UNIT–I GROUPS AND RINGS
PART A

1	**Define a subgroup and give one proper subgroup of** $(Z_6,+)$. **[NOV/DEC 19]**
	Let G be a group and H is a non empty subset of G. If H is a group under the same binary operation of G then H is a subgroup of G. $H=\{0,2,4\}$ *or* $K=\{0,3\}$ are the proper subgroups of $(Z_6,+)$.
2	**Find the identity element under** $*$ **defined by** $a*b=\dfrac{ab}{2}$**, for all** $a,b\in R$.
	$a=e*a=a*e=\dfrac{ae}{2}\Rightarrow e=2.$
3	**Prove that a group is abelian if and only if** $(ab)^{-1}=a^{-1}b^{-1}\ \forall a,b\in G.$
	By closure property $\forall a,b\in G\Rightarrow ab\in G$ $Let\ \ x=(ab)^{-1}, then\ \ x(ab)=e$ By associative property $\Rightarrow\ (xa)b=e$ post multiply by b^{-1} $\Rightarrow\ (xa)bb^{-1}=eb^{-1}$ $(xa)=b^{-1}$ post multiply by a^{-1} $\Rightarrow (xa)a^{-1}=b^{-1}a^{-1}$ $\Rightarrow x=b^{-1}a^{-1}$ Assume that G is an abelian group $\therefore\ (ab)^{-1}=b^{-1}a^{-1}=a^{-1}b^{-1}\qquad (\because\ \ G\, is\, abelian)$\` Conversely assume that $(ab)^{-1}=a^{-1}b^{-1}\ \forall a,b\in G$ To Prove : G is abelian $ab=\left((ab)^{-1}\right)^{-1}=\left(a^{-1}b^{-1}\right)^{-1}=\left(b^{-1}\right)^{-1}\left(a^{-1}\right)^{-1}=ba\,.$ Thus G is abelian
4	**Prove that if every element of the group is its own inverse, then G is abelian.**
	If every element of the group is its own inverse, then $a^{-1}=a$ for all $a\in$G $\Rightarrow(ab)^{-1}=ab\ \ \forall\ a,b\in G$ $\Rightarrow b^{-1}a^{-1}=ab\quad \left(\because (ab)^{-1}=\text{b}^{-1}\text{a}^{-1}\right)$ $\Rightarrow ba=ab\qquad \left(\because \text{b}^{-1}=\text{b and a}^{-1}=\text{a}\right)$ Therefore G is abelian.
5	**Define a group homomorphism with an example.**
	Let (G, $*$) and $(S,\circ)$ be two groups. A mapping f: G → S is said to be a group homomorphism if for any a, b $\in$G, $f(a*b)=f(a)\circ f(b).$ **Example:** Consider $f:\left(R^{+},.\right)\rightarrow\left(R,+\right)$ where $f(x)=\log_{10}(x)$ for any a, b $\in R^{+}$, $f(a\cdot b)=\log_{10}(ab)=\log_{10}(a)+\log_{10}(b)=f(a)+f(b)$. Therefore f(x) is a group homomorphism.

6	**Consider two groups G and G′ where G={Z, +} and G′={z^m/m=0,± 1,± 2 ,± 3,..., • }. Let** $\phi:Z\to\{z^m \,/\, \text{m is an integer}\}$ **defined by** $\phi(m)=2^m$ **where m∈Z. Prove that** ϕ **is homomorphism.**
	$\phi(m)=2^m$ where $m\in$Z $\therefore \phi(m+r)=2^{m+r}=2^m\bullet 2^r=\phi(m)\bullet\phi(r)$ Hence ϕ is homomorphism.
7	**Let** $f:(G,*)\to(G',+)$ **be an isomorphism. If** G **is an abelian group then prove that** G' **is also an abelian group.**
	$Let\ a',b'\in G'.$ Then there exists $a,b\in G$, such that $f(\text{a})=a'$ & $f(\text{b})=b'$ $a'+b'=f(a)+f(\text{b})=f(a*\text{b})=f(\text{b}*a)=f(\text{b})+f(a)=b'+a'$ Hence G' is an abelian group.
8	**Let G =** $\left(Z_{12},+_{12}\right)$ **, Find the left cosets of** $H=\{[0],[4],[8]\}$ **and show that the distinct left cosets of H forms a partition of G.**
	$Z_{12}=\{[0],[1],[2],[3],[4],[5],[6],[7],[8],[9],[10],[11]\};\ H=\{[0],[4],[8]\}$ $[0]+H=\{[0],[4],[8]\}=H=[4]+H=[8]+H$ $[1]+H=\{[1],[5],[9]\}=[5]+H=[9]+H$ $[2]+H=\{[2],[6],[10]\}=[6]+H=[10]+H$ $[3]+H=\{[3],[7],[11]\}=[7]+H=[11]+H$ $\therefore G=H\cup([1]+H)\cup([2]+H)\cup([3]+H)$
9	**Define cyclic group.**
	A group (G,*) is said to be cyclic if there exists an element a∈G such that every element of G can be written as some power of ‘a’.
10	**State any two properties of cyclic group.**
	1. Every subgroup of a cyclic group is cyclic. 2. Suppose that G is a finite cyclic group of order m. Let ‘ a’ be a generator of G. Suppose j ∈ Z, then a^j is a generator of G if and only if gcd(j, m) = 1.
11	**Give an example for a cyclic group along with its generator. [NOV/DEC 19]**
	$G=\{1,-1,i,-i\}$ is a cyclic group with generators $\langle i\rangle$ *and* $\langle -i\rangle$.
12	**Show that every cyclic group is abelian.**
	Let (G,*) be a cyclic group with ‘a’ as generator $\therefore \forall x,y\in G\Rightarrow x=a^m, y=a^n\ \therefore x*y=a^m*a^n=a^{m+n}=a^{n+m}=y*x$
13	**Prove that the multiplicative group** $Z_7^*=\{1,2,3,4,5,6\}$ **is cyclic and find its generator.**
	The element 3 is a cyclic generator since $3^1 \bmod 7=3$ $3^2 \bmod 7=9 \bmod 7=2$ $3^3 \bmod 7=(3^2\cdot 3) \bmod 7=(2\cdot 3) \bmod 7=6 \bmod 7=6$ $3^4 \bmod 7=(3^3\cdot 3) \bmod 7=(6\cdot 3) \bmod 7=18 \bmod 7=4$

$$3^5 \bmod 7 = (3^4 \cdot 3) \bmod 7 = (4 \cdot 3) \bmod 7 = 12 \bmod 7 = 5$$
$$3^6 \bmod 7 = (3^5 \cdot 3) \bmod 7 = (5 \cdot 3) \bmod 7 = 15 \bmod 7 = 1$$

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

$$4^1 \bmod 7 = 4$$
$$4^2 \bmod 7 = 16 \bmod 7 = 2$$
$$4^3 \bmod 7 = (4^2 \cdot 4) \bmod 7 = (2 \cdot 4) \bmod 7 = 1$$

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

14 Define Ring.

A *ring* $< R, +, \cdot >$ is a non-empty set R with two binary operations + and $\cdot$ normally called addition and multiplication, defined on R such that R is closed under + and $\cdot$, that is for $a, b \in R$, $a + b \in R$ and $a \cdot b \in R$, and where the following axioms are satisfied for all $a, b, c \in R$:

1. $R_1 : < R, + >$ is an abelian group, that is
   a. $(a+b)+c = a+(b+c)$ (Associativity under + is satisfied)
   b. For each $a \in R$, there exists an identity $0 \in R$ where
   $a + 0 = 0 + a = a$ (R has an additive Identity)
   c. For each $a \in R$, there exists an $-a \in R$ where
   $a + (-a) = (-a) + a = 0$ (Each element in R has an additive inverse)
   d. $a + b = b + a$ (Addition is commutative)
2. $R_2 : (ab)c = a(bc)$ (Associativity under $\cdot$ is satisfied)
3. $R_3 : a(b+c) = ab + ac$ (Left and Right Distributive laws are satisfied)
   $(a+b)c = ac + bc$

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

(i) $< R, + >$ is an abelian group
(ii) $< R, \cdot >$ is a semi group
(iii) R satisfies distributive law

15 Define a Commutative ring.

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

16 Define Zero divisors of a ring with example.

A ring (R, +, $\cdot$) is said to be ring with zero divisors, if there exists non zero elements *a*, *b* in R, such that *ab* = 0. Such elements are called zero divisors.

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

2 and 3 are zero divisors of the ring.

17 Define Subring with example.

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.

18 Define Integral Domain.

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

19 **Define (a) Unit of a ring (b) Division Ring.**

(a) Let R be a ring with unity $1 \neq 0$. An element $u \in R$ is a unit of R if it has a multiplicative inverse in R. (i.e), for $u \in R$, there exists an element $u^{-1} \in R$ where $u \cdot u^{-1} = u^{-1} \cdot u = 1 \in R$.

(b) If every non-zero element of R is a unit, then R is a division ring.

(OR)

A ring R with unit element having atleast two elements is called a division ring, if every non-zero element of R possesses their multiplicative inverse.

20 **Define field in an algebraic system with example.**

A commutative ring (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.

(OR)

A commutative division ring is called a field.

Examples:

The set of real numbers R and set of rational numbers Q under the operations of addition + and multiplication $\cdot$ are fields.

However, the set of integers Z under addition + and multiplication $\cdot$ is not a field since the only non-zero elements that are units is -1 and 1.

For example, the integer 2 has no multiplicative inverse since ½ ∉Z.

PART B

1i) **Let G be the set of all rigid motions of a equilateral triangle. Identify the elements of G. Show that it is a non-abelian group of order six. [NOV/DEC 19]**

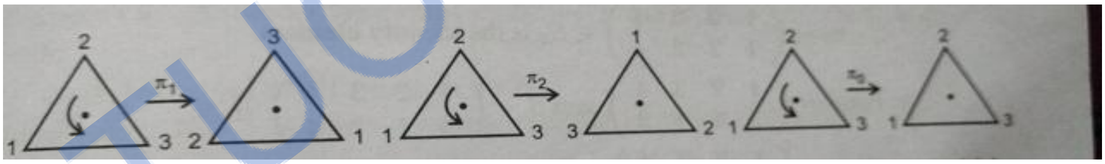
Solution:

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

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

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

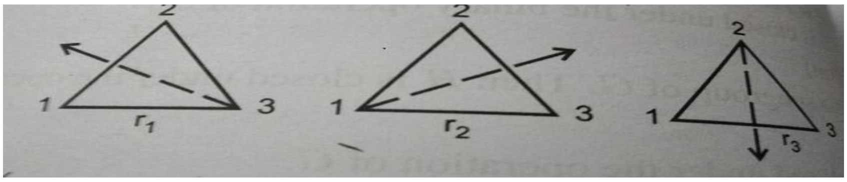
$$\pi_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \pi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$



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

Each reflection is a 3-dimensional rigid motion.

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



Let G = {π_0, π_1, π_2, r_1, r_2, r_3}.

Define binary operations on G as follows

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

Cayley's table for G is given by

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

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

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

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

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

Solution:

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

For all $1 \leq$ m, n ≤ 4,

A^m. A^n = A^{m+n} = A^r where 1< r < 4 and m + n $\cong$ r (mod 4).

Thus **.** is a closure operation.

Since matrix multiplication is associative so is '**.**'.

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

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

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

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

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

For all $1 \leq$ m, n ≤ 4, A^m**.** A^n = A^{m+n}

= A^{n+m}

= A^n**.** A^m,

so '**.**' is communicative.

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

Define f: M $\rightarrow$ G such that $\mathrm{f}\left(\mathrm{A}\right)=\mathrm{i},\ \mathrm{f}(\mathrm{A}^2)=-1=\mathrm{i}^2,\mathrm{f}(\mathrm{A}^3)=-\mathrm{i}=\mathrm{i}^3,\mathrm{f}(\mathrm{A}^4)=1=\mathrm{i}^4$

$\therefore$ f is 1-1 and onto

Since i^3 = -i = f(A^3) = f (A.A^2) **=** f(A) f(A^2) = i.i^2 = i^3 = -i

Hence f is isomorphic from M to G.

2i) Let G be a group subgroups H and K. If |G|=660, |K|=66 and K⊂H⊂G, what are the possible values of |H| ? **[NOV/DEC 19]**

Solution:

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

O(K) = |K| = 66 = 2·3·11.

O(G) = |G| = 660 = 2^2·3·5·11.

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

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

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

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

⇒660 = *y x* (2.3.11)

2^2.3.5.11 = *y x* (2.3.11)

2.5= *y x* ,with *x* > 1, *y* > 1

⇒ *x* = 2 or *x* = 5

When *x* = 2 ⇒|H| = 2 (2.3.11) =132

When *x* = 5 ⇒|H| =5 (2.3.11) =330.

2ii) Find $[100]^{-1}$ in Z_{1009}. [NOV/DEC 19]

Solution:

gcd(100, 1009)=1,
By Euclidean Algorithm,

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

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

By (2) ⇒ 1 = 100 – 11(9)

= 100 – 11 [1009 – 10(100)] (by (1))

= 100 + 110 (100) – 11(1009)

= 111(100) – 11 (1009)

= (111) (100) (mod 1009)

∴ [1] = [111] [100] (mod 1009)

⇒ $[100]^{-1}$ is [111] in Z_{1009}.

2iii) Prove that every subgroup of a cyclic group is cyclic.

Proof:

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

Claim: H is cyclic

Case1: H is a trivial subgroup of G (i.e) H = G or H = {e}

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

Case2: H is a non - trivial subgroup of G

If not the elements of H are non-zero integral powers of a.

Since if a^r∈H, its inverse a^{-r}∈H.

Let “m” be the smallest positive integer such that a^m ∈H. → **(1)**

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

Then n = qm + r where 0 ≤ r < m. → **(2)**

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

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

Since a^m ∈H, $(a^m)^q$ ∈H by closure property,⇒ a^{mq}∈H

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

Since a^n∈H and a^{-mq}∈H by closure property ⇒a^{n-mq} ∈H ∴ a^r∈H

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

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

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

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

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

Proof:

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

,

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

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

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

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

Distributive Laws:

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

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

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

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

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

Thus A is a ring.

(b) To prove isomorphism, consider a one-to-one and onto function f from R onto A defined as follows For all $r \in R, f: R \to A$ where $f(r)=\begin{bmatrix} r & 0 \\ 0 & r \end{bmatrix}$

i.e., for any real number we associate a 2^{nd} order scalar matrix.

Now for any $r, s \in R$

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

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

	$f(r\cdot s)=\begin{bmatrix} rs & 0\\ 0 & rs\end{bmatrix}=\begin{bmatrix} r & 0\\ 0 & r\end{bmatrix}\cdot\begin{bmatrix} s & 0\\ 0 & s\end{bmatrix}=f(r)\cdot f(s)$ Thus two operations $+,\cdot$ are preserved and f is $1-1$ and onto. $\therefore$ f is an isomorphism from R to A.
3ii)	**Prove that every group of prime order is cyclic.**
	Proof: Let O(G) = p, where p is a prime number. Let a $(\neq e)\in$ G. Consider a subgroup generated by a. Let $H=\langle a\rangle$ $\Rightarrow O(H)>1\left[\because H=\langle a\rangle\Rightarrow a\in H\ \&\ also\ e\in H\Rightarrow O(H)>1\right]$ Since H is a subgroup of G, then by Lagrange's theorem, O(H)/O(G) $\Rightarrow$ O(H)/p $\Rightarrow O(H)=1\ or\ p\ \left[\because p\ is\ prime\right]$ $But\ \ O(H)>1, \therefore O(H)\neq 1.$ $Thus\ \ O(H)=p=O(G)\qquad \therefore G=H$ But H is a cyclic group, $\therefore$ G is a cyclic group.
4i)	**Let (G, ∘) and (H,*) be groups with respective identities e$_G$, e$_H$ .If *f* :G→H is a homomorphism, then show that** $\boldsymbol{(a)\ \ f(e_G)=e_H}$ $\boldsymbol{(b)\ \ f(a^{-1})=[f(a)]^{-1}\ \forall a\in G}$ $\boldsymbol{(c)\ f(a^{n})=[f(a)]^{n}\ \forall a\in G\ and\ all\ n\in Z}$ $(d)\ \ f(S)$ is a subgroup of H for each subgroup S of G.
	Proof: $(a)\ e_H * f(e_G)=f(e_G)=f(e_G\circ e_G)=f(e_G)*f(e_G)$ $\therefore e_H=f(e_G)$, by right cancellation law (b) Let $a\in G$, since G is a group, $a^{-1}\in G$ Since G is a group, $a*a^{-1}=e_G$ By homomorphism $f(a*a^{-1})=f(e_G)$ $f(a)\circ f(a^{-1})=e_H$ Hence $f\left(a^{-1}\right)$ is the inverse of $f(a)$ $i.e., f(a^{-1})=[f(a)]^{-1}\ \forall a\in G$ (c) $\forall a\in G\ and\ all\ n\in Z$ Case(i): if n=0 then $a^{n}=a^{0}=e_G$ $f\left(a^{0}\right)=f\left(e_G\right)=e_H=\left[f\left(a\right)\right]^{0}$ $\Rightarrow f(a^{n})=[f(a)]^{n}$ Case(ii): if n is a positive integer then

$$a^n = a \circ a \circ a \circ \cdots \circ a \ \ (n\ times)$$

$$f\left(a^n\right) = f\left(a \circ a \circ a \circ \cdots \circ a\right) \text{ (n times)}$$

$$= f\left(a\right) * f\left(a\right) * f\left(a\right) * \cdots * f\left(a\right)$$

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

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

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

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

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

Then x = *f*(a), y = *f*(b) for some a, b∈S.

