UNIT I
GROUPS AND RINGS
PART-A

1. State any two properties of a group.

Closure property: a*b ∈ G, for all a,b ∈ G

Associative property: (a*b)*c=a*(b*c), for all a,b,c ∈ G

2. Define Homomorphism of groups.

Let (G,*) and (G,o) be two groups and f be a function from G into G1. Then f is called a ***homomorphism*** of G into G1 if for all a,b ∈ G,

f(a*b) = f(a) o f(b).

3. Give an example of Homomorphism of groups.

Consider the group (Z,+). Define f:Z →Z by f(n) = 3n for all n∈ Z

Here the function f is from the group (Z,+) to (Z,+)

Let n,m ∈ Z then we get n+m ∈ Z and we have f(n+m) = 3(n+m) = 3n + 3m = f(n) + f(m)

Hence the function f is a homomorphism.

4. Define Isomorphism.

Let (G,*) and (G',o) be two groups and f : G → G' be a homomorphism of groups then f is called a isomorphism if f is a bijective(one-to-one and onto) function.

5. Give any two Example of Isomorphism.

Example:1

Consider the function f: Z → Z by f(x) = x, Now we have to show that f is a homomorphism.

Take any two elements x, y belongs to Z ,Then x + y belongs to Z, Hence f(x+y) = x + y = f(x) + f(y)

Hence f is homomorphism.

Since the function f(x) = x is bijective. f is an isomorphism.

Example :2

Consider the function f: Z → Z by f(x) = x. Take any two elements x,y belongs to Z ,Then x + y belongs to Z, Hence f(x+y) = x + y = f(x) + f(y) Hence f is homomorphism.

Since the function f(x) = x is bijective. f is an isomorphism.

6. Show that ($Z_5,+_5$) is a cyclic group.

$+_5$	[0]	[1]	[2]	[3]	[4]
[0]	0	1	2	3	4
[1]	1	2	3	4	0
[2]	2	3	4	0	1
[3]	3	4	0	1	2
[4]	4	0	1	2	3

$1^1 = 1$

$1^2 = 1 +_5 1 = 2$

$1^3 = 1 +_5 1^2 = 1 +_5 2 = 3$

$1^4 = 1 +_5 1^3 = 1 +_5 3 = 4$

$1^5 = 1 +_5 1^4 = 1 +_5 4 = 0$

Hence ($Z_5,+_5$) is a cyclic group and 1 is a generator.

7. Prove that the group $H = (Z_4,+)$ is cyclic.

Here the operation is addition, so we have multiplies instead of powers. We find that both [1] and [3] generate *H*. For the case of [3], we have

1.[3]=[3], 2.[3]=[2], 3.[3]=[1], and 4.[3]=[0].

Hence *H*=<[3]>=<[1]>.Hence $H = (Z_4,+)$ is cyclic

8. Prove that $U_9 = \{1,2,4,5,7,8\}$ is cyclic group.

Here we find that 2^1=2, 2^2=4, 2^3=8, 2^4=7, 2^5=5,2^6=1,

So U_9 is a cyclic group of order 6 and $U_9 = \langle 2 \rangle$ and also true that $U_9 = \langle 5 \rangle$

because 5^1=5, 5^2=7, 5^3=8, 5^4=4, 5^5=2, 5^6=1.

9. Define Left coset and Right coset of the group.

If H is a subgroup of G,then for each $a \in G$,the set $aH = \{ah / h \in H\}$is called a l eft coset of H in G and $Ha = \{ha / h \in H\}$is a right coset of H in G.

10. Consider the group Z_4= {[0],[1],[2],[3]} of integers modulo 4. Let H={[0],[2]} be a subgroup of Z_4 under $+_4$. Find the left cosets of H.

[0] + [H] = {[0],[2]} = H
[1] + [H] = {[1],[3]}
[2] + [H] = {[2] ,[4]} = {[2],[0]} = {[0],[2]} = H
[3] + [H] = {[3] , [5]} = {[3],[1]} = {[1],[3]} = [1] + H

∴ [0] + H = [2] + H = H and [1] + H = [3] + H are the two distinct left cosets of H in Z_4

11. State Lagrange's theorem for finite groups. Is the converse true?

If G is a finite group and H is a sub group of G, then the order of H is a divisor of order of G. The converse of Lagrange's theorem is false.

