begin{aligned}
& 242=576 \equiv-2(\bmod 17) \\
& \therefore \quad(242)^{2} \equiv(-2)^{2}(\bmod 17) \\
& \Rightarrow \quad 244 \equiv 4(\bmod 17) \\
& (244)^{2} \equiv 4^{2}(\bmod 17) \\
& \Rightarrow \quad 248 \equiv 16(\bmod 17) \\
& \equiv-l(\bmod 17) \\
& 2411=248.242 .24 \equiv(-1)(-2) .7(\bmod 17) \\
& \equiv 14(\bmod 17) \\
& \therefore \quad 241947 \equiv 14(\bmod 17) \\
& \equiv 14(\bmod 17)
\end{aligned}
$$

$\therefore$ 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 $a^{\Phi(m)} \equiv 1(\bmod m)$.
Proof :
Given $m$ is a positive integer and $a$ is any integer such that $(a, m)=1$.
Let $\mathbf{r}_{1}, \mathbf{r}_{2}, \ldots, \mathbf{r}_{\Phi(\mathrm{m})}$ be all the positive integers $<\mathrm{m}$ and relatively prime to m .
Since $r_{i}-r_{j}<m$, clearly $r_{i} \neq r_{j}(\bmod m)$ if $i \neq j$
Consider the products $\operatorname{ar}_{1}, \operatorname{ar}_{2}, \ldots, \operatorname{ar}_{\Phi(m)}$
Since $(a, m)=1, \mathbf{a r}_{i} \neq \mathbf{a r}_{\mathbf{j}}(\bmod \mathbf{m})$ if $\mathbf{i} \neq \mathbf{j}$
we find $a r_{1}, \mathrm{ar}_{2}, \ldots, \mathrm{ar}_{\Phi(\mathrm{m})} \bmod \mathrm{m}$ are distinct.
We now prove $\left(\mathrm{ar}_{\mathrm{i}}, \mathrm{m}\right)=1$
For, suppose $\left(\mathrm{ar}_{i}, m\right)>1$, then let $p$ be a prime factor of $\left(\mathrm{ar}_{i}, \mathrm{~m}\right)=d$.

If $p \mid a$ and $p \mid m$, then $p \mid(a, m) \Rightarrow(a, m) \neq 1$, which is again a contradiction.

$$
\therefore \quad\left(\mathrm{ar}_{\mathrm{i}}, \mathrm{~m}\right)=\mathbf{l}, \mathrm{i}=1,2,3, \ldots, \Phi(\mathrm{~m})
$$

$\therefore$ the $\Phi(m)$ least residues $\mathrm{ar}_{1}, \mathrm{ar}_{2}, \ldots, \mathrm{ar}_{\Phi(\mathrm{m})}$ 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 $m$.
$\therefore$ their product $\operatorname{ar}_{1} \cdot \operatorname{ar}_{2} \cdot \ldots \cdot \operatorname{ar}_{\Phi(m)} \equiv \mathbf{r}_{1} \cdot \mathbf{r}_{2} \cdot \ldots \cdot \mathbf{r}_{\Phi(m)}(\bmod m)$
$\Rightarrow \quad \mathbf{a}_{\Phi(m)} \mathbf{r}_{1}, \mathbf{r}_{2,}, \mathbf{r}_{\Phi(m)} \equiv \mathbf{r}_{1} \mathbf{r}_{2} . . \mathbf{r}_{\Phi(\mathrm{m})}(\bmod m)$
Since each $r_{i}$ is relatively prime to $\left.m,\left(r_{1} \mathbf{r}_{2} . . \mathbf{r}_{\Phi(m)}\right), m\right)=1$
We get $a^{\Phi(m)} \equiv 1(\bmod m)$
2. Using Euler's theorem, find the remainder when $\mathbf{~ 2 4 5}^{\mathbf{1 0 4 0}}$ is divided by 18 .