Since S is a subgroup of G, it follows that

$$\therefore a \circ b \in S,$$

$$f(a) * f(b) = f\left(a \circ b\right) \in f\left(S\right)$$

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

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

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

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

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

4ii) **Prove that Z_n is a field if and only if n is a prime.** **[NOV/DEC 20]**

Proof:

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

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

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

∴ there exists integers s, t such that as + tn = 1

⇒ sa – 1= (- t) n

∴ sa-1 is divisible by n

⇒ $\text{sa} \equiv 1 (\text{mod n})$

⇒ $[\text{s}][\text{a}] = [1]$

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

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

Conversely, let Z_n be a field.

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

To prove n is a prime.

if n is not a prime, then n= $n_1 n_2$, where 1 < n_1 ,n_2 <n. So $[\text{n}_1] \neq [0]$ and $[\text{n}_2] \neq [0]$

But $[\text{n}_1][\text{n}_2] = [\text{n}_1\text{n}_2] = [\text{n}] = [0]$

$\therefore [\text{n}_1],[\text{n}_2]$ are divisors of zero which contradicts the fact Z_n is a field.

Hence n is a prime.

5i) **Prove that the set R of numbers of the form $a+b\sqrt{2}$, where a and b are integers, is a ring with respect to ordinary addition and multiplication.**

Proof:

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

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

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

$\therefore$ R is closed under +.

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

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

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

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

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

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

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

5. Commutative law:

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

<u>Under Multiplication</u>

6. Closure Axioms:

$$\begin{aligned}
x_1 x_2 &= \left(a_1 + b_1\sqrt{2}\right).\left(a_2 + b_2\sqrt{2}\right) \\
&= \left(a_1 a_2 + 2b_1 b_2\right) + \left(a_2 b_1 + a_1 b_2\right)\sqrt{2}
\end{aligned}$$

$a_1 a_2 + 2b_1 b_2,\ a_2 b_1 + a_1 b_2 \in Z$, $\therefore x_1 x_2 \in R$

7. Associative:

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

$$= \left[\left(a_1a_2 + 2b_1b_2\right) + \left(a_2b_1 + a_1b_2\right)\sqrt{2}\right] \cdot \left(a_3 + b_3\sqrt{2}\right)$$

$$= \left[\left(a_1a_2 + 2b_1b_2\right)a_3 + 2\left(a_2b_1 + a_1b_2\right)b_3\right]$$

$$+ \left[\left(a_1a_2 + 2b_1b_2\right)b_3 + \left(a_2b_1 + a_1b_2\right)a_3\right]\sqrt{2}$$

$$= x_1 \cdot (x_2 \cdot x_3)$$

8. Distributive Laws :

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

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

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

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

$$= a_1a_2 + a_1a_3 + 2b_1b_2 + 2b_1b_3 + \sqrt{2}a_2b_1 + \sqrt{2}a_3b_1 + \sqrt{2}a_1b_2 + \sqrt{2}a_1b_3$$

$$= \left[\left(a_1a_2 + 2b_1b_2\right) + \left(a_1b_2 + a_2b_1\right)\sqrt{2}\right] + \left[\left(a_1a_3 + 2b_1b_3\right) + \left(a_1b_3 + a_3b_1\right)\sqrt{2}\right]$$

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

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

Hence the given set is a ring.

5ii) **Prove that (Q,⊕,∘) is a ring on the set of rational numbers under the binary operations $x \oplus y = x + y + 7$, $x \circ y = x + y + (xy/7)$ for $x, y \in Q$. [NOV/DEC 19]**

Proof:

1. Closure : For $x, y \in Q$, $x \oplus y = x + y + 7 \in Q$

(sum of two rational numbers is always rational)

2. Associative: $x, y, z \in Q$

$(x \oplus y) \oplus z = (x + y + 7) \oplus z = (x + y + 7) + z + 7 = x + (y + z + 7) + 7$

$= x \oplus (y + z + 7)$

$= x \oplus (y \oplus z)$

3. Identity: $x, e \in Q$, $x \oplus e = x + e + 7$

if e is the identity then $x \oplus e = x$

$\therefore x = x + e + 7 \Rightarrow e = -7$

4. Inverse: For $x, x^{-1} \in Q$ $x \oplus x^{-1} = x + x^{-1} + 7$

If x^{-1} is the inverse of x then, $x \oplus x^{-1} = e$

$\therefore x + x^{-1} + 7 = e \quad (e = -7)$

$x + x^{-1} + 7 = -7 \Rightarrow x^{-1} = -x - 14$

5. Commutative law:

For $x, y \in Q$, $x \oplus y = x + y + 7 = y + x + 7 = y \oplus x$

Under Multiplication

6. Closure Axioms:

For $x, y \in Q$, $x \circ y = x + y + (xy/7) \in Q$

7. Associative:

$x, y, z \in Q$, $(x \circ y) \circ z = [x + y + (xy/7)] \circ z$

$=[x + y + (xy/7)]+ z+\{[x + y + (xy/7)]\, z\}/7$

$= x + y + z + (xy/7) +\{[xz + yz + (xyz/7)] /7\}$

$= x + y + z + (xy/7)+ (xz/7)+(zy/7)+ (xyz/49)$ ----------(1)

$x \circ (y \circ z) = x \circ [y + z + (yz/7)]$

$= x +[y + z + (yz/7)] +\{[y + z + (yz/7)]x\}/7$

$= x + y + z + (yz/7) +\{[y + z + (yz/7)]x\}/7$

$= x + y + z + (xy/7)+ (xz/7)+(zy/7)+ (xyz/49)$ -----------(2)

From (1) and (2) , $(x \circ y) \circ z = x \circ (y \circ z)$

8. Distributive Laws :

$x \circ (y \oplus z) = x \circ (y + z + 7)= x +(y + z + 7) + [x (y + z + 7)]/7$

$= x +y + z + 7+(xy/7)+ (xz/7)+x$

$(x \circ y) \oplus (x \circ z)= [x + y + (xy/7)] \oplus [x + z + (xz/7)]$

$=[x + y + (xy/7)] +[x + z + (xz/7)] +7$

$= x +y + z + 7+(xy/7)+ (xz/7)+x$

$\therefore\ x \circ (y \oplus z) = (x \circ y) \oplus (x \circ z)$ Hence the given set (Q, ⊕, ∘) is a ring.

5iii) **Show that a finite integral domain is a field**

Proof:

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

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

Let a(≠ 0) be any element of D.

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

The elements $a\cdot a_1, a\cdot a_2, a\cdot a_3, \cdots a\cdot a_n$ are distinct, because if

$a\cdot a_i = a\cdot a_j \in D$, then $a\cdot\left(a_i - a_j\right) = 0.$

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

Hence the sets $\{a\cdot a_1, a\cdot a_2, a\cdot a_3, \cdots a\cdot a_n\}$ and $\{a_1, a_2, a_3, \cdots a_n\}$ are the same.

Since $a \in D$ is in both sets,

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

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

Let $a_j = a\cdot a_{i,}\ a_j \in D$ $\rightarrow$ **(2)**

Now $a_j\cdot a_k = a_k\cdot a_{j,}$ by commutative property

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

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

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

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

$= a_j$, by(2)

Since a_j is an arbitrary element of D, a_k is the unity of D. Let it be denoted by 1.

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

∴ a has an inverse. Hence {D, +, ·} be a finite integral domain.

UNIT– II FINITE FIELDS AND POLYNOMIALS

PART A

1 Define Polynomial rings.

Given a ring (R, + , **.**) an expression of the form $f(x)=a_0+a_1x+\cdots+a_nx^n$ where $a_i\in R,\ \forall 0\le i\le n,$ is called polynomial in the indeterminant x with the coefficients from R. Then $(R[x],+,.)$ is a ring called the polynomial ring over R under the operation of addition and multiplication given by , if $f(x)=a_0+a_1x+\cdots+a_nx^n$ and $g(x)=b_0+b_1x+\cdots+b_nx^n$ $a_i,b_i\in R,\ \forall 0\le i\le n,$ then **polynomial addition** $f+g$ is given in terms of its values at the points x, i.e., by $(f+g)(x)$ and it is given by

$$f(x)+g(x)=\sum_{i=0}^{n}c_ix^i=c_0+c_1x+\cdots+c_nx^n, where\ c_i=a_i+b_i\ ,\ 0\le i\le n$$

and for **polynomial multiplication** fg, we have

$$(fg)(x):=f(x)g(x)=d_0+d_1x+\cdots+d_nx^n\quad ,\qquad \text{where } d_n=\sum_{i=0}^{n}a_ib_{n-i}.$$

2. If $f(x)=3x^4+7x^3+5x^2+2x+4$ and $g(x)=2x^3+8x^2+6x+5$ are the polynomial in Q[x], then find the value of $f(x)+g(x)$ and $f(x)-g(x)$.

Given that $f(x)=3x^4+7x^3+5x^2+2x+4$ and $g(x)=2x^3+8x^2+6x+5$, then

$f(x)+g(x)=\ (3+0)x^4+(7+2)x^3+(5+8)x^2+(2+6)x+(4+5)=3x^4+9x^3+13x^2+8x+9$

$\&\, f(x)-g(x)=\ (3-0)x^4+(7-2)x^3+(5-8)x^2+(2-6)x+(4-5)=3x^4+5x^3-3x^2-3x-4$

3. If $f(x)=2x^4-2x^3+5x^2$ and $g(x)=5x^2+4x+3$ are the polynomial in Q[x], then find the value of $f(x).g(x)$.

$$\begin{aligned}f(x).g(x)&=\ (2x^4-2x^3+5x^2).(5x^2+4x+3)\\&=10x^6+(8-10)x^5+(6-8+25)x^4+(-6+20)x^3+15x^2\\&=10x^6-2x^5+23x^4+14x^3+15x^2\end{aligned}$$

4. If $f(x)=3x^4+5x^3+4x^2+6x+3$ and $g(x)=4x^3+3x^2+2x+1$ are the polynomial in $Z_7[x]$, then find the value of $f(x)+g(x)$ and $g(x)-f(x)$.

$f(x)+g(x)=\ (3+0)x^4+(5+4)x^3+(4+3)x^2+(6+2)x+(3+1)=3x^4+9x^3+7x^2+8x+4$

$In\ \ Z_7[x],\ \ f(x)+g(x)=3x^4+2x^3+0x^2+x+4=3x^4+2x^3+x+4$

and $f(x)-g(x)=\ (3-0)x^4+(5-4)x^3+(4-3)x^2+(6-2)x+(3-1)=3x^4+x^3+x^2+4x+2.$

Therefore $g(x)-f(x)=-3x^4-x^3-x^2-4x-2.$

$In\ \ Z_7[x],\ \ g(x)-f(x)=-3x^4-x^3-x^2-4x-2=4x^4+6x^3+6x^2+3x+5.$

5. If $f(x)=x^3-2x^2-x+2$ and $g(x)=x^3+x^2-x-2$ are the polynomial in $Z_3[x]$, then find $f(x).g(x)$

$$\begin{aligned}f(x).g(x)&=\ (x^3-2x^2-x+2).(x^3+x^2-x-2)\\&=x^6+(-2+1)x^5+(-1-2-1)x^4+(2-1-2+2)x^3+(4+1+2)x^2+(2-2)x-4\\&=x^6-x^5-4x^4+x^3+7x^2-4\end{aligned}$$

$In\ \ Z_7[x],\ \ f(x).\mathrm{g}(x)=x^6-x^5-4x^4+x^3+7x^2-4=x^6+6x^5+3x^4+x^3+3.$

6. Find two non-zero polynomials $f(x)$ and $g(x)$ in $Z_{12}[x]$ such that $f(x).g(x)=0$.

Let $f(x)=3x^2+6x+9, \quad g(x)=4x^2+8x+4$

$$f(x).g(x)=(3x^2+6x+9).(4x^2+8x+4)=12x^4+48x^3+96x^2+96x+36$$

In $Z_{12}[x]$, $f(x).g(x)=0x^4+0x^3+0x^2+0x+0=0$

7. State factor theorem and find the factors of $x^2+3x+2\in Z_6[x]$

If $f(x)\in F[x]$ and $a\in F$, then $(x-a)$ is the factor when f(x) if and only if 'a' is a root of $f(x)$.

$f(x)=x^2+3x+2$, $Z_6=\{[0],[1],[2],[3],[4],[5]\}$

$f(0)=(0)^2+3(0)+2=2$

$f(1)=(1)^2+3(1)+2=6=0$

$f(2)=(2)^2+3(2)+2=12=0$

$f(3)=(3)^2+3(3)+2=20=2$

$f(4)=(4)^2+3(4)+2=30=0$

$f(5)=(5)^2+3(5)+2=42=0$

Therefore $f(x)=x^2+3x+2$ in $Z_6[x]$ has four roots $x=1,2,4,5.$

The factors are $(x-1), (x-2), (x-4), (x-5)$

8. Find all the roots of $f(x)=x^2+4x$ in $Z_{12}[x]$

Given $f(x)=x^2+4x$, $Z_{12}=\{[0],[1],[2],[3],[4],[5],[6],[7],[8],[9],[10],[11]\}$

$f(x)=x^2+4x$	Under $Z_{12}[x]$
$f(0)=0^2+4(0)=0$	$f(0)=0$
$f(1)=(1)^2+4(1)=5$	$f(1)=5$
$f(2)=(2)^2+4(2)=12$	$f(2)=12(\text{mod } 12)=0$
$f(3)=(3)^2+4(3)=21$	$f(3)=21(\text{mod}12)=9$
$f(4)=(4)^2+4(4)=32$	$f(4)=32(\text{mod}12)=8$
$f(5)=(5)^2+4(5)=45$	$f(5)=45(\text{mod}12)=9$
$f(6)=(6)^2+4(6)=60$	$f(6)=60(\text{mod}12)=0$
$f(7)=(7)^2+4(7)=77$	$f(7)=77(\text{mod}12)=5$
$f(8)=(8)^2+4(8)=96$	$f(8)=96\ (\text{mod}12)=0$
$f(9)=(9)^2+4(9)=117$	$f(9)=117\ (\text{mod}12)=9$
$f(10)=(10)^2+4(10)=140$	$f(10)=140(\text{mod}12)=8$
$f(11)=(11)^2+4(11)=165$	$f(11)=165(\text{mod}12)=9$

Therefore $f(x)=x^2+4x$ in $Z_{12}[x]$ has four roots $x=0,2,6,8.$

9. **Find all the roots of $f(x)=x^3+5x^2+2x+6$ in $Z_7[x]$ and then write $f(x)$ as a product of first-degree polynomials.**

$f(x)=x^3+5x^2+2x+6$, $Z_7=\{[0],[1],[2],[3],[4],[5],[6]\}$

$f(x)=x^3+5x^2+2x+6$	Under $Z_7[x]$
$f(0)=6$	$f(0)=0$
$f(1)=1+5+2+6=14$	$f(1)=0$
$f(2)=8+20+8+6=42$	$f(2)=0$
$f(3)=27+45+6+6=84$	$f(3)=0$
$f(4)=64+80+8+6=158$	$f(4)=158 \pmod 7=4$
$f(5)=125+125+10+6=266$	$f(5)=266 \pmod 7=0$
$f(6)=216+180+12+6=404$	$f(6)=404 \pmod 7=5$

Therefore $f(x)=x^3+5x^2+2x+6$ in $Z_7[x]$ has four roots $x=1,3,5.$

The factors are $(x-1),(x-3),(x-5)$

In $Z_7[x]$, $f(x)=x^3+5x^2+2x+6=(x+6)(x+4)(x+2)$

10. **Show that x^2-2 has no roots in Q[x]**

x^2-2 has roots √2 and -√2 which are irrational numbers. Thus √2 and -√2$\notin$Q.
Therefore x^2-2 has no roots in Q[x]

11. **State Division Algorithm**

Let F be a field and let $f(x)$ and $g(x)$ be two polynomials in $F(x)$ with $g(x)\neq 0$.
Then there exists unique polynomials $q(x)$ and $r(x)$ such that

$$f(x)=q(x)g(x)+r(x) \text{ where either } r(x)=0 \text{ (or) } \deg r(x)<\deg g(x)$$

12. **State remainder theorem and What is the remainder when $f(x)=x^5+2x^3+x^2+2x+3\in Z_5[x]$ is divisible by $(x-1)$**

If $f(x)\in F[x]$ & $a\in F$ for any field F, then $f(a)$ is the remainder when $f(x)$ is divided by x–a.
By remainder theorem, remainder for given $f(x)=x^5+2x^3+x^2+2x+3$ is $f(1)$.

Here $f(1)=(1)^5+2(1)^3+(1)^2+2(1)+3=9.$

In $Z_5[x]$, $f(1)=4.$
Hence remainder is 4.

13. **Find quotient and remainder when $g(x)=x^2+5$ divides $f(x)=x^5+2x^3+3x^2+x-1$ where $f(x),g(x)\in Z_7[x]$.**

$$\begin{array}{r l}
 & x^3+4x+3 \\ \cline{2-2}
 & \cancel{x^5}+0x^4+2x^3+3x^2+x-1 \\
 & \cancel{x^5}+0x^4+5x^3 \\
 & ---------------- \\
 & \qquad \cancel{4x^3}+3x^2 \\
x^2+5 & \qquad \cancel{4x^3}-0x^2+20x \\
 & ---------------- \\
 & \qquad\quad \cancel{3x^2}+2x+6 \\
 & \qquad\quad \cancel{3x^2}+0x+15 \\
 & ---------------- \\
 & \qquad\qquad 2x+5
\end{array}$$

Quotient = x^3+4x+3 and Remainder $=2x+5$.