12. Define ring and give an example of a ring with zero-divisors.

An algebraic system (R,+,.) is called a ring if the binary operation + and . satisfies the following conditions.

(i) (a+b)+c=a+(b+c) a,b,c ∈ R
(ii) There exists an element 0 ϵ R called zero element such that a+0 = 0+a =a for all a ∈ R
(iii) For all aϵR,a+(-a) =(-a)+a = 0,-a is the negative of a.
(iv) a+b =b+a for all a,b ϵR
(v) (a.b).c =a.(b.c) for all a,b,c ∈ R

The operation * is distributive over + i.e.,for any a,b,c ϵ R, a.(b+c) = a.b +a.c , (b+c).a = b.a +c.a In otherwords, if R is an abelian group under addition with the properties (iv) and (v) then R is a ring.

Example:The ring $(Z_{10},+_{10},X_{10})$ is not an integral domain.Since $5X_{10}2$,yet $5 \neq 0,2 \neq 0$ in Z_{10}.

13. Define unit and multiplicative inverse of a Ring.

Let R be a ring with unity u. If a ∈ R and there exists b ∈ R such that ab=ba=u, then b is called a multiplicative inverse of a and a is called a unit of R.

14. Define integral domain and give an example.

Let R be a commutative ring with unity. Then R is called an integral domain if R has no proper divisors of zero.

Example: (Z,+,●) is an integral domain and Q,R,C are integral domain under addition and multiplication

15. Define Field and give an example.

A commutative ring (R,+,●) with identity is called a field if every non-zero element has a multiplicative inverse. Thus (R,+,●) is a field if

(i) (R,+) is abelian group and
(ii) (R-{0},●) is also abelian group.

Example: (R,+,●) is a field.

16. Give an example of a ring which is not a field.

(Z,+,●) is a ring but not a field, if every non-zero element need not a multiplicative inverse.

17. Define Integer modulo n.

Let $n \in Z^+$, n>1. For a,b ∈ Z, we say that " a is congruent to b modulo n", and we write $a \equiv b (\mathrm{mod}\, n)$, if $n|(a-b)$, or equivalently, $a = b + kn$ for some $k \in Z$.

18. Determine the values of the integer n>1 for the given congruence $401 \equiv 323 (\mathrm{mod}\ n)$ is true.

401-323=78=2.3.13 there are five possible divisors (n>1),namely 2,3,6,26,39.

19. Determine the values of the integer n>1 for the given congruence $57 \equiv 1 (\mathrm{mod}\ n)$ is true.

57-1=56=2^3.7. So there are six divisors, namely 2,4,8,14,28,56

20. Determine the values of the integer n>1 for the given congruence $68 \equiv 37 (\mathrm{mod}\ n)$is true.

68-37=31, prime, consequently n=31.

21. Determine the values of the integer n>1 for the given congruence $49 \equiv 1 (\mathrm{mod}\ n)$is true.

49-1=48=2^4.3. So there are nine possible values for n>1, namely 2,4,8,16,3,6,12,24,48.

22. Find all subrings of Z_{24}.

The set of all subrings of Z_{24} is {0},{0,12},{0,8,16}, {0,6,12,18}, {0,4,8,12,16,20}, {0,3,6,...,18,21}, {0,2,4,6,...,20,22), Z_{24}

23. Define Ring homomorphism.

Let $(R,+,\bullet)$ and $(S,\oplus,\otimes)$ be rings. A function $f:R\to S$ is called a ring homomorphism if for all $a,b\in R$,

a) f(a+b)=f(a) $\oplus$ f(b), and

b) f (a.b)=f(a) $\otimes$ f(b). When the function f is onto we say that S is a homomorphic image of R.

24. Define Ring isomorphism.

Let $f:(R,+,\bullet)\to(S,\oplus,\otimes)$ be a ring homomorphism. If f is one-to-one and onto, then f is called a ring isomorphism and we say that R and S are isomorphic rings.

25. State Chinese Remainder Theorem.

Let $m_1,m_2,...,m_k\in Z^+-\{1\}$ with $k\geq 2$, and with $\gcd(m_i,m_j)=1$ for all $1\leq i<j\leq k$. Then the system of k congruences.

$$x\equiv a_1(\mathrm{mod}\, m_1)$$
$$x\equiv a_2(\mathrm{mod}\, m_2)$$
$$\ldots$$
$$x\equiv a_k(\mathrm{mod}\, m_k)$$

Has a simultaneous solution. Further , any two such solutions of the system are congruence modulo $m_1,m_2,...,m_k$.