Solution.
We have to find the remainder when 2451040 is divided by 18.
Here $\mathbf{a}=245=5 \cdot 72$ and $\mathbf{m}=18=32 \cdot 2,(a, m)=1$
Hence by Euler's theorem,

But

$$
\begin{array}{r}
\mathbf{a}^{\varphi(\mathbf{m})} \equiv \mathbf{1}(\bmod \mathbf{m}) \Rightarrow 245^{\varphi(\mathbf{m})} \equiv \mathbf{1}(\bmod \mathbf{m}) \\
\varphi(18)=\varphi\left(3^{2} \cdot 2\right)=\varphi\left(3^{2}\right) \cdot \varphi(2)=3^{2}\left(1-\frac{1}{3}\right) \cdot 1=6
\end{array}
$$

$$
\therefore 245^{6} \equiv 1_{(\bmod 18)}
$$

$$
\begin{aligned}
& \therefore\left(245^{6}\right)^{173} \equiv 1^{173}(\bmod 18) \\
& \quad 245^{1038} \equiv 1(\bmod 18) \\
& 245^{1040}=245^{1038+2}=245^{1038} 245^{2}
\end{aligned}
$$

But $245 \equiv 11(\bmod 18)$

$$
\begin{aligned}
2452 & \equiv 11^{2}(\bmod 18) \\
& \equiv 121(\bmod 18) \\
& \equiv 13(\bmod 18) \\
2451040 & \equiv 1 \cdot 13(\bmod 18) \\
& \equiv 13(\bmod 18)
\end{aligned}
$$

$\therefore$ The remainder is 13 when 2451040 is divided by 18.
If ${ }^{\mathbf{n}}=\mathbf{p}_{1}{ }^{\mathbf{e}_{1}} \mathbf{p}_{2}{ }^{\mathbf{e}_{2}} \ldots \mathbf{p}_{\mathbf{k}}{ }^{\mathbf{e}_{\mathbf{k}}}$ is the canonical decomposition of a positive integer $\mathbf{n}$ then derive the formula for the phi function $\phi(\mathrm{n})$ and use it to find $\varphi(6860)$
Proof:
To prove : If $\mathbf{p}$ is prime and e any positive integer then prove that $\varphi\left(p^{e}\right)=p^{e}-p^{e-1}=p^{e}\left(1-\frac{1}{p}\right)$
$\varphi\left(p^{e}\right)=$ number of positive integers $\leq p^{e}$ and relatively prime to it $=\left\{\right.$ number of positive integers $\left.\leq p^{e}\right\}$-\{ 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 $\mathbf{1 , 2 , 3}, \ldots, p^{e}$ )
The number of positive integers $\leq p^{e}$ and not prime to it are the various multiples of $\mathbf{p}$.
They are $p, 2 p, 3 p, \ldots .,\left(p^{e-1}\right) p$
The number of such numbers $=p^{e-1}$

$$
\text { Hence } \varphi\left(p^{e}\right)=p^{e}-p^{e-1}=p^{e}\left(1-\frac{1}{p}\right)
$$

Since $\varphi\left(p^{e}\right)=p^{e}-p^{e-1}=p^{e}\left(1-\frac{1}{p}\right)$ is a multiplicative function,

$$
\begin{aligned}
\varphi(n) & =\varphi\left(p_{1}^{e} p_{2}^{e} \ldots p_{k}^{e}\right)=\varphi\left(p_{1}^{e}\right) \varphi\left(p_{2}^{e}\right) \ldots \varphi\left(p_{k}^{e}\right) \\
& =p_{1}^{e}\left(1-\frac{1}{p_{1}}\right) p_{2}^{e}\left(1-\frac{1}{p_{2}}\right) \ldots p_{k}^{e}\left(1-\frac{1}{p_{k}}\right) \\
& =p_{1}^{e} p_{2}^{e} \ldots p_{k}^{e}\left(1-\frac{1}{p_{1}}\right)\left(1-\frac{1}{p_{2}}\right) \ldots\left(1-\frac{1}{p_{k}}\right) \\
& =n\left(1-\frac{1}{p_{1}}\right)\left(1-\frac{1}{p_{2}}\right) \ldots\left(1-\frac{1}{p_{k}}\right)
\end{aligned}
$$