14. **If $f(x)=2x^4+5x^3-7x^2+4x+8$ and $g(x)=2x-1$ are polynomials in** Q[x]**, determine $q(x)$ and $r(x)$ such that $f(x)=q(x)g(x)+r(x)$.**

$$\begin{array}{r l}
 & x^3+3x^2-2x+1 \\ \cline{2-2}
 & \cancel{2x^4}+5x^3-7x^2+4x+8 \\
 & \cancel{2x^4}-x^3 \\
 & ---------------- \\
 & \qquad \cancel{6x^3}-7x^2 \\
 & \qquad \cancel{6x^3}-3x^2 \\
 & ---------------- \\
2x-1 & \qquad\quad -\cancel{4x^2}+4x \\
 & \qquad\quad -\cancel{4x^2}+2x \\
 & ---------------- \\
 & \qquad\qquad \cancel{2x}+8 \\
 & \qquad\qquad \cancel{2x}-1 \\
 & ---------------- \\
 & \qquad\qquad\quad 9
\end{array}$$

q(x) = x^3+3x^2-2x+1 and r(x) $=9$

15. **Define g.c.d of $f(x)$ and $g(x)$**

If $f(x),g(x)\in F[x]$, then $h(x)\in F[x]$ is a greatest common divisor of $f(x)$ and $g(x)$

(i) if $h(x)$ divides each of $f(x)$ and $g(x)$

(i) if $k(x)\in F[x]$ and $k(x)$ divides each of $f(x)$ and $g(x)$ then $k(x)$ divides $h(x)$.

16. **Define irreducible polynomial or prime**

Let $f(x)\in F[x]$, with F a field and deg $f(x)\geq 2$. Then $f(x)$ is said to be reducible over F if there exists $g(x),h(x)\in F[x]$ where $f(x)=g(x)h(x)$ and each of $g(x),h(x)$ has degree ≥ 1. If $f(x)$ is not reducible, then it is called irreducible polynomial or prime.

17. **Determine whether $x^2 + x + 1$ is reducible over $Z_7[x]$**

Given that $f(x) = x^2 + x + 1$, $Z_7 = \{[0],[1],[2],[3],[4],[5],[6]\}$

$f(x) = x^2 + x + 1$	**Under** $Z_7[x]$
$f(0) = 0^2 + 0 + 1 = 1$	$f(0) = 1$
$f(1) = (1)^2 + (1) + 1 = 3$	$f(1) = 3$
$f(2) = (2)^2 + (2) + 1 = 7$	$f(2) = 7(\text{mod } 7) = 0$
$f(3) = (3)^2 + (3) + 1 = 13$	$f(3) = 13(\text{mod } 7) = 6$
$f(4) = (4)^2 + (4) + 1 = 21$	$f(4) = 21(\text{mod } 7) = 0$
$f(5) = (5)^2 + (5) + 1 = 31$	$f(5) = 31(\text{mod } 7) = 3$
$f(6) = (6)^2 + (6) + 1 = 43$	$f(6) = 43(\text{mod } 7) = 1$

The roots of $f(x) = x^2 + x + 1$ are $2, 4$

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

Therefore *f*(*x*) is reducible over $Z_7[x]$

18. **Give an example for an irreducible & reducible polynomials in $Z_2[x]$** **[NOV/DEC 19]**

$Z_2 = \{[0],[1]\}.$

Irreducible polynomial	**Reducible polynomial**
$f(x) = x^2 + x + 1$	$g(x) = x^2 + x$
$f(0) = 0^2 + 0 + 1 = 1$	$g(0) = 0^2 + 0 = 0$
$f(1) = 1^2 + 1 + 1 = 3 = 1\ (\text{mod } 2)$	$g(1) = 1^2 + 1 = 2 = 0\ (\text{mod } 2)$

19. **Given an example of a polynomial that is irreducible in Q[x] and reducible in C[x].** **[NOV/DEC 20]**

Consider the polynomial $f(x) = x^2 + 2$

Solving $f(x) = 0 \Rightarrow x^2 + 2 = 0$

$$\Rightarrow x^2 = -2$$
$$\Rightarrow x = \pm i\sqrt{2}$$

Clearly $x = \pm i\sqrt{2} \notin Q$, therefore $f(x) = x^2 + 2$ is irreducible in Q[x].

But $x = \pm i\sqrt{2} \in C[x]$, therefore $f(x) = x^2 + 2$ is reducible in C [x].

20. **Define Characteristic of a ring with example.**

Let (R, +, ·) be a ring. If there is a least positive integer n such that nr = z (the zero of R) for all r ∈ R, then we say that R has characteristic n and write char (R) = n.
When no such integer exists, R is said to have characteristic 0.
Examples:

- The ring (Z_3 , +, ·) has characteristic 3; (Z_4, +, ·) has characteristic 4;
  In general, (Z_n, +, .) has characteristic n.
- The rings (Z, +, .) and (Q, + , .) both have characteristic 0.

PART B

1i). If R is a ring under usual addition and multiplication, show that (R[x], +, x) is a ring of polynomials over R.

Solution:

Let $f(x), g(x) \in R[x]$. Then $f(x)+g(x), f(x)\times g(x)$ are also polynomials over R. Therefore $R[x]$ is close with respect to addition and multiplication of polynomials.

$$\text{Now let } f(x)=\sum a_i x^i = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \ldots.. + a_m x^m + ..$$

$$g(x)=\sum b_i x^i = b_0 + b_1 x + b_2 x^2 + b_3 x^3 + \ldots.. + b_m x^m + \ldots...$$

$$h(x)=\sum c_i x^i = c_0 + c_1 x + c_2 x^2 + c_3 x^3 + \ldots.. + c_m x^m + \ldots..$$

Commutativity of Addition:

$$f(x)+g(x) = (a_0+b_0)+(a_1+b_1)\,\mathrm{x}+(a_2+b_2)x^2+\ldots(a_m+b_m)x^m+\ldots....$$

$$=(b_0+a_0)+(b_1+a_1)\,\mathrm{x}+(b_2+a_2)x^2+\ldots(b_m+a_m)x^m+\ldots.=g(x)+f(x)$$

Associative of Addition

$$[f(x)+g(x)]+h(x)=\left(\sum a_i x^i + b_i x^i\right)+\sum c_i x^i$$

$$=\sum a_i x^i + \left(\sum b_i x^i + c_i x^i\right) = f(x)+[g(x)+h(x)]$$

Identity element of Addition

$0(x)=0+0x+0x^2+\ldots...$ is the additive identity element of $R[x]$

Inverse Element of Addition

$-f(x)=-a_0-a_1x-a_2x^2-a_3x^3-\ldots..-a_mx^m-\ldots.$ is the additive inverse element of $R[x]$

Associativity of Multiplication

$$[f(x)\times g(x)]=(a_0+a_1x+a_2x^2+\ldots.)(b_0+b_1x+b_2x^2+\ldots.)$$

$$=(d_0+d_1x+d_2x^2+\ldots.) \quad ,\text{where } d_i=\sum_{k=0}^{i} a_{i-k}b_k$$

Now

$$[f(x)\times g(x)]\times h(x)=(d_0+d_1x+d_2x^2+\ldots.)(c_0+c_1x+c_2x^2+\ldots.)=(e_0+e_1x+e_2x^2+\ldots.),$$

$$where\ e_n = \text{the coeff } x^n \text{in} [f(x)\times g(x)]\times h(x)=\sum d_j c_k = \sum a_i b_j c_k$$

Similarly, we show that the coeff x^n in $f(x)\times[g(x)\times h(x)]=\sum a_i b_j c_k$

Thus $[f(x)\times g(x)]\times h(x)=f(x)\times[g(x)\times h(x)]$, since corresponding coefficients in these two polynomials are equal.

Distributive of multiplication on addition

We have

$$f(x)\times[g(x)+h(x)]=(a_0+a_1x+a_2x^2+\ldots.)[(b_0+b_1x+b_2x^2+\ldots.)+(c_0+c_1x+c_2x^2+\ldots.)]$$

If n is the non-negative integer, the coeff x^n in $f(x)\times[g(x)+h(x)]$

$$=\sum a_i(b_j+c_k)=\sum a_i b_j + \sum a_i c_k$$

$$=Coeff\ of\ x^n\ in\ f(x)\mathrm{g(x)}+Coeff\ of\ x^n\ in\ f(x)h(\mathrm{x})$$

$$=Coeff\ of\ x^n\ in\ [f(x)\times \mathrm{g(x)}+f(x)\times h(\mathrm{x})]=f(x)\times g(x)+f(x)\times h(x)$$

Similarly, we can prove right distributive law for $R[x]$

Hence $R[x]$ is a ring.

1ii)	**Find the remainder when** $f(x)$ **is divided by** $g(x)$**.** **(a)** $f(x), g(x) \in Q[x], \quad f(x) = x^8 + 7x^5 - 4x^4 + 3x^3 + 5x^2 - 4; g(x) = x - 3$ **(b)** $f(x), g(x) \in Z_2[x], \quad f(x) = x^{100} + x^{90} + x^{80} + x^{50} + 1; g(x) = x - 1$ **[NOV/DEC 20]**
	(a) Given $f(x) = x^8 + 7x^5 - 4x^4 + 3x^3 + 5x^2 - 4; g(x) = x - 3$ By long division $\begin{array}{r\|l} & x^7 + 3x^6 + 9x^5 + 34x^4 + 98x^3 + 297x^2 + 896x + 2688 \quad (= q(x)) \\ \hline & x^8 + 7x^5 - 4x^4 + 3x^3 + 5x^2 - 4 \\ & x^8 - 3x^7 \\ & ----------- \\ & 3x^7 - 0x^6 \\ & 3x^7 - 9x^6 \\ & ----------- \\ & 9x^6 + 7x^5 \\ & 9x^6 - 27x^5 \\ & ----------- \\ & 34x^5 - 4x^4 \\ & 34x^5 - 102x^4 \\ & ----------------- \\ x-3 & 98x^4 + 3x^3 \\ & 98x^4 - 294x^3 \\ & --------------------- \\ & 297x^3 + 5x^2 \\ & 297x^3 - 891x^2 \\ & ------------------------ \\ & 896x^2 + 0x \\ & 896x^2 - 2688x \\ & ---------------------------- \\ & 2688x - 4 \\ & 2688x - 8064 \\ & ------------------------------- \\ & 8060 = r(x) \end{array}$ $\therefore$ Remainder $= r(x) = 8060.$ Verification: By remainder theorem, If $f(x) \in F[x]$ and $a \in F$, for any field F then $f(a)$ is the remainder when f(x) is divided by (x–a). $\therefore$ Remainder $= r(x) = (3)^8 + 7(3)^5 - 4(3)^4 + 3(3)^3 + 5(3)^2 - 4$ $= 6561 + 1701 - 324 + 81 + 45 - 4 = 8060.$

(a) Given $f(x)=x^{100}+x^{90}+x^{80}+x^{50}+1; g(x)=x-1$

$$\begin{array}{r|l} & x^{99}+x^{98}+\ldots+2x^{89}+\ldots+3x^{80}+\ldots.+4x^{50}+\ldots..4(=q(x)) \\ \cline{2-2} & x^{100}+x^{90}+x^{80}+x^{50}+1 \\ & x^{100}-x^{99} \\ & ----------- \\ & \quad x^{99}+0x^{98} \\ & \quad x^{99}-x^{98} \\ x-1 & ----------- \\ & \quad \ldots\ldots. \\ & ----------------- \\ & \qquad\qquad\qquad 4x+1 \\ & \qquad\qquad\qquad 4x-4 \\ & ------------------ \\ & \qquad\qquad\qquad\quad 5(=r(x)) \end{array}$$

$\therefore$ Remainder $= r(x)=5.$ In $Z_2[x]$, $5\equiv 1(\text{mod}\,2)$ Hence remainder is 1.

Verification:

By remainder theorem, If $f(x)\in F[x]$ and $a\in F$, for any field F then f(a) is the remainder when f(x) is divided by (x–a).

$\therefore$ Remainder $= r(x)=(1)^{100}+(1)^{90}+(1)^{80}+(1)^{50}+1=5$.

In $Z_2[x]$, r(x) = 1. Hence remainder is 1.

2i) **Find the greatest common divisor of**

(i) $x^{10}-x^7-x^5+x^3+x^2-1$ & $x^8-x^5-x^3+1$ in the ring Q[x] **[NOV/DEC 19]**

(ii) x^3+3x^2+3x+1 & x^3+2x+1 in $Z_5[x]$

(i) Given $f(x)=x^{10}-x^7-x^5+x^3+x^2-1$ & g(x) $=x^8-x^5-x^3+1$

By actual division

$$\begin{array}{r|l} & \qquad x^2 \\ \cline{2-2} & \cancel{x^{10}}-\cancel{x^7}-\cancel{x^5}+x^3+\cancel{x^2}-1 \\ x^8-x^5-x^3+1 & \cancel{x^{10}}-\cancel{x^7}-\cancel{x^5}+0x^3+\cancel{x^2}-0 \\ & ----------------- \\ & \qquad\qquad\qquad\quad x^3-1 \end{array}$$

$x^{10}-x^7-x^5+x^3+x^2-1 = x^2(x^8-x^5-x^3+1)+(x^3-1)$

Similarly,

$$\begin{array}{r|l} & \quad x^5-1 \\ \cline{2-2} & \cancel{x^8}-\cancel{x^5}-x^3+1 \\ & \cancel{x^8}-\cancel{x^5} \\ & ----------- \\ x^3-1 & \qquad -\cancel{x^3}+1 \\ & \qquad -\cancel{x^3}+1 \\ & ----------- \\ & \qquad\quad 0 \end{array}$$

$(x^8-x^5-x^3+1)=(x^3-1)(x^5-1)+0$ Hence required G.C.D is (x^3-1).

	(ii) Given $f(x)=x^3+3x^2+3x+1$ & $g(x)=x^3+2x+1$ By actual division $\begin{array}{r\|l} & x \\ \cline{2-2} x^3+2x+1 & \cancel{x^3}+3x^2+3x+\cancel{1} \\ & \cancel{x^3}+0x^2+2x+\cancel{1} \\ \cline{2-2} & 3x^2+x \end{array}$ $\therefore\ x^3+3x^2+3x+1 = x(x^3+2x+1)+(3x^2+x)$ Similarly, $\begin{array}{r\|l} & 2x+1 \\ \cline{2-2} & \cancel{x^3}+0x^2+2x+1 \\ & \cancel{x^3}+2x^2+0x \\ \cline{2-2} 3x^2+x & \cancel{3x^2}+2x+1 \\ & \cancel{3x^2}+x+0 \\ \cline{2-2} & x+1 \end{array}$ $\therefore\ x^3+2x+1 = (3x^2+x)(2x+1)+(x+1)$ Similarly, $\begin{array}{r\|l} & 3x \\ \cline{2-2} & \cancel{3x^2}+x \\ x+1 & \cancel{3x^3}+3x \\ \cline{2-2} & 3x \end{array}$ $\therefore\ 3x^2+x = (x+1)(3x)+(3x)$ Similarly, $\begin{array}{r\|l} & 2x \\ \cline{2-2} & \cancel{x}+1 \\ 3x & \cancel{x} \\ \cline{2-2} & 1 \end{array}$ $\therefore\ x+1 = 3x(2x)+1$ Hence required G.C.D is 1.
2ii)	**If $f(x)\in F[x]$ has degree $n\geq 1$, then prove that $f(x)$ has at most n roots in F.** **[NOV/DEC 19]**
	Proof: We prove this theorem by mathematical induction on the degree *f*(*x*). If *f*(*x*) has degree 1, then *f*(*x*) = *a*x + b, *a*, b∈ F and *a* ≠ 0. $\Rightarrow f(-a^{-1}\text{ b}) = 0$ $\Rightarrow$ *f*(*x*) has at least one root in F If c_1 and c_2 are both roots, then

	$f(c_1) = a\,c_1 + b = 0 = a\,c_2 + b = f(c_2)$ By cancellation law in a ring, $a\,c_1 + b = a\,c_2 + b \Rightarrow a\,c_1 = a\,c_2$ Since F is a field and $a \neq 0$, we have, $a\,c_1 = a\,c_2 \Rightarrow c_1 = c_2$ So $f(x)$ has only one root in F. Now assume that the result is true for all polynomials of degree $k \geq 1$ in $F[x]$ Consider a polynomial $f(x)$ of degree $k + 1$. If $f(x)$ has no roots in F, the theorem follows. Otherwise, let $r \in$F, $f(r) = 0$ By factor theorem, $f(x) = (x - r)\,g(x)$, where $g(x)$ has degree k. By the induction hypothesis, $g(x)$ has at most k roots in F and $f(x)$ has at most $k + 1$ roots in F.
3i)	**If $(F,+,.)$ is a field and Char (F) > 0, then prove that Char(F) must be prime.** **[NOV/DEC 20]**
	Proof: Let $Char(F) = n > 0$. If n is not prime, we write $n = mk$ where $m, k \in Z^+$ and $1 < m < n, 1 < k < n$. By definition of Characteristic, $nu = z$, the zero of F. Hence $(mk)u = z.$ But $(mk)u = \underbrace{(u+u+......u)}_{mk\ summation} = \underbrace{(u+u+u.....+u)}_{m\ summation}.\underbrace{(u+u+u.....+u)}_{k\ summation} = (mu)(ku)$ With F as field, $(mu)(ku) = z$ $\Rightarrow (mu) = z \ or \ (ku) = z$ Assume without loss of generality, $(ku) = z$. Then for each $r \in F$, $kr = k(ur)$ $= (ku)r$ $= zr = z,$ contradicting the choice of n as the $Char(F)$ $\therefore Char(F) = n$ is prime.
3ii)	**In $Z_3[x], s(x) = x^2 + x + 2$ Show that s(x) is irreducible over Z_3 and construct the field $\frac{Z_3[x]}{< s(x) >}$ What is the order of the field? Also Find (i) [x+2][2x+2]+[x+1] (ii)** $[2x+1]^{-1}$
	Solution: Here $Z_3 = \{0,1,2\}$, $s(x) = x^2 + x + 2$ $s(0) = 2 \neq 0$ $s(1) = 1+1+2 \equiv 1(\bmod 3) \neq 0$ $s(2) = 4+2+2 \equiv 8(\bmod 3) \neq 0$ Therefore s(x) has no root in Z_3. Hence s(x) is irreducible in Z_3[x]. Therefore $\frac{Z_3[x]}{< s(x) >}$ is a field Since deg s(x) = 2 , this field has 9 elements. This field consists of 9 different equivalence classes Let $f(x) \in z_3[x]$ then $f(x) = q(x)(x^2 + x + 2) + r(x)$, where $r(x) = 0$ (Or) $\deg r(x) < \deg(x^2 + x + 2) = 2$ $\therefore \deg r(x)$ is 0 (or) 1