PART-B

1. (a) Let $(G,o),(H,*)$ be groups with respective identities e_G,e_H. If $f:G\to H$ is a homomorphism, then

a) $f(e_G)=e_H$ b) $f(a^{-1})=[f(a)]^{-1}$ for all $a\in G$.

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

d) $f(S)$ is a subgroup of H for each subgroup S of G. **(8)**

(b) Let $a\in G$ with O(a)=n. if $k\in Z$ and $a^k=e$, then n/k. **(8)**

2. State and prove the fundamental theorem of group homomorphism's. **(16)**

3. (a) Let G be a cyclic group. **(8)**

a) If $|G|$ is infinite, then G is isomorphic to $(Z,+)$.

b) If $|G|$=n, where $n>1$, then G is isomorphic to $(Z_n,+)$.

(b) Every subgroup of a cyclic group is cyclic **(8)**

4. Show that $(M,\bullet)$ is an abelian group where $M=\{A,A^2,A^3,A^4\}$ with $A=\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}$ and $\bullet$ is ordinary matrix multiplication. Further prove that $(M,\bullet)$ is isomorphic to the abelian group $(G,\bullet)$ where $G=\{1,-1,i,-i\}$ and $\bullet$ is ordinary multiplication. **(16)**

5. (a) Find the left cosets of the subgroup $H=\{[0],[3]\}$ of the group $(Z_6,+_6)$ **(8)**

(b) Show that H = { [0],[4],[8] } is a subgroup of $(Z_{12},+_{12})$. Also find the left Cosets of H in $(Z_{12},+_{12})$. **(8)**

6. State and prove Lagrange's theorem for finite group. **(16)**

7. (a) For $\beta=\begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 1 & 2 & 3\end{pmatrix}$ find the subgroup $k=\langle\beta\rangle$. **(8)**

(b) Determine the left cosets of k in $G=S_4$. **(8)**

8. (a) Let R be a ring with unity u. Prove that the units of R form a group under the multiplication of the ring. **(8)**

(b) Determine whether $(z,\oplus,\circ)$ is a ring with the binary operations
$x \oplus y = x + y - 7, x \circ y = x + y - 3xy$ for all $x, y \in Z$. **(8)**

9. (a) For any ring $(R,+,\bullet)$ and any $a \in R$, we have $az = za = a$. **(8)**
(b) Given a ring $(R,+,\bullet)$, for all $a,b \in R$, **(8)**
   a) –(-a)=a,
   b) a(-b)=(-a)b=-(ab), and
   c) (-a)(-b)=ab.

10. For a ring $(R,+,\bullet)$, **(16)**
   a) if R has a unity, then it is unique, and
   b) if R has a unity, and x is a unit of R, then the multiplicative inverse of x is unique.

11. Let $(R,+,\bullet)$ be a commutative ring with unity. Then R is an integral domain if and only if, for all $a,b,c \in R$, where $a \neq z, ab = ac \Rightarrow b = c$. **(16)**

12. (a) Show that $(Z,+,\times)$. is an integral domain where Z is the set of all integers. **(8)**
(b) If $(F,+,\bullet)$ is a field, then it is an integral domain. **(8)**

13. Given a ring $(R,+,\bullet)$, a nonempty subset S of R is a subring of R if and only if **(16)**
   a) for all $a,b \in S$, we have $a+b, ab \in S$,
   b) for all $a,b \in S$, we have $-a \in S$.