To find $\varphi(6860)$ :

$$
\begin{aligned}
\varphi(6860) & =\varphi\left(2^{2}\right) \cdot \varphi(5) \cdot \varphi\left(7^{3}\right) \\
& =2^{2}\left(1-\frac{1}{2}\right) 4 \cdot 7^{3}\left(1-\frac{1}{7}\right)=252
\end{aligned}
$$

## Euler phi function:

Let $\varphi: N \rightarrow N$ be a function defined by
$\varphi(1)=1$ and
for $n>1 \varphi(n)=$ the number of positive integer $\leq n$ 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 $\varphi(\mathbf{m n})=\varphi(\mathbf{m}) \varphi(\mathbf{n})$
Arrange the mn integers $1,2,3, \ldots, \mathrm{mn}$ in m rows of n numbers each.

| 1 | $m+1$ | $2 m+1$ | $3 m+1$ | $\ldots$ | $(n-1) m+1$ |
| :---: | :---: | :---: | :---: | :---: | :---: |
| 2 | $m+2$ | $2 m+2$ | $3 m+2$ | $\ldots$ | $(n-1) m+2$ |
| 3 | $m+3$ | $2 m+3$ | $3 m+3$ | $\ldots$ | $(n-1) m+3$ |
| $:$ | $:$ | $:$ | $:$ | $:$ | $:$ |
| $:$ | $:$ | $:$ | $:$ | $:$ | $:$ |
| $r$ | $m+r$ | $2 m+r$ | $3 m+r$ | $\ldots$ | $(n-1) m+r$ |
| $:$ | $:$ | $:$ | $:$ | $:$ | $:$ |
| $m$ | $2 m$ | $3 m$ | $4 m$ | $\ldots$ | $n m$ |

Let $r$ be a positive integer $\leq m$ 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 $d \mid r$ and $d|\mathbf{m} \Rightarrow \mathbf{d}| \mathbf{k m}+r$ 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 $m n$ if $(\mathbf{r}, \mathrm{m})>1$.
In other words, the elements in the array relatively prime to mn come from the rth row only if $(\mathbf{r}, \mathrm{m})=1$.
Since $r<m$ and relatively prime to $m$, we find there are $\varphi(m)$ such integers $r$ and have $\varphi(m)$ such rows.
Now let us consider the rth row where $(\mathbf{r}, \mathrm{m})=1$.
The elements in the rth row are $r, m+r, 2 m+r, \ldots,(n-1) m+r$.
When they are divided by $n$, the remainders are $0,1,2, \ldots, n-1$ in some order of which $\varphi(n)$ arc relatively prime to $n$.
Therefore, exactly $\varphi(n)$ elements in the rth row are relatively prime to n and hence to mn . Thus there are $\varphi(\mathrm{m})$ rows containing positive integers relatively prime to mn and each row contain $\varphi(\mathbf{n})$ elements relatively prime to it.
Hence the array contains $\varphi(\mathrm{m}) \varphi(\mathrm{n})$ positive integers $\leq \mathrm{mn}$ and relatively prime to mn .
That is $\varphi(\mathrm{mn})=\varphi(\mathrm{m}) \varphi(\mathrm{n})$.
Hence $\varphi$ is multiplicative function.
2. If $p$ is prime and e any positive integer then prove that $\varphi\left(p^{e}\right)=p^{e}-p^{e-1}$. Also show that $\varphi(n)=\frac{n}{2}$ when $n=2^{k}$
Proof:

$$
\begin{aligned}
\varphi\left(p^{e}\right) & =\text { number of positive integers } \leq p^{e} \text { and relatively prime to it } \\
& =\left\{\text { number of positive integers } \leq p^{e}\right\}-\left\{\text { number of positive integers } \leq p^{e}\right. \\
& \text { and not relatively prime to it }\}
\end{aligned}
$$