$\therefore\ r(x)=ax+b \quad and\,[f(x)]=[r(x)]$

Each a and b can take 3 values

S. No	Values of a and b	$r(x)=ax+b$	Equivalent Classes
1	a=0 , b =0	$r(x)=0x+0=0$	$[0]$
2	a=0 , b =1	$r(x)=0x+1=1$	$[1]$
3	a=0 , b =2	$r(x)=0x+2=2$	$[2]$
4	a=1 , b =0	$r(x)=1x+0=x$	$[x]$
5	a=1 , b =1	$r(x)=1x+1=x+1$	$[x+1]$
6	a=1 , b =2	$r(x)=1x+2=x+2$	$[x+2]$
7	a=2 , b =0	$r(x)=2x+0=2x$	$[2x]$
8	a=2 , b =1	$r(x)=2x+1=2x+1$	$[2x+1]$
9	a=2 , b =2	$r(x)=2x+2=2x+2$	$[2x+2]$

Therefore $\dfrac{Z_3[x]}{<x^2+x+2>}=\{\,[0]\ ,[1]\ ,[2]\ ,[x]\ ,[x+1]\ ,[x+2]\ ,[2x]\ ,[2x+1]\ ,[2x+2]\ \}$

The order of the field is 9

(i) To find $[x+2][2x+2]+[x+1]$

Now $[x+2]\ [2x+2]=[2x^2+6x+4]=[2x^2+0x+4]=[2x^2+4]=[x]$

$$\begin{array}{r|l} & \quad 2 \\ \hline & \cancel{2x^2}+4 \\ x^2+x+2 & \cancel{2x^2}+2x+4 \\ & ---------- \\ & \qquad -2x=x \end{array}$$

Therefore $[x+2]\ [2x+2]\ +\ [x+1]\ =\ [x]+[x+1]=[2x+1]$

(ii) To Find $[2x+1]^{-1}$

Now consider $[2x+1][2x]=[4x^2+4x]$

$=[x^2+x]$ Since $4\equiv 1(\bmod 3)$

$=[-2]$ Since $x^2+x\equiv -2(\bmod x^2+x+2)$

$=[1]$ Since $-2\equiv 1(\bmod 3)$

$\therefore\ [2x+1][2x]=[1]$

$\Rightarrow [2x+1]^{-1}=[2x]$

4 **Prove that a finite field has order p^t, where p is prime and $t\in Z^+$.** **[NOV/DEC 19]**

Proof:

Let *u* denote the unity and *z* the zero element.

Given that is a finite field and *Char(F) = p*, *p* is prime

Then S_0 =*{u,2u,3u, …..pu = z}*is a set of *p* distinct element in *F*

If not, *mu = nu* for *1≤m ≤n ≤p* and *(n – m)u = z* with *0 < n – m < p*

For any *x* ∈*F*, *(n – m)x =(n – m)ux*

=[(n – m)u]x

= zx =z

this is contradiction to *Char(F) = p*

⇒ S_0 =*{u,2u,3u, …..pu = z}*is a set of *p* distinct element in *F*

If $F = S_0$, then $|F| = p^1$ and the result as follows.

If not let $a \in F - S_0$, then $S_1 =\{ma + nu/ 0 < m, n \leq p\}$ is a sub set of F with $| S_1 | \leq p^2$

If $| S_1 | \leq p^2$,

then $m_1 a + n_1 u= m_2 a + n_2 u$ with $0 < m_1,m_2, n_1,n_2 \leq p$

and at least one $m_1 - m_2$, $n_1 - n_2 \neq 0$.

If $m_1 - m_2 =0$, then $(m_1 - m_2)a = z = (n_1 - n_2)u$, with $0 < | n_1 - n_2 | < p$

So, $\forall x \in F$, $|n_1 - n_2 |x = |n_1 - n_2 |(ux)$

$= (|n_1 - n_2 |u)x$

$= zx = z$

with $0 < |n_1 - n_2 |< p = Char(F)$ A contradiction

If $n_1 - n_2 = 0$, then $(m_1 - m_2)a = z$ with $0 < | m_1 - m_2 | < p$

Since F is a field and $a \neq z$, we know that $a^{-1} \in F$

so $(m_1 - m_2)a\, a^{-1} = z\, a^{-1}$

$= z$ with $0 < | m_1 - m_2 | < p = Char(F)$ which is another contradiction.

Hence neither $m_1 - m_2 \neq 0$ nor $n_1 - n_2 \neq 0$.

Therefore $(m_1 - m_2)a = (n_1 - n_2)u \neq z$

Choose $k \in Z^+$ such that $0 < k < p$ and $k(m_1 - m_2)\equiv u(mod\ p)$

[since p is prime, Z_p is field $\Rightarrow$multiplicative inverse exists in Z_p]

Then $a = au$

$= a(m_1 - m_2)k$

$= k(m_1 - m_2)a$ $= k(n_1 - n_2)u$

[since p is prime, Z_p is field and $0 < k, n_1 - n_2 < p$

$\Rightarrow k(n_1 - n_2) \in Z_p$ by closure property on multiplication Z_p]

$\Rightarrow a \in S_0$, one more contradiction.

Hence $| S_1 | = p^2$, and if $F = S_1$ the theorem is proved.

If not, continue this process with an element $b \in F - S_1$

Then $S_2 =\{lb+ ma + nu/ 0 < l, m, n \leq p\}$ will have order p^3

Since F is finite ,

we reach a point where $F = S_{t-1}$ for some $t \in Z^+$ and $|F| =| S_{t-1} |= p^t$, where p is prime

5i) If F is a field, then prove that F[x] is an integral domain and not a field

Proof:

Given that F is a filed. Therefore, F is a commutative ring.

Therefore $F[x]$ is a commutative ring.

Case (1) To prove F is an integral Domain

Let $ab \neq 0, a \neq 0$ in F.

$$a^{-1}(ab) = a^{-1}(0) = 0$$

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

Therefore, F Is an integral Domain.

Case (2) To Prove $F[x]$ is an integral Domain

Let $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + ... + a_mx^m$, $(a_m \neq 0)$ and

$g(x) = b_0 + b_1x + b_2x^2 + b_3x^3 + ... + b_nx^n, (b_n \neq 0)$

Be any two non-zero elements in $F[x]$.

Since R is integral domain and $a_m, b_n \neq 0$, so as $a_mb_n \neq 0$.

The product of $f(x)g(x)$ of $f(x)$ and $g(x)$ will contain the term $a_mb_nx^{m+n}$

Therefore $f(x)g(x) \neq 0$.

Therefore $f(x) \neq 0$, $g(x) \neq 0 \Rightarrow f(x)g(x) \neq 0$.

F[x] is an integral domain.

Case (3) To Prove $F[x]$ is not a filed

Let $f(x)(\neq 0) \in F$ and deg $f(x) \geq 1$. The unit element of F is the constant polynomial ‘1’.

If possible, there exists a multiplicative inverse of $f(x)$ exists and let it be $g(x)$.

$\therefore f(x)g(x) = 1$ ....(1)

$\Rightarrow g(x) \neq 0.$

Suppose $g(x) = 0$, then $f(x)g(x) = 1 \Rightarrow f(x)(0) = 1 \Rightarrow 0 = 1$ which is not possible.

Since F is an integral Domain, we have

$\deg(f(x).g(x)) = \deg(f(x)) + \deg(g(x)) \geq 1.$

$\therefore$ (1) is impossible because deg (1) =0

$\therefore$ A non-zero element in $F[x]$ may not have multiplicative inverse in $F[x]$

$\therefore F[x]$ is not field.

5ii) **State and Prove Division Algorithm**

Statement :

Let F be a field and let $f(x)$ and $g(x)$ be two polynomials in $F(x)$ with $g(x) \neq 0$. Then there exists unique polynomials $q(x)$ and $r(x)$ such that $g(x) = q(x)f(x) + r(x)$ where either $r(x) = 0$ (or) deg $r(x) <$ deg $f(x)$

Proof:

Let $S = \{g(x) - t(x)f(x) / \text{t(x)} \in F\text{[x]}\}$.

If $0 \in S$, $0 = g(x).-t(x)f(x)$, for some $\text{t(x)} \in \text{F[x]}$.

Then with $\text{q(x)} = \text{t(x)}$ and $r(x) = 0$, we have $g(x) = t(x)f(x) + r(\text{x})$.

If $0 \notin S$, Consider the degrees of the elements of S, and let $r(x) = g(\text{x}) - q(x)f(x)$ be an element in S of minimum degree.

Since $r(x) \neq 0$, the result follows if $\deg(r(x)) < \deg(\text{f(x)})$.

If not, let

$$r(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_2 x^2 + a_1 x + a_0, \quad a_n \neq 0$$

$$f(x) = b_m x^m + b_{m-1}x^{m-1} + ... + b_2 x^2 + b_1 x + b_0, \ b_m \neq 0 \quad \text{with } n \geq m.$$

$$\text{Define } h(x) = r(x) - [a_n b_m^{-1} x^{n-m}] f(x)$$

$$= (a_n - a_n b_m^{-1} b_m)x^n + (a_{n-1} - a_n b_m^{-1} b_{m-1})x^{n-1} + ..$$

$$+ ...... + (a_{n-m} - a_n b_m^{-1} b_0)x^{n-m} + a_{n-m-1}x^{n-m-1} + ... + a_1 x + a_0.$$

Then $h(x)$ has degree less than n, the degree of $r(x)$.

More importantly,

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

$$= \text{g(x)} - [q(x) + a_n b_m^{-1} x^{n-m}] f(x) \quad ,$$

so $h(x) \in \text{S}$ and this contradicts the choice of $r(x)$ as having minimum degree.

Consequently $\deg(r(x)) < \deg(f(x))$ and we have the existence part of the theorem.

For uniqueness,

let $g(x) = q_1(x)f(x) + \text{r}_1(x) = q_2(x)f(x) + \text{r}_2(x)$

where $\text{r}_1(x) = 0$ or deg $\text{r}_1(x) <$ deg $f(x)$, and $\text{r}_2(x) = 0$ or deg $\text{r}_2(x) <$ deg $f(x)$.

Then $[q_2(x) - q_1(x)]f(x) = r_1(x) - r_2(x)$,

If $[q_2(x) - q_1(x)] \neq 0$, then $\deg[q_2(x) - q_1(x)]f(x) \geq \deg(f(x))$,

	whereas $[r_1(x)-r_2(x)]=0$ *or* $\deg[r_1(x)-r_2(x)] \le \max\{\deg r_1(x), \deg r_2(x)\} < \deg f(\mathrm{x})$. Consequently $r_1(x)=r_2(x)$ and $q_1(x)=q_2(x)$.

UNIT-III DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS

PART-A

1	**Explain Divisibility.**
	Let $a,b\in z$ we say 'a' divides b if their exist $c\in z$ such that b=ac. 'a' is called divisor or factor of 'b'. and 'b' is called multiple of 'a'. So we write it as a/b (*i.e.*) b is divisible by a. If a does not divide b, then we write $a\nmid \mathrm{b}$.
2	**State the properties of divisibility.**
	(i). $a/\mathrm{b}\Rightarrow a/bc$ for all integer c (ii). If $a/\mathrm{b},\ \mathrm{b}/\mathrm{c}\Rightarrow a/c$ (iii). If $a/\mathrm{b},\ a/\mathrm{c}\Rightarrow a/(\mathrm{bx}+\mathrm{cy})\quad \forall$ integers x & y (iv). If $a/\mathrm{b},\ b/a\Rightarrow a=\pm b$
3	**If** $a/\mathrm{b}, a/c$ **prove that** $a/\mathrm{bx}+\mathrm{cy}\ \forall$ intgers x & y
	since $a/b\Rightarrow b=am$ -----(1); $a/c\Rightarrow c=al$ -----(2) $(1)\times\ x\Rightarrow bx=amx$-----(3) $(2)\times\ y\Rightarrow cy=aly$-----(4) $(3)+(4)\Rightarrow bx+cy=amx+aly=a(mx+ly)$, where $mx+ly$ is integer $\Rightarrow a/(\mathrm{bx}+\mathrm{cy})$
4	**Find the number of positive integers ≤ 2076 and divisible by neither 4 or 5**
	Let $A=\{x\in N/x\le 2076$ and divisible by $4\}$; $B=\{x\in N/x\le 2076$ and divisible by $5\}$ *then* $\lvert A\cup B\rvert=\lvert A\rvert+\lvert B\rvert-\lvert A\cap B\rvert$ $=\lfloor 2076/4\rfloor+\lfloor 2076/5\rfloor-\lfloor 2076/20\rfloor=519+415-103=831$ Thus, among the first 2076 positive integers, there are 2076-831=1245 integers not divisible by 4 or 5.
5.	**Find the number of positive integers ≤ 3076 and not divisible by 17. [NOV/DEC 19]**
	Number of positive integers ≤ 3076 and divisible by 17 $=\left\lfloor\dfrac{3076}{17}\right\rfloor=180$ Therefore number of positive integers ≤ 3076 and not divisible by 17 = 3076 – 180 = 2896
6.	**Add two more rows to the following pattern, and write conjecture formula for the n$^{\text{th}}$ row**: $9\cdot 9+7=88$ $98\cdot 9+6=888$ $987\cdot 9+5=8888$ $9876\cdot 9+4=88888$ $98765\cdot 9+3=888888$
	Answer: The next two rows of the given pattern are, $987654\cdot 9+2=8888888$ $9876543\cdot 9+1=88888888$ The general pattern is $98765.....(10-n)\cdot 9+(8-n)=\underbrace{888.....88}_{(n+1)\,Eights}$
7.	**State the Pigenhole Principle. [NOV/DEC 20]**
	If m pigeons are assigned to n pigenholes where m > n, then atleast two pigeons must occupy the same pigenhole.

8.	**Explain base-b representation.**
	The expression $a_k b^k + a_{k-1} b^{k-1} + ... + a_1 b + a_0$ is the base-b representation of the integer N. Accordingly, we write $N = \left(a_k\, a_{k-1} ..... a_1 a_0\right)_b$ in base b.
9.	**Determine if 1601 is a prime number.**
	We know that if n has no prime factors $\le \lfloor\sqrt{n}\rfloor$, then n is a prime consider prime nos $\le \lfloor\sqrt{1601}\rfloor$ $\Rightarrow$ prime nos ≤ 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.
10.	**Find the GCD of 1819 & 3587.**
	$(3587,1819) = 1\times 1819 + 1768$ $(1819,1768) = 1\times 1768 + 51$ $(1768,51) = 34\times 51 + 34$ $(51,34) = 1\times 34 + 17$ $(34,17) = 2\times 17 + 0$ $\therefore$ gcd of 1819, 3587 is 17
11	**Find the GCD of** $a+b, a^2-b^2$.
	$GCD\left(a+b, a^2-b^2\right) = GCD\left(a+b, (a-b)(a+b)\right) = a+b$
12	**Find a positive integer ‘*a*’ , if** $[a, a+1] = 132$
	We know that $[a,b] = \dfrac{ab}{(a,b)} ------(1)$ Since LCM *of* $[a,\ a+1] = 132$ & GCD of $(a, a+1) = 1$ $(1) \Rightarrow 132 = \dfrac{a\ \times a+1}{1} \Rightarrow a^2 + a - 132 = 0 \Rightarrow a = -12, 11$ Since *a* is positive integer, *a* = 11
13	**Using (252, 360) compute [252, 360].**
	Since GCD of 252 and 360 = $(252, 360) = 36$ $[a,b] = \dfrac{ab}{(a,b)} \Rightarrow [252,\ 360] = \dfrac{252\times 360}{36} = 2520$
14	**If** $(a,4) = 2$ & $(b,4) = 2$ **show that** $(a+b, 4) = 2$
	$(a,4) = 2 \Rightarrow$ gcd of $(a,4) = 2 \Rightarrow 2/a$ but $4 \nmid a$ $\therefore a = 2k$, and k is odd $(\mathrm{b},4) = 2 \Rightarrow$ gcd of $(\mathrm{b},4) = 2 \Rightarrow 2/\mathrm{b}$ but $4 \nmid \mathrm{b}$ $\therefore b = 2l$, and l is odd $a + b = 2k + 2l = 2(k+l) = 2(\text{even}) = 2(2m) = 4m$ $\therefore 4/a+b \Rightarrow \gcd(a+b, 4) = 4$
15	**If x and y are odd integers show that** $x^2 + y^2$ **cannot be perfect square.**
	Since x and y are odd integers $\therefore$ $x^2 + y^2$ is even $\Rightarrow 2/x^2 + y^2$ To prove: $x^2 + y^2$ cannot be perfect square, it is enough to show that $\left(x^2 + y^2, 4\right) = 2$ Let $x = 2k+1, y = 2l+1$ $x^2 + y^2 = 4\left(k^2 + l^2 + k + l\right) + 2$

$\therefore \left(x^2+y^2,4\right)=\left(4\left(k^2+l^2+k+l\right)+2,4\right)=\left(2,4\right)$

hence x^2+y^2 cannot be perfect square.