14. Let consider the ring $R = M_2(Z)$ and the subset $S = \left\{ \begin{bmatrix} x & x+y \\ x+y & x \end{bmatrix}; x, y \in Z \right\}$ of R. Prove that S is subring of R. **(16)**

15. Let $A = \left\{ \begin{bmatrix} a & 0 \\ b & c \end{bmatrix}; a,b,c \in Z \right\}$ be the subset of the ring $R = M_2(z)$. Prove that A is a subring **(16)**

16. (a) For $n \in Z^+, n > 1$, under the closed binary operations defined above, Prove that Z_n is a commutative ring with unity. **(8)**
(b) Prove that Z_n is a field if and only if n is a prime. **(8)**

17. (a) In Z_n, prove that [a] is a unit if and only if gcd(a,n)=1. **(8)**
(b) Find $[25]^{-1}$ in Z_{72}. **(8)**

18. Let $f : (R,+,\bullet) \to (S,\oplus,\otimes)$ is a ring homomorphism, then **(16)**
   a) $f(Z_R) = Z_S$, where Z_R, Z_S are the zero elements of R and S, respectively;
   b) $f(-a) = -[f(a)]$, for all $a \in R$;
   c) $f(na) = nf(a)$, for all $a \in R, n \in Z$;
   d) $f(a^n) = [f(a)]^n$, for all $a \in R, n \in Z^+$; and
   e) If A is a subring of R, it follows that f(A) is a subring of S.

19. State and prove The Chinese Remainder Theorem. **(16)**

20. Let $A = \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}; a \in R \right\}$ **(16)**
   a) show that A is a ring under matrix addition and multiplication
   b) Prove that R is isomorphic to A.

UNIT II
FINITE FIELDS AND POLYNOMIALS
PART-A

1. Define ring.

A non empty set R with two binary operations + and. is called a ring if (R,+) is an abelian group,(R,.) is closed under the associative operation . , and the two operations are related by the distributive laws:

a (b+c)=ab+ac and (b+c)a=ba+ca, for all a,b,c$\in R$ (Here ab=a.b)

2. Define polynomial.

Given a ring (R,+,.), an expression of the form
$f(x)=a_nx^n+a_{n-1}x^{n-1}+.....+a_1x^1+a_0x^0$, *where* $a_i \in R$ *for* $0\le i\le n$, is called a polynomial in the indeterminate x with coefficients from R.

3. Define Field.

A field is a nonempty set F of elements with two operations '+' (called addition) and '·' (called multiplication) satisfying the following axioms. For all a, b, c ∈ F:

(i) F is closed under + and · ; i.e., a + b and a · b are in F.
(ii) Commutative laws: a + b = b + a, a · b = b · a.
(iii) Associative laws: (a + b) + c = a + (b + c), a · (b · c) = (a · b) · c.
(iv) Distributive law: a · (b + c) = a · b + a · c.

4. What is meant by a finite field?

A field containing only finitely many elements is called a finite field, A finite field is simply a field Whose underlying set is finite. Eg: F_2, whose element 0 and 1.

5. What is meant by polynomial ring?

If R is a ring , then under the operations of addition and multiplication + and .,(R[x],+,.) is a ring ,called the polynomial ring, or ring of polynomials over R.

6. Define root of the polynomial.

Let R be a ring with unity u and let f(x) $\in R(x)$,with degree f(x) ≥ 1. If r$\in R$ and f(r)=z, then r is called a root of the polynomial f(x)

7. When do you you say that f(x) is a divisor of g(x)?

Let F be a field. For f(x), g(x) $\in F(x)$, where f(x) is not a zero a polynomial , we all f(x) a divisor of g(x) if there exists h(x) $\in F(x)$ with f(x)h(x)=g(x). In this situation we also say that f(x) divides g(x) and that g(x) is a multiple of f(x)

8. Find the roots of f(x)=x²-2 $\in Q(x)$.

f(x)= x²-2=$(x+\sqrt{2})(x-\sqrt{2})$

Since $\sqrt{2}$ and -$\sqrt{2}$ are irrational numbers , f(x) has no roots.

9.Find all roots of f(x)=x²+4x if f(x) $\in z_{12}[x]$

Z_{12}={0,1,2,3,4,5,6,7,8,9,10,11}
f(0)=0+0=0 ∴ 0 is a root of f)x)
f(1)1+4=5
f(2)=4+8=12=0
So 2 is a root.
f(3)=21, f(4)32
f(5)=45,f(6)=60=0
So 6 is a root
f(7)=77, f(8)=96=0
So 8 is aroot.
f(9)=81+36=117. f(10)100+40=140
f(11)=121+44=165
Thus x=0,2,6,8 are the roots of f(x)

10. State division algorithm

Let f(x),g(x) $\in F(x)$ with f(x) not the zero polynomial. There exists unique polynomials q(x), r(x) $\in F(x)$such that g(x)=q(x)f(x)+r(x),where r(x)=0 or degree r(x)< degree f(x).