The number of positive integers $\leq p^{e}$ is $p^{e}$ (because they are $\mathbf{1 , 2 , 3}, \ldots, p^{e}$ )

The number of positive integers $\leq p^{e}$ and not prime to it are the various multiples of $\mathbf{p}$.
They are $p, 2 p, 3 p, \ldots .,\left(p^{e-1}\right) p$
The number of such numbers $=p^{e-1}$
Hence $\varphi\left(\mathbf{p}^{e}\right)=p^{e}-p^{e-1}$

To prove that

$$
\varphi(n)=\frac{n}{2} \text { when } n=2^{k}
$$

Given $n=2^{k}$
$\therefore \varphi(n)=\varphi\left(2^{k}\right)=2^{k}\left(1-\frac{1}{2}\right)=2^{k} \cdot \frac{1}{2}=\frac{n}{2}$
3. Find the primes $p$ for which $\frac{2^{p-1}-1}{p}$ is a square.

Solution:
Suppose $\quad \frac{2^{p-1}-1}{p}=n^{2} \quad$ for some positive integer $\mathbf{n}$. Then $2^{p-1}-1=p n^{2}$
Clearly both $p$ and $n$ must be odd.
Let $p=2 k+1$ for some positive integer $k$.
Then $2^{2 k}-1=p n^{2}$
$\Rightarrow \quad\left(2^{k}-1\right)\left(2^{k}+1\right)=p n^{2}$
Suppose $\left(2^{k}-1\right)$ is a perfect square, $\left(2^{k}-1\right)=r^{2} \Rightarrow 2^{k}=r^{2}+1$
$2^{p-1}=2^{2 k}=\left(2^{k}\right)^{2}=\left(r^{2}+1\right)^{2}$
Since $r \geq 1$ and is odd, $r=2 i+1$ for some integer $i \geq 0$.
Then $r 2=(2 i+1) 2$ has to be an odd number.
But $\mathbf{r} 2+1=2 k \Rightarrow r 2+1$ has to divide 2 .

$$
\Rightarrow r 2+1=1 \text { or } 2 .
$$

$\Rightarrow \mathbf{r}=0$ or 1
$r=0,2^{p-1}=\left(0^{2}+1\right)^{2}=1 \Rightarrow \mathbf{p}=\mathbf{0}$ which is not possible
$r=1, \quad 2^{p-1}=\left(1^{2}+1\right)^{2}=4 \Rightarrow \mathbf{p}=\mathbf{3}$
Suppose ${ }^{\left(2^{k}+1\right)}$ is a perfect square

$$
\begin{gathered}
\left(2^{k}+1\right)=s^{2} \Rightarrow 2^{k}=s^{2}-1 \\
2^{p-1}=(s+1)^{2}(s-1)^{2}
\end{gathered}
$$

Then both $\mathbf{s}-1$ and $\mathbf{s + 1}$ both must be the factors of $\mathbf{2}$

$$
\begin{aligned}
s-1 & =1 \text { or } 2, \quad \& \quad s+1=1 \text { or } 2 \\
& \Rightarrow s=0,1,2 \text { or } 3
\end{aligned}
$$

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 $s=3 ; 2^{p-1}=(3+1)^{2}(3-1)^{2}=2^{6} \Rightarrow p=7$.
Thus p must be 3 or 7
Tau function:
Let $\mathbf{n}$ be a positive integer then
$\tau(\mathrm{n})$ denotes the number of positive factors of n that is $\tau(\mathrm{n})=\sum_{\mathrm{d} / \mathrm{n}} 1$

## Sigma function:

Let $\mathbf{n}$ be a positive integer then $\sigma(\mathbf{n})$ denotes the sum of the positive factors of $\mathbf{n}$ that is $\sigma(\mathbf{n})=\sum_{\mathbf{d} / \mathbf{n}} d$
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 $\sigma(28)=1+2+4+7+14+28=56$