16 **Prove that any prime of the form 3k+1 is of the form 6k+1.**

Let the prime p =3k+1, then k must be even.
[if k is odd, then 3k is odd ⇒3k+1 is even ⇒ 3k+1 is not prime]
∴ k=2k′, then p =3(2k′)+1=6k′+1.
Hence any prime of the form 3k+1 is of the form 6k+1.

17. **Using canonical decomposition of 1050 and 2574 find their LCM.** **[NOV/DEC 19]**

$1050 = 2\cdot3\cdot5^2.7 \qquad 2574 = 2\cdot3^2\cdot11.13$

$LCM = [1050, 2574] = 2\ \cdot3^2\cdot5^2\cdot7.11.13 = 450$

18. **Find the canonical decomposition of** 2^9-1

$2^9-1=\left(2^3\right)^3-1^3=\left(2^3-1\right)\left(2^6+2^3+1\right) \quad \because\ a^3-b^3=\left(a-b\right)\left(a^2+ab+b^2\right)$

$=\left(7\right)\left(73\right)$

19. **If $\mathbf{d=\left(a,b\right)}$ and d' is any common divisor of a and b, then d'/d.**

Since $\mathrm{d}=\left(\mathrm{a},\mathrm{b}\right)$, ∃ α and β such that $\mathrm{d}=\alpha a+\beta b$.

also since d' is common divisor of a & b. ∴ d'/ a & d'/ b

⇒ d'/ (αa+βb); so d'/d.

20. **Prove that $\mathbf{n^2+n}$ is an even integer, where n is arbitrary integer.**

To prove: $\mathrm{p(n)}=n^2+n$ is an even integer

$\mathrm{p}(1)=1^2+1=2$ is an even number

We assume that the result is true for all k, k be the arbitrary number.

$\Rightarrow \mathrm{p(k)}=k^2+k$ is an even integer

consider $\mathrm{p(k+1)}=\left(k+1\right)^2+\left(k+1\right)$

$=k^2+2k+1+k+1$

$=\left(k^2+k\right)+\left(2k+2\right)=$ Even number

hence p(n)=n^2+n is even integer ∀ n.

PART-B

1i) **Find the number of positive integers in the range 1976 through 3776 that are divisible by13.**

Solution:

The number of positive integers ≤1976 that are divisible by 13 $=\left\lfloor\dfrac{1976}{13}\right\rfloor$

$=152$

The number of positive integers ≤3776 that are divisible by 13 $=\left\lfloor\dfrac{3776}{13}\right\rfloor$

$=290$

∴ The number of positive integers 1976 to 3776 that are divisible by 13

$=290-152+1$

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

1ii) Prove that $(a,\, a-b)=1$ if and only if $(a,\, b)=1$

Proof:

Let $(a,\, a-b)=1$

Then there exist integer l and m such that

$$la+mb=1$$
$$la+ma+mb-ma=1$$
$$(l+m)a-m(a-b)=1$$
$$(l+m)a+(-m)(a-b)=1$$
$$\Rightarrow (a,a-b)=1$$

Conversely, let $(a,a-b)=1$. To prove : $(a,b)=1$

Then there exist integer α and β such that

$\alpha a+\beta(a-b)=1$

$\alpha a+\beta a-\beta b=1$

$(\alpha+\beta)a+(-\beta)b=1 \qquad \Rightarrow (a,b)=1$

1iii) Obtain six consecutive integers that are composite. [NOV/DEC 20]

Solution:

By theorem, for every integer n, there are n consecutive integers that are composite numbers.
Then the six consecutive composite numbers are

$(n+1)!+2,\ (n+1)!+3, (n+1)!+4,\ (n+1)!+5,\ (n+1)!+6,\ (n+1)!+7$

put $n=6$

$\therefore$ The six consecutive composite numbers are $5042, 5043, 5044, 5045, 5046,$ and 5047

2i) Apply Euclidean Algorithm and express (4076, 1024) as a linear combination of 4076, 1024.

Solution:

By successive application of division algorithm, we get:

$$4076=3\cdot 1024+1004$$
$$1024=1\cdot 1004+20$$
$$1004=50\cdot 20+4$$
$$20=5\cdot 4+0$$

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

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

2ii) Prove that there are infinitely many primes. [NOV/DEC 19,20]

Proof:

We prove by contradiction method.

Assume that there are only n primes $p_1, p_2, ..., p_n$ where n is prime.

Now consider the integer

$m=p_1\cdot p_2\cdot p_3 ..., p_n$

Since $m > 1$, by theorm, every integer $n \ge 2$ has a prime factor. $\therefore$ m has a prime factor p.

But none of the primes $p_1, p_2, p_3, ..., p_n$ divide m

For, if p_i / m and since $p_i / p_1 \cdot p_2 \cdot p_3 ..., p_n$

we get $p_i / m - p_1 \cdot p_2 \cdot p_3 ..., p_n \Rightarrow p_i / 1$, which is not true and hence a contradiction.

$$\therefore\ p_i \nmid m$$

So, we have a prime p which is not in the list of n primes.

Thus, we have n+1 primes $p_1, p_2, p_3, ..., p_n, p_{n+1}$

which contradicts the assumption there are only n primes.

So, our assumption of finiteness is wrong. Hence the number of primes is infinite.

3i) **Prove that the GCD of the positive integers a &b is linear combination of a and b.** **[NOV/DEC 19]**

Proof:

Let S be the set of positive linear combination of a and b; that is

$S = \{ma + nb / ma + nb > 0, m, n \in Z\}$

To show that S has a least element:

Since $a > 0$, $a = 1 \cdot a + 0 \cdot b \in S$, So S is non empty.

So, by the well-ordering principle, S has a least positive element d.

To show that $d = (a, b)$:

Since d belongs to S, d $= \alpha a + \beta b$ for some integer α and β.

1. First we will show that d / a and d / b :

By the division algorithm,

there exist integers q and r such that $a = dq + r$, where $0 \le r < d$.

$$\begin{aligned} r &= a - dq \\ &= a - (\alpha a + \beta b) q \qquad \text{substituting for d.} \\ &= (1 - \alpha q) a + (-\beta q) b \backslash \end{aligned}$$

This shows r is a linear combination of a and b.

If $r > 0$, then r $\in S$. Since $r < d$, r is less than the smallest element in S.

Which is a contrdiction. So $r = 0$; thus, a = dq, so d / a.

Similarly, d/b. Thus d is common divisor of a and b.

2. To show that any positive common divisior d' of a and b is $\le$ d :

Since d'/a, and $d'/b \Rightarrow d'/(\alpha a + \beta b)$

that is d'/d. So $d' \le d$.

Thus, by parts (1) and (2), d $= (a, b)$

3ii) **Show that for any integer n,** n^2-n **is divisible by 2 and** n^5-n **is divisible by 30.**

Solution:

$n^2 - n = n(n-1)$, product of two consecutive natural numbers is always divisible by2

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

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

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

Now to prove divisibility by 5, First we write the factorization as under

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

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 5×6=30.
Hence the proof.

4i) Using recursion, evaluate (18, 30, 60, 75, 132).

Solution.:

$$(18,30,60,75,132)=\left((18,30,60,75),132\right)$$
$$=\left(\left((18,30,60),75\right),132\right)$$
$$=\left(\left(\left((18,30),60\right),75\right),132\right)$$
$$=\left(\left((6,60),75\right),132\right)$$
$$=\left((6,75),132\right)=(3,132)=3$$

4ii) Find the number of positive integers ≤ 3000 and divisible by 3, 5, or 7. [NOV/DEC 20]

Solution:

Let A,B,C be the set of numbers ≤ 3000 and divisible by 3, 5,7 respectively.

Required $|A\cup B\cup C|$

By inclusion and exclusion principle, we get

$$|A\cup B\cup C|=S_1-S_2+S_3$$

Now

$$|A|=\left[\frac{3000}{3}\right]=[1000]=1000$$
$$|B|=\left[\frac{3000}{5}\right]=[600]=600$$
$$|C|=\left[\frac{3000}{7}\right]=[428.57]=428$$
$$S_1=|A|+|B|+|C|=1000+600+428=2028$$
$$|A\cap B|=\left[\frac{3000}{3\times 5}\right]=[200]=200$$
$$|A\cap C|=\left[\frac{3000}{3\times 7}\right]=[142.85]=142$$
$$|B\cap C|=\left[\frac{3000}{5\times 7}\right]=[85.71]=85$$
$$S_2=|A\cap B|+|A\cap C|+|B\cap C|=200+142+85=427$$

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

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

4iii) Show that product of k consecutive integers is divisible by k!

Proof:

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

Product of 'k' consecutive integer $=(n+1)(n+2)\cdots(n+k)$

$$=\frac{n!}{n!}(n+1)(n+2)\cdots(n+k) = \frac{(n+k)!}{n!}$$

Product of 'k' consecutive integer$=\frac{k!(n+k)!}{k!\ n!} = k!\ n+rC_r$ = Integer

Hence the product of k consecutive integers is divisible by k!

5i) State and prove fundamental theorem of arithmetic. [NOV/DEC 20]

Statement:

Every integer $n \geq 2$ either is a prime or can be expressed as a product of primes. The factorization into primes is unique except for the order of the factors.

Proof:

First, we will show by strong induction that n either is a prime or can be expressed as a product of primes. Then we will establish the uniqueness of such a factorization.

Let P(n) denote the statement that n is a prime or can be expressed as a product of primes.

To show that $P(n)$ is true for every integer $n \geq 2$:

since 2 is a prime, clearly P(2) is true.

Now assume P(2), P(3),…..P(k) are true; that is every integer 2 through k either is a prime or can be expressed as a product of primes.

If k+1 is a prime, then P(k+1) is true. So suppose k+1 is composite.

Then k+1 = ab for some integers a and b, where 1 < a, b < k+1.

By the inductive hypothesis, a and b either are primes or can be expressed as products of primes; in any event, k+1=ab can be expressed as products of primes.

Thus, P(k+1) is also true.

Thus by strong induction, the result holds for every integer $n \geq 2$

<u>To Establish the Uniqueness of the Factorization:</u>

Let n be a composite number with two factorization into primes; $n = p_1p_2\cdots p_r = q_1q_2\cdots q_s$

we will show that r = s and every p_i equals some q_j ,where $1 \leq i, j \leq r$;

that is, the primes $q_1, q_2, ...q_s$ are a permutation of the primes $p_1p_2\cdots p_r$

Assume, for convenience that $r \leq s$

since $p_1p_2\cdots p_r = q_1q_2\cdots q_s,\ \ p_1 / q_1q_2\cdots q_s,$

$$\Rightarrow p_1 = q_i \text{ for some i.}$$

Dividing both sides p_1, we get: $p_2.....p_r = q_1q_2...q_{i-1}\cancel{q_i}q_{i+1}...q_s$

Now, p_2 divides the RHS, so $p_2 = q_j$ for some j. *cancel p_2* form both sides:

$p_3.....p_r = q_1q_2...q_{i-1}\cancel{q_i}q_{i+1}...q_{j-1}\cancel{q_j}q_{j+1}q_s$

Since $r \leq s$, continuing like this, we can cancel p_t with some q_k.

This yields a 1 on the LHS at the end.

Then the RHS cannot be left with any primes, since a product of primes can never yield a 1; thus, we must have exhausted all q_k's by now.

therefore, r = s and hence the primes $q_1, q_2, ...q_s$ are the same as the primes $p_1p_2\cdots p_r$ in some order.

Thus, the factorization of n is unique, except for the order in which the primes as written.

5ii)	**Prove that the product of gcd and lcm of any two positive integers a and b is equal to their products. [NOV/DEC 19]**
	Proof: Let $a = p_1^{a_1} p_2^{a_2} .....p_n^{a_n}$, $b = p_1^{b_1} p_2^{b_2} .....p_n^{b_n}$ be the canonical decomposition of a and b. Then $[a,b] = p_1^{\max\{a_1,b_1\}} p_2^{\max\{a_2,b_2\}} .....p_n^{\max\{a_n,b_n\}}$ $(a,b) = p_1^{\min\{a_1,b_1\}} p_2^{\min\{a_2,b_2\}} .....p_n^{\min\{a_n,b_n\}}$ $\Rightarrow [a,b](a,b) = p_1^{\max\{a_1,b_1\}+\min\{a_1,b_1\}} p_2^{\max\{a_2,b_2\}+\min\{a_2,b_2\}} .....p_n^{\max\{a_n,b_n\}+\min\{a_n,b_n\}}$ $= p_1^{a_1+b_1} p_2^{a_2+b_2} .....p_n^{a_n+b_n}$ $= \left(p_1^{a_1} p_2^{a_2} .....p_n^{a_n}\right)\left(p_1^{b_1} p_2^{b_2} .....p_n^{b_n}\right)$ $= ab$ Hence $[a,b] = \frac{ab}{(a,b)}$

UNIT – IV DIOPHANTINE EQUATIONS AND CONGRUENCES
PART- A

1	**Define congruence modulo m.**
	If an integer m ($\neq 0$) divides the difference $a-b$, we say that a is congruent to b modulo m. $(i.e)\ a \equiv b(\text{mod}\, m)$.
2	**Define linear congruence.**
	A congruence of the form $ax \equiv b(\text{mod}\, m)$ is called a linear congruence. An integer x_1 is said to be a solution or root of this congruence, if $ax_1 \equiv b(\text{mod}\, m)$ $(i.e)$ $m \mid ax_1 - b$.
3	**Solve the congruence** $4x \equiv 5(\text{mod } 6)$.
	$4x \equiv 5(\text{mod } 6)$ Here $a = 4,\ b = 5,\ m = 6$ $(a,m) = (4,6) = 2 \Rightarrow 2 \nmid 5 \quad (i.e)\ (a,m) \nmid b$ $\therefore$ The congruence has no solution.
4	**What is digital root of a positive integer? What are the digital roots of square numbers? Is 16151613924 a square?**
	Let N = $(a_n a_{n-1} ... a_1 a_0)_{\text{ten}}$ and d be its digital root, then d $\equiv (a_n + a_{n-1} + ... + a_1 + a_0)$ (mod9). (i.e) the digital root of N is the remainder when N is divided by 9 with one exception: it is 9 if the remainder is 0. The digital roots of square numbers are 1, 4, 7, or 9. 1+6+1+5+1+6+1+3+9+2+4=39 $\Rightarrow$ remainder is 3 when divided by 9 Therefore digital root of 16151613924 is 3. Hence 16151613924 is not a square.

5	**Solve** $x^7+1\equiv 0\,(\text{mod } 7)$
	The complete residue system (CRS) *is* $\{0,1,2,3,4,5,6\}$ But $4\equiv -3\ (\text{mod } 7)$ $5\equiv -2\ (\text{mod } 7)$ $6\equiv -1\ (\text{mod } 7)$ The CRS is $\{0,\pm 1,\pm 2,\pm 3\}$ The CRS does not satisfy the congruence $x^2+1\equiv 0\,(\text{mod } 7)$ $\therefore$ The given congruence has no solution.
6	**State 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 $x\equiv a_i\,(\text{mod } m_i)$, $\text{i}=1,2,\ldots.,\text{r}$ have common solution.
7	**Determine whether the LDEs 12*x* + 18*y* = 30, 2*x* + 3*y* = 4, and 6*x* + 8*y* = 25 are solvable.**
	$(12,18)=6$ and $6\,\|\,30$, so the LDE $12x+18y=30$ has a solution. $(2,3)=1$, so the LDE has a solution. $(6,8)=2$, but $2\nmid 5$, so the LDE $6x+8y=25$ is not solvable.
8	**Prove that** $a\equiv b\,(\text{mod}\,m)$ if and only if $a=b+km$ for some integer k.
	Suppose $a\equiv b\,(\text{mod } m)$. Then $m/(a\text{-}b)$, so $a-b=km$ for some integer k. $(i.e)\ a=b+km.$ Conversely, suppose $a=b+km.$ *Then* $a-b=km$, *so* $m/(a-b)$ and consequently, $a\equiv b(\text{mod}\,m)$.
9	**Find the remainder when** $1!+2!+\ldots\ldots+100!$ **is divided by 15.**
	Notice that when $k\geq 5$, $k!\equiv 0\ (\text{mod } 15)$ $1!+2!+\ldots..+100!\equiv 1!+2!+3!+4!+0+\ldots..+0\,(\text{mod } 15)$ $\equiv 1+2+6+24\,(\text{mod}15)$ $\equiv 1+2+0\,(\text{mod}15)$ $\equiv 3(\text{mod}15)$ Thus, when the given sum is divided by 15, the remainder is 3.
10	**Let** $a\equiv b(\text{mod}\,m)$ *and* $c\equiv d\,(\text{mod}\,m)$, **then prove that** $a+c\equiv b+d\,(\text{mod}\,m)$.
	Since $a\equiv b(\text{mod } m)$ and $c\equiv d\,(\text{mod}\,m)$, $a=b+lm$ *and* $c=d+km$ for some inegers l and $m.$ Then $a+c=(b+lm)+(d+km)$ $=(b+d)+(l+k)m$ $=b+d\,(\text{mod}\,m)$
11	**Let** $a\equiv b(\text{mod}\,m)$ *and* $c\equiv d\,(\text{mod}\,m)$, **then prove that** $ac\equiv bd\,(\text{mod}\,m)$.
	Since $a\equiv b(\text{mod } m)$ and $c\equiv d\,(\text{mod}\,m)$, $a=b+lm$ *and* $c=d+km$ for some inegers l *and* $m.$ Then $ac-bd=(ac-bc)+(bc-bd)$ $=c(a-b)+b(c-d)$ $=clm+bkm$ $=(cl+bk)m$ $\quad\therefore\ ac\equiv bd\,(\text{mod}\,m)$