11. State the remainder theorem.

The remainder theorem:
For f(x) $\in F(x)$and a$\in F$, the remainder in the division of f(x) by x-a is f(a).

12. Determine all polynomials of degree 2 in z_2[x].

The polynomials are

(i) x^2
(ii) x^2+x
(iii) x^2+1
(iv) x^2+x+1

13. State the factor theorem.

If f(x) $\in F(x)$ and a f(x) $\in F$, then x-a ia a factor of f(x) if and only if a is a root of f(x).

14. Determine polynomial h(x) of degree 5 and polynomial k(x)of degree 2 such that degree of h(x)k(x) is 3.

Choose $h(x)=4x^5+x$ of degree 5 and $k(x)3x^2$ of degree 2. Then $h(x)k(x)= (4x^5+x)(3x^2)=12x^7+3x^3=0+3x^3$ which is of degree 3.

15. Define reducible and irreducible polynomials .

Let f(x) $\in F(x)$, with F a field and degree f(x) ≥ 2. We call f(x) 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 it is called irreducible or prime.

16. Give example for reducible and irreducible polynomials .

The polynomial f(x) $=x^4+2x^2+1$ is reducible . Since $x^4+2x^2+1=(x^2+1)^2$
The polynomial x^2+1 is irreducible in Q[x] and R[x]but in C[x] it is reducible.

17. Verify the polynomial x^2+x+1 over Z_3,Z_7 irreducible or not.

The polynomial $x^2+x+1=(x+2)(x+2)$ is irreducible over Z_3
The polynomial $x^2+x+1=(x+5)(x+3)$ is irreducible overZ_7.

18. What is meant by monic polynomial?

A polynomial f(x) $\in F(x)$ is called monic if its leading coefficients is 1, the unity of F.
Example: $x^2+2x+ 1$

19. When do you say that 2 polynomials are relatively prime?

If f(x),g(x) $\in F(x)$ and their gcd is 1, then f(x) and g(x)are calle d relatively prime.

20. What is the characteristic of R?

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

21. Find the characteristic of the following rings a) (Z_3,+,.) b)(Z_4,+,.) and $Z_3[x]$

The ring (Z_3,+,.) has characteristic 3.
The ring (Z_4,+,.) has characteristic 4
$Z_3[x]$ has characteristic 3.

22. Give an example of a polynomial f(x) $\in R(x)$ where f(x) has degree 8, is reducible but has no real roots.

Choose $f(x)=(x^2+9)^4$ is of degree 8, is reducible but has no real roots.

23. Write f(x)= $(2x^2+1)(5x^3-5x+3)(4x-3)\in z_7[x]$ as the product of unit and three monic polynomials.

$$f(x)=(2x^2+1)(5x^3-5x+3)(4x-3)$$
$$=2(x^2+4)5(x^3-x+2)4(x-6)$$
$$=40(x^2+4)(x^3-x+2)4(x-6)$$
$$=5(x^2+4)(x^3-x+2)4(x-6)$$

Here each polynomial is monic.

24. If f(x) and g(x) are relatively prime and $\in F(x)$ where F is any field , show that there is no element a$\in F$ such that f(a)=0 and g(a)=0

Suppose there exists a$\in F$ such that f(a)=0 and g(a)=0. Then (x-a) would be a factor of both f(x) and g(x). So (x-a) would divide the gcd of both f(x) and g(x).But this is a contradiction since f(x) and g(x) are relatively prime.

25. Define congruence modulo m.

Let a, b and m > 1 be integers. We say that a is congruent to b modulo m, written as

$a \equiv b \pmod m$, if $m|(a-b)$; i.e., m divides a − b.