12	**Find the remainder when** 16^{53} is divided by 7.
	$16 \equiv 2 (\bmod 7).$ If a $\equiv b (\bmod m)$, then $a^n \equiv b^n (\bmod m)$ for any positive integer $n \Rightarrow 16^n \equiv 2^n (\bmod 7).$ $16^{53} \equiv 2^{53} (\bmod 7)$ $2^3 \equiv 1 (\bmod 7)$ $\therefore 2^{53} \equiv 2^{3(17)+2}$ $\equiv (2^3)^{17}.2^2$ $\equiv 1^{17}.4(\bmod 7) \equiv 4(\bmod 7)$ So $16^{53} \equiv 4 (\bmod 7)$, by the transitive property. Thus, when 16^{53} is divided by 7, the remainder is 4
13	**Find the remainder when** 3^{31} **is divided by 7.** **[NOV/DEC 19]**
	$3^2 \equiv 2 (\bmod 7)$ $(3^2)^3 \equiv 2^3 (\bmod 7) = 1(\bmod 7) \Rightarrow 3^6 = 1(\bmod 7)$ $\therefore 3^{31} = (3^6)^5.3 \equiv 1^5.3 \ (\bmod\ 7)$ $\equiv 3(\bmod 7)$ Thus the remainder is 3.
14	**Determine whether the LDE** $2x + 3y + 4z = 5$ **is solvable?** **[NOV/DEC 19]**
	The gcd $(2,3,4) = 1$ i.e., $(2,3,4) = 1$ and $1/5 \Rightarrow$ The given LDE is Solvable.
15	**Define 2X2 linear system**
	A 2×2 linear system is a system of linear congruences of the form, $ax + by \equiv e(\bmod m); \quad cx + dy \equiv f(\bmod m)$ A solution of the linear system is a pair $x \equiv x_0 (\bmod m), y \equiv y_0 (\bmod m)$ that satisfies both congruences.
16	**Show that** $\mathbf{x \equiv 12 (mod\ 13)}$ **and** $\mathbf{y \equiv 2(mod 13)}$ **is a solution of the** $\mathbf{2 \times 2}$ **linear system** $\mathbf{2x + 3y \equiv 4(mod 13)}$ $\mathbf{3x + 4y \equiv 5(mod 13).}$
	When $x \equiv 12 (\bmod 13)$ and $y \equiv 2 (\bmod 13)$, $2x + 3y \equiv 2(12) + 3(2) \equiv 4(\bmod 13)$ $3x + 4y \equiv 3(12) + 4(2) \equiv 5(\bmod 13)$ Therefore, every pair $x \equiv 12 (\bmod 13), y \equiv 2 (\bmod 13)$ is a solution of the system.
17	**Verify that the linear system 2x+3y≡4(mod13) and 3x +4y ≡5 (mod 13) has a unique solution modulo 13.**
	We know that the system has a unique solution modulo m if and only if $(\Delta, m) = 1$ $\Delta = ad - bc = \begin{vmatrix} 2 & 3 \\ 3 & 4 \end{vmatrix} = -1 \equiv 12(\bmod 13).$ Since (12,13)=1 Therefore the system has a unique solution modulo 13.
18	**Prove that no prime of the form 4n + 3 can be expressed as the sum of two squares.** **[NOV/DEC 20]**
	Let N be a prime of the form 4n + 3. Then $N \equiv 3(\bmod 4).$ Suppose $N = A^2 + B^2$ for some integers A and B. Since N is odd, one of the squares (say A^2) must be odd and hence B^2 must be even. Then A must be odd and B even.

	Let $A=2a+1$ and $B=2b$ for some integers a and b. Then $N=(2a+1)^2+(2b)^2$ $=4(a^2+b^2+a)+1$ $=1(\text{mod}\,4)$ which is a contradiction, since $N=3(\text{mod}\,4)$
19	**Show that a palindrome with an even number of digits is divisible by 11.**
	Let be $n=n_{2k-1}n_{2k-2}......n_1n_0$ palindrome with an even number of digits $n=(n_0+\text{n}_2+.....+\text{n}_{2k-2})-(n_1+\text{n}_3+.....+\text{n}_{2k-1})(\text{mod}\,11)$ $=0\ (\text{mod}\,11)$ because n is palindrome with an even number of digits *Thus*, $11\,|\,n$.
20	**Define complete residue system.**
	A set $x_1,x_2,....,x_m$ is a complete residue system mod m if for integer y, there is one and only one x_j such that $y\equiv x_j(\text{mod}\,m)$.
	PART B
1i)	**Show that n^2+ n ≡ 0(mod 2) for any positive integer n.**
	Proof: $a\equiv b(\text{mod}\,k)\Rightarrow a-b\equiv km,\quad m\in z$ $a-b$ is divisible by k $n=\text{even}=2m$ $n^2+n=(2m)^2+(2m)=4m^2+2m=2(2m^2+m)$ n^2+n is divisible by 2 $n=\text{odd}=2m+1$ $n^2+n=(2m+1)^2+(2m+1)$ $=4m^2+4m+1+2m+1$ $=4m^2+6m+2$ $=2(2m^2+3m+1)$ n^2+n is divisible by $2\Rightarrow n^2+n\equiv 0(\text{mod}\,2)$
1ii)	**Prove that p is a prime iff (p – 1)! +1 ≡ 0(mod p).**
	Proof: Suppose p is not a prime then $p=p_1p_2$ where $1<p_1,p_2<p-1$ since $1<p_1<p-1$, we find p_1 is a factor of $(p-1)!$ $(ie)\quad p_1/(p-1)!$ Also p_1/p we are given $(p-1)!+1\equiv 0(\text{mod}\,p)$ $\therefore\ p/(p-1)!+1$ $\therefore\ p_1/(p-1)!+1$ Thus $p_1/(p-1)!+1$ & $p_1/(p-1)!\Rightarrow p_1/\left[(p-1)!+1\right]-(p-1)!$ $\therefore\ p_1/1$ which is not possible $\because p_1>1$ Hence p must be prime.

2 **State and prove Chinese remainder theorem. Using it 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. [NOV/DEC 19]**

Statement:

Let $m_1, m_2, ..., m_r$ denote r positive integers that are relatively prime in pairs and let $a_1, a_2, ..., a_r$ be any r integers. Then the congruence $x \equiv a_i (\text{mod } m_i)$, $\text{i} = 1, 2, ..., \text{r}$ have common solution.

Proof:

$Part1$: Existence of the solution

Let $n = m_1.m_2.m_3...m_k$ & $n_i = \frac{n}{m_i}$, $i = 1, 2, 3, ..., k.$

Since $m_1.m_2.m_3...m_k$ are pairwise relatively prime $(n_i, m_i) = 1$, $i = 1, 2, 3, ..., k$

Also $n_i \equiv 0 (\text{mod } m_j)$, $i \neq j$

Since $(n_i, m_i) = 1$, the congruence $n_i y_i \equiv 1 (\text{mod } m_i)$ has a unique solution y_i, $i = 1, 2, 3, ..., k$

Let $x = a_1 n_1 y_1 + a_2 n_2 y_2 + ... + a_k n_k y_k$

Now, we will show that x is a solution of the system of congruences.

Since $n_i \equiv 0 (\text{mod } m_k)$ *for* $i \neq k$, all terms except the k^{th} term in this are congruent to 0 modulo m_k

Since $n_k y_k \equiv 1 (\text{mod } m_k)$, we see that $x = a_k n_k y_k \equiv a_k (\text{mod } m_k)$, for $k = 1, 2, 3, ..., n$

Thus x satisfies every congruence in the system.

Hence x is a solution of the linear system.

$Part2$: *Uniquness* of the solution

Solution is unique *in* modulo $n = m_1.m_2.....m_k$.

Let x_1, x_2 be two solutions of the system

To prove $x_1 \equiv x_2 (\text{mod } n)$

Since $x_1 \equiv a_j (\text{mod } m_j)$ and $x_2 \equiv a_j (\text{mod } m_j)$, $j = 1, 2, 3, ..., k$

we have $x_1 - x_2 \equiv 0 (\text{mod } m_j) \Rightarrow m_j | x_1 - x_2$ for every j

Since $m_1, m_2, ..., m_k$ are pairwise ralatively prime,

$$LCM[m_1, m_2, ..., m_k] = m_1, m_2, ..., m_k | x_1 - x_2$$

$\Rightarrow \quad n | x_1 - x_2 \Rightarrow x_1 \equiv x_2 (\text{mod } n)$

Hence the solution is unique mod $m_1 m_2 ... m_k$.

Given system is $x \equiv 1 (\text{mod } 3)$; $x \equiv 2 (\text{mod } 4)$; $x \equiv 3 (\text{mod } 5)$

Here $a_1 = 1$, $a_2 = 2$, $a_3 = 3$; $m_1 = 3$, $m_2 = 4$, $m_3 = 5$

We find m_1, m_2, m_3 are pairwise relatively prime

Let $n = \text{m}_1 m_2 m_3 = 3.4.5 = 60$

and $n_1 = \frac{n}{m_1} = \frac{3.4.5}{3} = 20$; $n_2 = \frac{n}{m_2} = \frac{3.4.5}{4} = 15$; $n_3 = \frac{n}{m_3} = \frac{3.4.5}{5} = 12$

1. We find y_1, y_2, y_3 from the congruences

$n_1 y_1 \equiv 1 (\text{mod } m_1)$

$n_2 y_2 \equiv 1 (\text{mod } m_2)$

$n_3 y_3 \equiv 1 (\text{mod } m_3)$

	We have $n_1 y_1 \equiv 1(\bmod m_1)$, $20 y_1 \equiv 1(\bmod 3)$, Since $20.2 \equiv 40 \equiv 1(\bmod 3)$, we see $y_1 = 2$ is a solution We have $n_2 y_2 \equiv 1(\bmod m_2)$, $15 y_2 \equiv 1(\bmod 4)$, Since $15.3 \equiv 45 \equiv 1(\bmod 4)$, we see $y_2 = 3$ is a solution We have $n_3 y_3 \equiv 1(\bmod m_3)$, $12 y_3 \equiv 1(\bmod 5)$, Since $12.3 \equiv 36 \equiv 1(\bmod 5)$, we see $y_3 = 3$ is a solution 2. Then solution is $x \equiv a_1 n_1 y_1 + a_2 n_2 y_2 + a_3 n_3 y_3 \ (\bmod n)$ $\therefore$ $x \equiv 1.20.2 + 2.15.3 + 3.12.3 \ (\bmod 60)$ $\Rightarrow$ $x \equiv 40 + 90 + 72 \ (\bmod 60)$ $\Rightarrow$ $x \equiv 238 \ (\bmod 60)$ $\Rightarrow$ $x \equiv 58 \ (\bmod 60)$ $\therefore$ 58 is the unique solution $(\bmod 60)$ $\therefore$ the solution of the system is $x \equiv 58 \ (\bmod 60)$ and it is the unique solution.
3i)	**Solve the congruence** $x \equiv 1(\bmod 4),\ x \equiv 0(\bmod 3),\ x \equiv 5(\bmod 7)$.
	Solution: *Here* $a_1 = 1,\ a_2 = 0,\ a_3 = 5;\quad m_1 = 4,\ m_2 = 3,\ m_3 = 7$ $m = m_1 . m_2 . m_3 = 4.8.7 = 84$ $\frac{m}{m_1} = \frac{84}{4} = 21;\ \frac{m}{m_2} = \frac{84}{3} = 28;\ \frac{m}{m_3} = \frac{84}{7} = 12$ $\left(\frac{m}{m_1}, m_1\right) = (21,4) = 1;\ \left(\frac{m}{m_2}, m_2\right) = (28,3) = 1;\ \left(\frac{m}{m_3}, m_3\right) = (12,7) = 1$ *we know that* $\left(\frac{m}{m_j}\right) b_j \equiv 1(\bmod m_j)$ For $m_1 \Rightarrow \left(\frac{m}{m_1}\right) b_1 \equiv 1(\bmod m_1)$ $(21) b_1 \equiv 1(\bmod 4) \Rightarrow 4 / 21 b_1 - 1$ $\Rightarrow$ $21 b_1 - 1 = 4k$, k is an integer $21 \mathrm{b}_1 = 1 + 4k$ $b_1 = \frac{1+4k}{21}$ put $k = 5,\ b_1 = 1$ For $m_2 \Rightarrow \left(\frac{m}{m_2}\right) b_2 \equiv 1(\bmod m_2)$ $(28) b_2 \equiv 1(\bmod 3) \Rightarrow 3 / 28 b_2 - 1$

$\Rightarrow \qquad 28b_2 - 1 = 3k, \quad k$ is an integer

$$28b_2 = 1 + 3k$$

$$b_2 = \frac{1+3k}{28}$$

put $k = 9, \quad b_2 = 1$

For $m_3 \Rightarrow \left(\frac{m}{m_3}\right) b_3 \equiv 1 (\operatorname{mod} m_3)$

$$(12) b_3 \equiv 1 (\operatorname{mod} 7) \Rightarrow 7 / 12b_3 - 1$$

$\Rightarrow \qquad 12b_3 - 1 = 7k_2, \quad k_2$ is an integer

$$12b_3 = 1 + 7k_2$$

$$b_3 = \frac{1+7k_2}{12}$$

put $k_2 = 5, \quad b_3 = 3$

By chinese remainder theorem,

$$x = \sum_{i=1}^{3} \left(\frac{m}{m_i}\right) a_i b_i \, (\operatorname{mod} m)$$

$$= \left(\frac{m}{m_1} a_1 b_1 + \frac{m}{m_2} a_2 b_2 + \frac{m}{m_3} a_3 b_3\right) (\operatorname{mod} m)$$

$$= \left[(21 \times 1 \times 1) + (28 \times 0 \times 1) + (12 \times 5 \times 3)\right] (\operatorname{mod} 84)$$

$$= (21 + 180) (\operatorname{mod} 84)$$

$$= 201 (\operatorname{mod} 84)$$

3ii) **Determine whether the system**

$x \equiv 3(\operatorname{mod} 10); \quad x \equiv 8(\operatorname{mod} 15); \quad x \equiv 5(\operatorname{mod} 84)$ has a solution and find them all if it exists.

Solution:

The first congruence $x \equiv 3(\operatorname{mod} 10)$ is equivalent to the simultaneous congruences

$x \equiv 3(\operatorname{mod} 2)$ -------(1)

$x \equiv 3(\operatorname{mod} 5)$ --------(2)

The congruence $x \equiv 8(\operatorname{mod} 15)$ is equivalent to,

$x \equiv 8(mod\ 3)$ ------(3)

$x \equiv 8(\operatorname{mod} 5)$ -----(4)

The congruence $x \equiv 5(\operatorname{mod} 84)$ is equivalent to,

$x \equiv 5(mod\ 3)$ ------(5)

$x \equiv 5(\operatorname{mod} 4)$ ------(6)

$x \equiv 5(\operatorname{mod} 7)$ ------(7)

The congruence (1) & (6)

$x \equiv 3(\operatorname{mod} 2)$

$x \equiv 5(\operatorname{mod} 4)$ reduces to $x \equiv 1(\operatorname{mod} 4)$ -----(8)

The congruence (3) & (5)

$x \equiv 8(\operatorname{mod} 3)$

$x \equiv 5(\operatorname{mod} 3)$ reduces to $x \equiv 2(\operatorname{mod} 3)$ -----(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 $a_1=1,\ \ a_2=2,\ \ a_3=3,\ \ a_4=5;\ \ \ m_1=4,\ m_2=3,\ \ m_3=5,\ m_4=7$

$$m=m_1.m_2.\,m_3.m_4=4.3.5.7=420$$

$$\frac{m}{m_1}=105,\ \frac{m}{m_2}=140,\ \frac{m}{m_3}=84,\frac{m}{m_4}=60$$

we know that $\left(\dfrac{m}{m_j}\right)b_j=1(\bmod m_j)$

For $m_1\Rightarrow\left(\dfrac{m}{m_1}\right)b_1\equiv 1(\bmod m_1)$

$$(105)b_1\equiv 1(\bmod 4)\Rightarrow 4/105b_1-1$$

$\Rightarrow$ $105b_1-1=4k_1,\ \ k_1$ is an integer

$$105\mathrm{b}_1=1+4k_1$$

$$b_1=\frac{1+4k_1}{105}$$

put $k_1=26,\ \ b_1=1$

For $m_2\Rightarrow\left(\dfrac{m}{m_2}\right)b_2\equiv 1(\bmod m_2)$

$$(140)b_2\equiv 1(\bmod 3)\Rightarrow 3/140b_2-1$$

$\Rightarrow$ $140b_2-1=3k_2,\ \ k_2$ is an integer

$$140\mathrm{b}_2=1+3k_2$$

$$b_2=\frac{1+3k_2}{140}$$

put $k_2=93,\ \ b_2=2$

For $m_3\Rightarrow\left(\dfrac{m}{m_3}\right)b_3\equiv 1(\bmod m_3)$

$$(84)b_3\equiv 1(\bmod 5)\Rightarrow 5/84b_3-1$$

$\Rightarrow$ $84b_3-1=5k_3,\ \ k_3$ is an integer

$$84\mathrm{b}_3=1+5k_3$$

$$b_3=\frac{1+5k_3}{84}$$

For $m_4 \Rightarrow \left(\dfrac{m}{m_4}\right) b_4 \equiv 1 \pmod{m_4}$

$$(60)b_4 \equiv 1 \pmod 7 \Rightarrow 7/60b_4 - 1$$

$\Rightarrow \quad 60b_4 - 1 = 7k_4, \quad k_4$ is an integer

$$84\text{b}_4 = 1 + 7k_4$$

$$b_4 = \frac{1+7k_4}{84}$$

put $k_4 = 17, \quad b_3 = 2$

By chinese remainder theorem,

$$x = \sum_{i=1}^{4} \left(\frac{m}{m_i}\right) a_i b_i \pmod m$$

$$= \left(\frac{m}{m_1} a_1 b_1 + \frac{m}{m_2} a_2 b_2 + \frac{m}{m_3} a_3 b_3 + \frac{m}{m_4} a_4 b_4\right) \pmod m$$

$$= \left[(105 \times 1 \times 1) + (140 \times 2 \times 2) + (84 \times 3 \times 4) + (60 \times 5 \times 2)\right] \pmod{420}$$

$$= (105 + 560 + 1008 + 600) \pmod{420}$$

$$= 2273 \pmod{420} = 173 \pmod{420}$$

4i) Prove that $4^{2n} + 10n \equiv 1 \pmod{25}$.