PART B

1. (a)Show that (R,+,.) is a ring **(8)**
   (b)Show that R[x] is a polynomial ring over R. **(8)**
2. (a)If R is an integral domain ,prove that f(x) is an unit in R[x], then prove that f(x) is constant and is unit in R **(8)**
   (b)If R[x] is a polynomial ring then show that it is commutative. **(8)**
3. (a)Prove that every field is an integral domain. **(8)**
   (b)Let (R,+,.) be a commutative ring with unity u .Show that R is an integral domain if and only if for all f(x),g(x) $\in R(x)$, if neither f(x) nor g(x) is the zero polynomial , then degree f(x) g(x)=degree f(x)+degree g(x) **(8)**
4. (a)Find all the irreducible polynomials in $Z_2[x]$ **(8)**
   (b)Find all the roots of $f(x)=x^2+3x+2 \in Z_6[x]$ **(8)**
5. State and prove Division algorithm **(16)**
6. (a)State and prove remainder and factor theorem **(8)**
   (b) Discuss irreducible and reducible polynomials with example over R[x],Q[x],C[x]. **(8)**
7. (a)Find the remainder when f(x) is divisible by g(x)
   f(x),g(x) $\in Q(x)$, $f(x)=x^8+7x^5-4x^4+3x^3+5x^2-4$, $g(x)=x-1$ **(8)**
   (b) f(x),g(x) $\in Z_{11}(x)$, $f(x)=3x^5-8x^4+3x^3-x^2+4x-7$, $g(x)=x+9$ **(8)**
8. (a)If f(x) $\in F(x)$ has degree n ≥ 1, then prove that f(x) has atmost n roots. **(8)**
   (b)If g(x)= x^5-2x^2+5x-3 *and* $f(x)=x^4-5x^3+7x$, determine q(x) and r(x) such that g(x)=q(x)f(x)+r(x) **(8)**
9. (a)If $f(x)=x^4-16$, find its roots and factorization in Q(x). **(8)**
   (b)Determine all the polynomials of degree 2 in $Z_7[x]$. **(8)**
10. (a)Find all the roots of $f(x)=x^2+4x$ if f(x) $=Z_{12}[x]$ **(8)**
    (b)Show that for all f(x) $\in F(x)$, every nonzero polynomial of degree ≤ 1 is irreducible. **(8)**
11. (a)Let (F,+,.) be a field . If char(F)>0, then show that char(F) must be finite. **(8)**
    (b) Prove that the characteristic of a field is either 0 or a prime number **(8)**
12. (a)Prove that the polynomial $f(x) = x^4 + 2x^6 \in Z_3[x]$ is of degree 6 is reducible . **(8)**
    (b)Show that a finite field has order p^t, where p is a prime and t$\in Z^+$ **(8)**
13. (a)Construct a finite field of 25 elements. **(8)**
    (b)Give characteristic for the following rings **(8)**
    (a)Z_{11} (b)$Z_{11}[x]$ (c)Q[x]
14. (a)Find the roots of f(x)= $= x^2+3x+2 \in Z_6[x]$ **(8)**
    (b)State and prove Euclidean algorithm. **(8)**
15. (a)Show that g(x)=q(x)f(x)+r(x), if $g(x)=x^4+2x^3+x+4$, $f(x)=x^2+3x+1$ **(8)**
    (b) Show that Z_m is a field if and only if m is a prime. **(8)**

UNIT-III
DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS
PART-A

1. **Write about divisible.**
   An integer b is divisible by an integer a, not zero, if there is an integer x such that b = ax, and we write a/b. m In case b is not divisible by a, we write a\b.
2. **Define division algorithm.**
   Given any integers a and b, with a > 0, there exist unique integers q and r such that b =qa + r, 0 < r < a. If a\b, then r satisfies the stronger inequalities z < r < a.
3. **Define greatest common divisor of b.**

The integer a is a common divisor of b and c in case a/b and a/c. Since there is only a finite number of divisors of any nonzero integer, there is only a finite number of common divisors of b and c, except in the case b=c=0, If at least one of b and c is not 0, the greatest among their common divisors is called the greatest common divisor of b and c and is denoted by (b, c).

4. Define Euclidean algorithm.

Given integers b and c > 0, we make a repeated application of the division algorithm, to obtain a series of equations

$b = cq_1 + r_1, \quad 0<r_1<c$
$c = r_1q_2 + r_2, \quad 0<r_2<r_1$
$r_1 = r_1q_3 + r_3, \quad 0<r_2<r_1$
$\ldots\ldots\ldots\ldots \quad \ldots\ldots$
$r_{j-2} = r_{j-1}q_j + r_j, \quad 0<r_2<r_1$
$r_{j-1} = r_jq_{j+1}$

The greatest common divisor (b, c) of b and c is r_j, the last nonzero remainder in the division process. Values of x_0 and y_0 In (b, c) = bx_0+cy_0 can be obtained by writing each r_i as a linear combination of b and c.