Proof :

$4^{2n} + 10n \equiv 1 \pmod{25}$

proof by mathematical induction

$\Rightarrow n = 0$

$(4^0 + 0) - 1 = 1 - 1 = 0$

$\Rightarrow 0$ is divisible by 25

statement is true for $n = 0$.

$n = 1, \quad (4^2 + 10) - 1 = 25$

$\Rightarrow$ 25 is divisible by 25

statement is true for $n = 1$.

Assume that the statement is true for $n = k$

$(ie), 4^{2k} + 10k - 1 = 25l$

Consider $\quad 4^{2k+2} + 10(k+1) - 1$

$$= 4^{2k}.16 + 10k + 10 - 1$$

$$= 16(25l - 10k + 1) + 10k + 9$$

$$= 16(25l) - 160k + 16 + 10k + 9$$

$$= 16(25l) - 150k + 25$$

$$= 25(16l - 6k + 1)$$

$$= 25(y)$$

$4^{2k+2} + 10(k+1) - 1$ is divisible by 25

Statement is true for $n = k + 1$

By principle of mathematical induction, statement is true for all *n*.

4ii) **Find the remainder when $(n^2+n+41)^2$ is divisible by 12.**

Solution:

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

$(ie), (n-1)n(n+1)(n+2) \equiv 0 \pmod{12}$

$$\begin{aligned}(n^2+n+41)^2 &\equiv (n^2+n+5)^2 \pmod{12}\\ &\equiv (n^4+2n^3+11n^2+10n+25) \pmod{12}\\ &\equiv n(n^3+2n^2-n-2)+1 \pmod{12}\\ &\equiv n\left[n^2(n+2)-(n+2)\right]+1 \pmod{12}\\ &\equiv n((n+2)(n^2-1)+1 \pmod{12}\\ &\equiv (n-1)n(n+1)(n+2)+1 \pmod{12}\\ &\equiv 1 \pmod{12}\end{aligned}$$

Thus when $(n^2+n+41)^2$ is divided by 12, the remainder is 1.

5i) **Find the general solution of the LDE $6x+8y+12z=10$** **[NOV/DEC 20]**

Solution:

Given the LDE is $6x+8y+12z=10$ ------(1)

Here $a_1=6,\ a_2=8,\ a_3=12,\ c=10$

$\therefore\ (a_1.a_2,a_3)=(6,8,12)=2$ and $c=10$

$\therefore\quad d=(a_1.a_2,a_3)=2$

Since $2\,|\,10,\ d\,|\,c$

So, the given LDE is solvable.

Since $8y+12z$ is a linear combination of 8 and 12, *it* must be a multiple of $(8,12)=4$

$\therefore\quad 8y+12z=4u$ --------(2)

$\therefore (1) \Rightarrow\quad 6x+4u=10$ --------(3)

First we solve the LDE (3) in two variables x and u

Here $a=6, b=4,\ c=10$

$(a,b)=(6,4)=2$

$d=(a,b)=2$ and $c=10$

Since $2\,|\,10,\ d\,|\,c$

So, the given LDE (3) is solvable.

We find $x_0=1,\ u_0=1$ is a solution of (3) is

$x=x_0+\frac{b}{d}t$ *and* $u=u_0-\frac{a}{d}t,\quad t\in Z$

$x=1+\frac{4}{2}t$ *and* $u=1-\frac{6}{2}t,\quad t\in Z$

$x=1+2t$ *and* $u=1-3t,\quad t\in Z$

Substituting for u in (2), we get

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

Since d=$\begin{pmatrix} a & b \\ 8, & 12\end{pmatrix}=4$ and $4=2.8+(-1).12$ is a linear combination of 8 and 12.

Multiplying by $(1-3t)$, *we get*

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

$\therefore$ a solution of (2) is

$y_0 = 2-6t$ and $z_0 = -1+3t, \quad t \in Z$

So, the general solution of (2) is

$$y = y_0 + \frac{b}{d}t' \quad and \quad z = z_0 - \frac{a}{d}t', \quad t' \in Z$$

$$y = 2-6t+\frac{12}{4}t' \quad and \quad z = -1+3t-\frac{8}{4}t', \quad t' \in Z$$

$$y = 2-6t+3t' \quad and \quad z = -1+3t-2t', \quad t' \in Z$$

Thus the general solution of (1) is

$$x = 1+2t, \; y = 2-6t+3t', \; z = -1+3t-2t', \quad t' \in Z$$

5ii) **Find the general solution of the LDE** $15x+21y=39$ **[NOV/DEC 19]**

Solution:

$15x+21y=39 \Rightarrow a=15,\ b=21,\ c=39.$

$d=(15,21)$ and $d/39 \Rightarrow d=3$

So, the given LDE is solvable.

$15x+21y=39 \Rightarrow 5x+7y=13 --------(1)$

then $(5,7)=d=1 \quad \therefore d/13$

$a=5, b=7, d=1$

We find $x_0=-3,\ y_0=4$ is a solution of (1) is

$$x = x_0+\frac{b}{d}t \quad and \quad y = y_0 - \frac{a}{d}t, \quad t \in Z$$

$$x = -3+\frac{7}{1}t \quad and \quad y = 4-\frac{5}{1}t, \quad t \in Z$$

$$x = -3+7t \quad and \quad y = 4-5t, \quad t \in Z$$

6i) **Solve the linear system** $5x+6y \equiv 10(\text{mod}13);\ 6x-7y \equiv 2(\text{mod}13).$ **[NOV/DEC 19]**

Solution:

$5x+6y \equiv 10(\text{mod}13)$

$6x-7y \equiv 2(\text{mod}13)$

$\Rightarrow \text{a}=5, \text{b}=6, \text{c}=6, \text{d}=-7, \text{e}=10, \text{f}=2.$

$m=13,\ \Delta = ad-bc = -35-36 = -71(\text{mod}13) = 7(\text{mod}13)$

$(\Delta, m) = (13,1) = 1.$

Hence unique solution.

$$x_0 = \Delta^{-1}\begin{vmatrix} 10 & 6 \\ 2 & -7 \end{vmatrix}(\text{mod}13) -------(1)$$

$$y_0 = \Delta^{-1}\begin{vmatrix} 5 & 10 \\ 6 & 2 \end{vmatrix}(\text{mod}13) --------(2)$$

$\Delta\Delta^{-1} \equiv 1(\text{mod}13)$

$7\Delta^{-1} \equiv 1(\text{mod}13)$

$\Rightarrow \Delta^{-1} \equiv 2(\text{mod}13)$

$$\begin{aligned}(1) \Rightarrow x_0 \equiv \Delta^{-1}(-70-12)(\text{mod}13) &\equiv 2(-70-12)(\text{mod}13)\\ &\equiv -8(\text{mod}13)\\ &\equiv 5(\text{mod}13)\end{aligned}$$

$(2) \Rightarrow y_0 \equiv \Delta^{-1}(10-60)(\bmod 13) \equiv 2(-50)(\bmod 13)$

$\equiv 2.2\,(\bmod 13)$

$\equiv 4\,(\bmod 13)$

$\therefore x \equiv 5(\bmod 13); \quad y \equiv 4(\bmod 13).$

6ii) Compute the remainder when 3^{247} is divisible by 25.

Solution:

We have to find the remainder when 3^{247} is divisible by 25.

$$\begin{aligned}
\text{We have } 3^2 &\equiv 9\,(\bmod 25)\\
3^4 &\equiv 9^2 = 81 \equiv 6\,(\bmod 25)\\
3^8 &\equiv 6^2 = 36 \equiv 11\,(\bmod 25)\\
3^{16} &\equiv 11^2 = 121 \equiv 21\,(\bmod 25)\\
3^{32} &\equiv 21^2 \equiv 16\,(\bmod 25)\\
3^{64} &\equiv 16^2 \equiv 6\,(\bmod 25)\\
3^{128} &\equiv 6^2 \equiv 11\,(\bmod 25)\\
3^{247} &= 3^{128+64+32+16+4+2+1}\\
&= 3^{128}.3^{64}.3^{32}.3^{16}.3^{4}.3^{2}.3\\
3^{247} &\equiv 11.6.16.21.6.9.3\,(\bmod 25)\\
&\equiv 11\,(96)\,(21)\,(54)\,3\,(\bmod 25)\\
&\equiv 11\,(-4)\,(-4)\,(4)\,3\,(\bmod 25)\\
&\equiv 44.48\,(\bmod 25)\\
&\equiv (-6)\,(-2)\,(\bmod 25)\\
&\equiv 12\,(\bmod 25)
\end{aligned}$$

$\therefore$ the remainder is 12 when 3^{247} is divisible by 25.

UNIT – V CLASSICAL THEOREMS AND MULTIPLICATIVE FUNCTIONS

PART A

1 State Wilson's Theorem. **[NOV/DEC 20]**

If p is prime , then $(\mathbf{p}-\mathbf{1})! \equiv -\mathbf{1}(\bmod\,\mathbf{p})$

2 Find the remainder when 100! is divided by 101.

We know that, By Wilson theorem "If p is prime , then $(\mathbf{p}-\mathbf{1})! \equiv -\mathbf{1}(\bmod\,\mathbf{p})$"

p = 101 is a prime, by Wilson's theorem, (101-1)!≡ -1 (mod 101).
Therefore, Reminder when 100! Is divided by 101 is 101-1=100

3 What is the remainder when 100! is divided by $(97)^2$?

100! Mod 97^2 = 97*(100*99*98*96! Mod 97)
97 is prime. So, 96!(mod 97) = 96
⇒ 100*99*98*96!(mod 97) = 3*2*1*96(mod 97)
= 3*2*1*(-1) (mod 97)
= -6 (mod 97)
= 91 (mod 97)
So, required remainder = 91*97
= 8827

4 State Fermat's Little Theorem. **[NOV/DEC 19]**

Let p be a prime and 'a' any integer such that $\mathbf{p} \nmid \mathbf{a}$, then $\mathbf{a}^{\mathbf{p}-\mathbf{1}} \equiv \mathbf{1}(\bmod\,\mathbf{p})$

5 Using Fermat's theorem, find the last digit of 3^{100} when divided by 10.

We know that $3^2 = 9 \equiv -1 \pmod{10}$

$$3^{(2n)} \equiv (-1)^n \pmod{10}$$

$$3^{(2\times 50)} \equiv (-1)^{50} \pmod{10}$$

Therefore last digit = 1

6 What is the remainder when 109 divides 17^{325}?

By Fermat's theorem,

remainder when 109 divides $17^{(109-1)}$ is 1 as109 is prime & 109 does not divide 17.

Remainder when 109 divides $17^{3(109-1)}$ is 1

remainder when 109 divides $[17^{3(108)}]$x17 is 1 x17

remainder when 109 divides $17^{(324+1)}$ is 17

7 Define Multiplicative function

A number-theoretic function f is multiplicative if f(mn) = f(m) f(n) whenever m and n are relatively prime.

8 State Fundamental theorem for multiplicative function

Let f be a multiplicative function and n a positive integer with canonical decompositions

$n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$ then $f(n) = f(p_1^{e_1}) f(p_2^{e_2}) \ldots f(p_k^{e_k})$

9 Define Euler phi function or totient function or Indicator function.

Euler phi function represent as $\phi(n)$ gives for a number 'n' the number of co-primes in the [1,2,…,n] , in other words, the quantity number in the range [1,2,…,n] whose greatest common divisor with n is the unity.

10 Find all positive integers n such that ϕ(n)=6.

We know that $\phi(7)=6$, $\phi(3^2)=6$, and $\phi(2)=1$ and ϕ is multiplicative

Therefore, the numbers should be 7, 7·2=14, 3^2=9, and 3^2·2=18

11 Find $\phi(221)$

$$\phi(221) = \phi(13.17) = \phi(13).\phi(17) \quad [\because \text{the function } \phi \text{ is multiplicative}]$$

$$= 12.\ 16 \quad [\because \text{A positive integer } p \text{ is prime iff } \phi(p) = p-1]$$

$$= 192$$

12 Find $\phi(8)$, $\phi(81)$ and $\phi(15625)$

We know that $\phi(p^e) = p^e - p^{e-1}$, p be prime and e be any positive int eger

$$\phi(8) = \phi(2^3) = 2^3 - 2^2 = 8 - 4 = 4$$

$$\phi(81) = \phi(3^4) = 3^4 - 3^3 = 81 - 27 = 54$$

$$\phi(15625) = \phi(5^6) = 5^6 - 5^5 = 12500$$

13 *If $n = 2^k$*, then show that the value of Euler's phi function $\phi(n) = \frac{n}{2}$ [NOV/DEC 19]

We know that $\phi(p^e) = p^e - p^{e-1}$, p be prime and e be any positive int eger

Given $n = 2^k$

$$\phi(n) = \phi(2^k)$$

$$= 2^k - 2^{k-1}$$

$$= 2^k \left\{1 - \frac{1}{2}\right\} = \frac{2^k}{2} = \frac{n}{2}$$

14	**State Euler's Theorem.**
	Let m be a positive integer and a be any integer with (a, m)=1 then $\mathbf{a^{\phi(m)} \equiv 1(\text{mod}\, m)}$
15	**Verify that** $\displaystyle\sum_{d/18} \phi(d) = 18$
	The positive divisors of 18 are 1,2,3,6,9,18 $\displaystyle\sum_{d/18} \phi(d) = \phi(1)+\phi(2)+\phi(3)+\phi(6)+\phi(9)+\phi(18)$ = 1+1+2+2+6+6=18
16	**Define Tau function**
	Let n be a positive integer then $\tau(n)$ denotes the number of positive factors of n that is $\tau(n) = \displaystyle\sum_{d/n} 1$
17	**Define sigma function.**
	Let n be a positive integer then $\boldsymbol{\sigma(n)}$ denotes the sum of the positive factors of n that is $\boldsymbol{\sigma(n) = \displaystyle\sum_{d/n} d}$
18	**Evaluate $\tau(18)$ and $\tau(23)$**
	The positive divisors of 18 are 1,2,3,6,9,18 so that $\boldsymbol{\tau(18) = 6}$ 23 being a prime , has exactly two positive divisors so $\boldsymbol{\tau(23) = 2}$
19	**Evaluate $\sigma(12)$ and $\sigma(28)$**
	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 $\sigma(28) = 1+2+4+7+14+28 = 56$
20	**Find the number of divisors and the sum of the divisors of 600.**
	Decomposition of 600 in canonical form $600 = 2^3 \times 3 \times 5^2$ where $p_1 = 2, p_2 = 3, p_3 = 5,\ \alpha_1 = 3, \alpha_2 = 1, \alpha_3 = 2$ If decomposition of N by canonical form = $p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3}$..... $\text{Number of divisor} = (\alpha_1 + 1)(\alpha_2 + 1)(\alpha_3 + 1).....(\alpha_n + 1)$ $= (3+1)(1+1)(2+1) = 24$ $\text{Sum of divisor} = \left(\dfrac{p_1^{\alpha_1+1} - 1}{p_1 - 1}\right)\left(\dfrac{p_2^{\alpha_2+1} - 1}{p_2 - 1}\right)..... = \left(\dfrac{2^4 - 1}{2 - 1}\right)\left(\dfrac{3^2 - 1}{3 - 1}\right)\left(\dfrac{5^3 - 1}{5 - 1}\right) = 1860$
	PART-B
1i)	**State and prove Wilson's Theorem** **[NOV/DEC 19]**
	Statement: If p is prime, then (p – 1)! ≡ –1 (mod p). **Proof :** We have to prove *(p* – 1)! ≡ –1 (mod *p)* When *p* = 2, (*p*– 1)! = (2– 1)! = 1 ≡–l (mod 2). So, the theorem is true when *p = 2.* Now let *p > 2* and let *a* be a positive integer such that 1 ≤ *a* ≤ *p* – 1. Since *p* is a prime and *a* < *p*, (*a*, *p*) = 1. Then the congruence *ax* ≡ 1 (mod *p*) has a solution *a'* congruence modulo *p*. ∴ *aa'* ≡ l(mod *p*), where 1 ≤ *a'* <*p* – 1 ∴ *a, a'* are inverses of each other modulo p. If *a'* = *a,* then *a .a* ≡ 1 (mod *p*) ⇒ a^2 – 1 ≡ 0·(mod *p*) ∴ .*p* | $a^2 - l$ ⇒ *p* | (*a* – 1) (*a*+ 1)

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

Since $a < p$, *if* $p \mid a + 1$ then $a = p - 1$.

If $p \mid a - 1$, then $a - 1 = 0 \Rightarrow a = 1\cdot$

$\Rightarrow a = 1$ or p-1 if $a = a'$

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

If $a' \neq a$, excluding 1 and $p - 1$, the remaining $p - 3$ residues 2, 3, 4, …, $(p - 3)$, $(p - 2)$ can be grouped into $\frac{p-3}{2}$ pairs of the type a, a' such that $aa' \equiv 1 \pmod p$

Multiplying all these pairs together we get, $2\cdot3\cdot4 \ldots (p-3)(p-2) \equiv 1 \pmod p$

$\Rightarrow 1.2 \cdot 3 \cdot 4 \ldots (p-2)(p-1) \equiv p - 1 \bmod p$

$(p-1)! \equiv -1 \pmod p$ (Since $p - 1 \equiv -1 \pmod p$)

Hence the theorem.

This can be rewritten as $(p - 1)! + 1 \equiv 0 \pmod p$

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

which is the result suggested by Wilson.

1ii) **Let p be a prime and n any positive integer. Prove that $\frac{(np)!}{n!p^n} \equiv (-1)^n \pmod p$**

Proof:

First, we can make an observation. Let a be any positive integer congruent to 1 modulo p. Then by Wilson's theorem , $a(a+1)\ldots(a+(p-2)) \equiv (p-1)! \equiv -1 \pmod p$

In other words, the product of the p-1 integers between any two consecutive multiples of p is congruent to -1 mod p.

Then $\frac{(np)!}{n!p^n} = \frac{(np)!}{p.2p.3p\ldots(np)}$

$$= \prod_{r=1}^{n} \left[(r-1)p+1\right]\ldots\left[(r-1)p+(p-1)\right]$$

$$\equiv \prod_{r=1}^{n} (p-1)! \pmod p$$

$$\equiv \prod_{r=1}^{n} (-1) \pmod p$$

$$\equiv (-1)^n \pmod p$$

2i) **State and prove Fermat's little theorem. [NOV/DEC 20]**

Statement:

If p is a prime and *a* is any integer not divisible by p, then $a^{p-1} \equiv 1 \pmod p$

Proof:

Given p is a prime and *a* is any integer not divisible by p

When an integer is divided by p, the set of possible remainders are 0, 1, 2, 3, ...,$p - 1$

Consider the set of integers $1\cdot a, 2\cdot a, 3\cdot a, \ldots, (p-1)\cdot a$ --------------(1)

Suppose $ia \equiv 0 \pmod p$, then $p \,/\, ia$.

But $p \nmid a$ $\therefore$ $p \,/\, i$, which is impossible, since $i < p$.

$Ia \not\equiv 0 \pmod p$ *for* $i = 1, 2, \ldots, p - 1$.

So, no term of (1) is zero.

Next we prove they are all distinct

Suppose $ia \equiv ja \pmod p$, where $1 \le i,j \le p-1$.

Then $(i - j)a \equiv 0 \pmod p \Rightarrow p \,/\, (i - j)\, a$

Since $p \nmid a$, $p \,/ i{-}j$ *and* $i, j < p \Rightarrow /i - j/ < p$.

$\therefore\ i - j = 0 \Rightarrow i \equiv j(mod\ p)$

$\therefore\quad i \neq j \Rightarrow ia \neq ja.$

This means, no two of the integers in (1) are congruent modulo p.

$\therefore$ The least residues (or remainders) of the integers $a, 2a, 3a, ...,(p-l)a$ modulo p are the same as the integers $1, 2, 3, ...,p-1$ in some order.

So, their products are congruent modulo p.

$$A\ .\ 2\ a \cdot 3\ a\ ...\ (p-l)\ a \equiv 1 \cdot 2 \cdot 3\ ...\ (p-1)\ (mod\ p)$$

$\Rightarrow\quad l \cdot 2 \cdot 3 ... (p-l) \cdot a^{p-1} \equiv (p-l)!(mod\ p)$

$\Rightarrow\quad (p-l)!\ a^{p-1} \equiv (p\text{-}l)!(mod\ p)$

$\Rightarrow\quad a^{p-1} \equiv l(mod\ p)$ (since $p \nmid (p\text{-}l)$)

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

2ii) Find the remainder when 24^{1947} is divided by 17

Solution.

We have to find the remainder when 24^{1947} is divided by 17.

Here $a = 24$, $p = 17$

We know 17 is a prime & $17 \nmid 24$

$\therefore$ By Fermat's theorem, $24^{17-1} \equiv 1(mod\ 17)$

$\Rightarrow\quad 24^{16} \equiv 1(mod\ 17)$

$\therefore\quad (24^{16})^{121} \equiv 1^{121}(mod\ 17)$

$\Rightarrow\quad 24^{1936} \equiv 1(mod\ 17)$

Now $\quad 24^{1947} = 24^{1936+11} = 24^{1936}\ .24^{11}$

$24^{2} = 576 \equiv -2(mod\ 17)$

$\therefore\quad (24^{2})^{2} \equiv (-2)^{2}(mod\ 17)$

$\Rightarrow\quad 24^{4} \equiv 4(mod\ 17)$

$(24^{4})^{2} \equiv 4^{2}(mod\ 17)$

$\Rightarrow\quad 24^{8} \equiv 16(mod\ 17)$

$\equiv -l(mod\ 17)$

$24^{11} = 24^{8}.24^{2}.24 \equiv (-l)(-2).\ 7(mod\ 17)$

$\equiv 14(mod\ 17)$

$\therefore\quad 24^{1947} \equiv 14(mod\ 17)$

$\equiv 14(mod\ 17)$

$\therefore$ the remainder is 14 when 24^{1947} is divided by 17.

3i) State and prove Euler's theorem.

Statement:

Let m be a positive integer and a be any integer such that $(a, m) = 1$. Then $a^{\Phi(m)} \equiv 1(mod\ m)$.

Proof :

Given m is a positive integer and a is any integer such that $(a, m) = 1$.

Let $r_1, r_2, ...,r_{\Phi(m)}$ be all the positive integers $< m$ and relatively prime to m.

Since $r_i - r_j < m$, clearly $r_i \neq r_j$ (mod m) if $i \neq j$

Consider the products $ar_1, ar_2, ...,ar_{\Phi(m)}$

Since $(a, m) = 1, ar_i \neq ar_j\ (mod\ m)\ if\ i \neq j$

we find $ar_1, ar_2, ...,ar_{\Phi(m)}$ $mod\ m$ are distinct.

We now prove $(ar_i, m) = 1$

For, suppose $(ar_i, m) > 1$, then let p be a prime factor of $(ar_i, m) = d$.

$\therefore\quad p\ /\ ar_i$ and $p\ /m$

$\Rightarrow\quad p\ /\ a$ or $p\ /\ r_i$ and $p\ /m.$

If $p\ /\ r_i$ and $p\ /\ m$ then, $(r_i,m) \neq 1$, a contradiction.

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

$\therefore\quad (ar_i\cdot,m) = l,\ \ i = 1,2,3, ...,\Phi(m)$

$\therefore$ $\Phi(m)$ least residues $ar_1, ar_2, \ldots, ar_{\Phi(m)}$ modulo m are distinct and relatively prime to m. So, they are the same as integers $r_1, r_2, \ldots, r_{\Phi(m)}$, in some order modulo m.

$$\therefore \text{ their product } ar_1 \cdot ar_2 \cdot \ldots \cdot ar_{\Phi(m)} \equiv r_1 \cdot r_2 \cdot \ldots \cdot r_{\Phi(m)} \pmod m$$

$$\Rightarrow \quad a^{\Phi(m)}\, r_1 \,.\, r_2,, r_{\Phi(m)} \equiv r_1 r_2 .. r_{\Phi(m)} \pmod m$$

Since each r_i is relatively prime to m, $(r_1 r_2 .. r_{\Phi(m)}, m) = 1$

We get $a^{\Phi(m)} \equiv 1 (mod\ m)$

3ii) Using Euler's theorem, find the remainder when 245^{1040} is divided by 18. [NOV/DEC 19]

Solution.

We have to find the remainder when 245^{1040} is divided by 18.

Here $a = 245 = 5 \cdot 72$ and $m = 18 = 32 \cdot 2$, $(a, m) = 1$

Hence by Euler's theorem, $a^{\varphi(m)} \equiv 1 (mod\ m)$

$$\Rightarrow 245^{\varphi(m)} \equiv 1 (mod\ m)$$

$$\varphi(18) = \varphi(3^2 . 2)$$

$$= \varphi(3^2).\varphi(2)$$

$$= 3^2\left(1 - \frac{1}{3}\right).1 = 6$$

$$\therefore\ 245^6 \equiv 1 (mod 18)$$

$$\therefore\ (245^6)^{173} \equiv 1^{173} (mod 18)$$

$$245^{1038} \equiv 1 (mod 18)$$

$$245^{1040} = 245^{1038+2}$$

$$= 245^{1038} 245^2$$

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

$$245^2 \equiv 11^2 \text{ (mod 18)}$$

$$\equiv 121 \text{ (mod 18)}$$

$$\equiv 13 \text{ (mod 18)}$$

$$245^{1040} \equiv 1 \cdot 13 \text{ (mod 18)}$$

$$\equiv 13 \text{ (mod 18)}$$

$\therefore$ the remainder is 13 when 245^{1040} is divided by 18.

4i) If $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$ is the canonical decomposition of a positive integer n then derive the formula for the phi function $\varphi(n)$ and use it to find $\varphi(6860)$ & $\varphi(6125)$

[NOV/DEC 19, 20]

Proof:

To prove :

If p is prime and e any positive integer then $\varphi(p^e) = p^e - p^{e-1} = p^e(1 - \frac{1}{p})$

$\varphi(p^e) =$ number of positive integers $\leq p^e$ and relatively prime to it

$=$ {number of positive integers $\leq p^e$ }-{ number of positive integers $\leq p^e$ and not relatively prime to it}

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

The number of positive integers $\leq p^e$ and not prime to it are the various multiples of p.

They are $p, 2p, 3p, \ldots.., (p^{e-1})p$

The number of such numbers $= p^{e-1}$

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

	Since $\varphi(p^e)=p^e-p^{e-1}=p^e(1-\frac{1}{p})$ is a multiplicative function, $\varphi(n)=\varphi(p_1^e p_2^e ... p_k^e)=\varphi(p_1^e)\varphi(p_2^e)...\varphi(p_k^e)$ $=p_1^e(1-\frac{1}{p_1})p_2^e(1-\frac{1}{p_2})...p_k^e(1-\frac{1}{p_k})$ $=p_1^e p_2^e ... p_k^e(1-\frac{1}{p_1})(1-\frac{1}{p_2})...(1-\frac{1}{p_k})$ $=n(1-\frac{1}{p_1})(1-\frac{1}{p_2})...(1-\frac{1}{p_k})$ To find $\varphi(6860)$: $\varphi(6860)=\varphi(2^2).\varphi(5).\varphi(7^3)$ $=2^2\left(1-\frac{1}{2}\right)4.7^3\left(1-\frac{1}{7}\right)=252$ To find $\varphi(6125)$: $\varphi(6125)=\varphi(5^3).\varphi(7^2)$ $=5^3\left(1-\frac{1}{5}\right).7^2\left(1-\frac{1}{7}\right)=4200$
4ii)	**Prove that τ and σ are multiplicative functions.**
	Proof: We know that $F(n)=\sum_{d/n} f(d)$ is multiplicative if *f* is multiplicative. **(i) To prove τ is multiplicative** If *f*(d) = $d^0=1$, is constant for each *d/n* If d_1, d_2 are two divisors (d_1,d_2) = 1, then $f(d_1d_2)=1$, $f(d_1)=1$; $f(d_2)=1$ $\therefore f(d_1d_2)=f(d_1)f(d_2)$ So, constant function is multiplicative. Then $F(n)=\sum_{d/n} 1=\tau(n)$ If (m,n)=1, then F(mn) = F(m) F(n) $\Rightarrow \tau(mn)=\tau(m)\tau(n)$ So τ is multiplicative. **(ii) To prove σ is multiplicative** Take *f*(d)=d, identity function If d_1, d_2 are two divisors and $(d_1,d_2)=1$, then $f(d_1d_2)=d_1d_2$ $=f(d_1)f(d_2)$ $\therefore$ *f* is multiplicative Hence $F(n)=\sum_{d/n} d=\sigma(n)$ For (m,n)=1 , F(mn)=F(m) F(n) Then $\sigma(mn)=\sigma(m)\sigma(n)$ So σ is multiplicative. $\therefore$ τ and σ are multiplicative functions.
5	**Define Euler phi function and prove that it is multiplicative.**
	Solution: **Euler phi function:** Let $\varphi: N \rightarrow N$ be a function defined by $\varphi(1)$= 1 and for n>1 φ(n)=the number of positive integer $\leq$ n and relative prime to n.

To prove that it is multiplicative:

Let m and n be positive integers such that $(m, n) = 1$.

To prove φ(mn) = φ(m) φ(n)

Arrange the *mn* integers 1, 2, 3, ..., *mn* in m rows of *n* numbers each.

$$\begin{array}{lcccccc}
 & 1 & m+1 & 2m+1 & 3m+1 & \ldots & (n-1)m+1 \\
 & 2 & m+2 & 2m+2 & 3m+2 & \ldots & (n-1)m+2 \\
 & 3 & m+3 & 2m+3 & 3m+3 & \ldots & (n-1)m+3 \\
 & : & : & : & : & : & : \\
 & : & : & : & : & : & : \\
r^{th}\text{ row} & r & m+r & 2m+r & 3m+r & \ldots & (n-1)m+r \\
 & : & : & : & : & : & : \\
 & : & : & : & : & : & : \\
 & m & 2m & 3m & 4m & \ldots & nm
\end{array}$$

Let r be a positive integer $\leq m$ such that $(r, m) > 1$.

We will now show that no element of the r^{th} row in the array is relatively prime to mn.

Let $d = (r, m)$. Then $d \,/\, r$ and $d \,/\, m \Rightarrow d \,/ km + r$ for any integer k

This means d is a factor of every element in the r^{th} row.

Thus, no element in the r^{th} row is relatively prime to m and hence to mn if $(r, m) > 1$.

In other words,

the elements in the array relatively prime to mn come from the r^{th} row only if $(r, m) = 1$.

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 r^{th} row where $(r, m) = 1$.

The elements in the r^{th} row are r, $m + r$, $2m + r$, ..., $(n-1)m + r$.

When they are divided by n, the remainders are $0, 1, 2, \ldots, n - 1$ in some order of which $\varphi(n)$ are relatively prime to n.

Therefore, exactly $\varphi(n)$ elements in the r^{th} row are relatively prime to n and hence to mn.

Thus there are $\varphi(m)$ rows containing positive integers relatively prime to mn and each row contain $\varphi(n)$ elements relatively prime to it.

Hence the array contains $\varphi(m)\ \varphi(n)$ positive integers $\leq mn$ and relatively prime to mn.

That is $\varphi(mn) = \varphi(m)\ \varphi(n)$.

Hence φ is multiplicative function.

6i) **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:

$\varphi(p^e) =$ number of positive integers $\leq p^e$ and relatively prime to it

$=$ {number of positive integers $\leq p^e$ **}-{** number of positive integers $\leq p^e$ and not relatively prime to it}

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

The number of positive integers $\leq p^e$ and not prime to it are the various multiples of p.

They are $p, 2p, 3p, \ldots\ldots, (p^{e-1})p$

The number of such numbers $= p^{e-1}$

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

To prove that $\boldsymbol{\varphi(n)=\frac{n}{2}}$ **when** $\boldsymbol{n=2^{k}}$

Given $n=2^{k}$

$$\therefore \varphi(n)=\varphi(2^{k})=2^{k}\left(1-\frac{1}{2}\right)$$

$$=2^{k}.\frac{1}{2}=\frac{n}{2}$$

6ii) **Find the primes p for which** $\boldsymbol{\frac{2^{p-1}-1}{p}}$ **is a square.**

Solution:

Suppose $\frac{2^{p-1}-1}{p}=n^{2}$ for some positive integer n. Then $2^{p-1}-1=p\,n^{2}$

Clearly both p and n must be odd.

Let p=2k+1 for some positive integer k.

Then $2^{2k}-1=p\,n^{2} \quad\Rightarrow\quad (2^{k}-1)(2^{k}+1)=pn^{2}$

Suppose $(2^{k}-1)$ is a perfect square, $(2^{k}-1)=r^{2} \;\Rightarrow\; 2^{k}=r^{2}+1$

$$2^{p-1}=2^{2k}=(2^{k})^{2}=\left(r^{2}+1\right)^{2}$$

Since $r\geq 1$ and is odd, $r = 2i + 1$ for some integer $i \geq 0$.

Then $r^{2} = (2i + 1)^{2}$ has to be an odd number.

But $r^{2} + 1= 2^{k} \Rightarrow r^{2} + 1$ has to divide 2.

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

$\Rightarrow r = 0 \text{ or } 1$

$r=0,\;\; 2^{p-1}=(0^{2}+1)^{2}=1 \Rightarrow$ p=0 which is not possible

$r=1,\;\; 2^{p-1}=(1^{2}+1)^{2}=4 \Rightarrow$ p=3

Suppose $(2^{k}+1)$ is a perfect square

$$(2^{k}+1)=s^{2} \;\Rightarrow\; 2^{k}=s^{2}-1$$

$$2^{p-1}=\left(s+1\right)^{2}\left(s-1\right)^{2}$$

Then both s -1 and s+1 both must be the factors of 2

$$s-1=1 \;or\; 2, \quad \& \quad s+1=1 \;or\; 2 \;\Rightarrow s=0,\ 1,\ 2 \;or\; 3$$

$If\;\; s=0;\; 2^{p-1}=\left(0+1\right)^{2}\left(0-1\right)^{2}=1 \Rightarrow p=1$ which is not possible

$If\;\; s=1;\; 2^{p-1}=\left(1+1\right)^{2}\left(1-1\right)^{2}=0$ which is not possible

$If\;\; s=2;\; 2^{p-1}=\left(2+1\right)^{2}\left(2-1\right)^{2}=9$ which is not possible

$If\;\; s=3;\; 2^{p-1}=\left(3+1\right)^{2}\left(3-1\right)^{2}=2^{6} \Rightarrow p=7$. Thus p must be 3 or 7