5. Solve by Euclidean algorithm for b=288 and c=158.

288=158.2-28
158=28.6-10
28=10.3-2
10=2.5

6. Define least common multiple.

The integers $a_1,a_2,\ldots.a_n$. all different from zero, have a common multiple b if a_i/b for i=1,2,....n. The least of the positive common multiples is called the least common multiple [le, and it is denoted by $[a_1,a_2,\ldots.a_n]$.

7. Define prime number.

An integer p>1 is called a prime number, or a prime , in case there is no divisor d of satisfying 1<d<p.

8. Define Composite number with example.

If an integer a>1 is not a prime, it is called a composite number. Eg: 4,6,8,9....

9. State the binomial theorem.

For any integer n≥1 and any real numbers x and y $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$.

10. Define arithmetical function with example.

A function f(n) defined for all natural numbers n is called an arithmetical function. Eg:x^2+x-3

11. Prove that if n is an even number, then 3^n+1 is divisible by 2; if n is an odd number, k then 3^n+1 is divisible by 2^2; if n is any number, whether even or odd, then 3^n+1 is not divisible by 2^m with m≥3.

Since the square of an odd number minus 1 is a multiple of 8, when n=2m we have $3n=3^{2m}=(3^m)^2=8a+1$, and therefore$3^n+1=2(4a+1)$. When n=2m+1, we have $3^n+1=3^{2m}+1=3(8a+1)+1=4(6a+1)$. Since 4a+1 and 6a+1 are odd , the statement is true.

12. Show that if $1<a_1<a_2\ldots.<a_{n-1}<a_n$, then there exist i and j with i<j, such that a_i/a_j.

Let $a_i=2^{ni}b_i,n_i\geq 0)$, b_i is odd. Since among 1,2,....,2n, there are only n distinct odd numbers $b_1,\ldots.,b_{n+1}$ are not all distinct, in other words, among them there are some equal odd numbers, Let $b_i=b_j$. Then ai/aj.

13. Define square number with example.

If an integer a is a square of some other integer, then a is called a square number.Eg:4,9,16...

14. Find the greatest common divisor of 525 and 231.

From 525=2.231+63
231=3.63+42
63=1.42+21
42=2.21

Therefore g.c.d.(525,231)=21

15. Find GCD(136,221,391).

(136,221,391)= (136,221-136,391-2.136)
= (136,85,119)
= (51,85,34)
=(17,17,34)=17

PART-B

1. (a) State and prove division algorithm. **(8)**
   (b) If g is the greatest common divisor of b and c, then prove that there exist integers x0 and y0 such that g=(b,c)=bx0+cy0. **(8)**
2. (a) If c\ab and (b,c)=1, then prove that c\a. **(8)**
   (b) State and prove Euclidean algorithm. **(8)**
3. (a) Find the greatest common divisor of 42823 and 6409. **(8)**
   (b) Find integers x and y to satisfy 42823x + 6409y=17. **(8)**
4. (a) Find g=(b,c) where b=5033464705 and c=3137640337, and determine x and y such that bx + cy = g. **(8)**
   (b) Find the least common multiple of (i)482 and 1687, (ii)60 and 61. **(8)**
5. (a) How may integers between 100 and 1000 are divisible by 7? **(8)**
   (b) Prove that the product of three consecutive integers is divisible by 6 of four consecutive integers by 24. **(8)**
6. (a) Show that if k is any positive integer, then k^2+k+1. **(8)**
   (b) Let a>1, and m, n be positive integers. Prove that $(a^m-1,a^n-1)=a^{(m,n)}-1$ **(8)**
7. (a) If m is a composite integer prove that the following integer is so too: n_m=11……11(m times). **(8)**
   (b) If p is prime, propve that there exist no positive integers a and b such that $a^2=pb^2$. **(8)**
8. (a) If an integer a is greater than 2 , prove that $S(a)<a\sqrt{(a)}$ **(8)**
   (b) Prove that if $3/(a^2+b^2)$, then 3/a and 3/b. **(8)**
9. (a) Find the smallest positive integer having only 10 positive divisors. **(8)**
   (b) Find the smallest positive integer if the sum of all its divisors is 15. **(8)**
10. (a) Find all the integers n such that P(n)=64. **(8)**
    (b) Prove that there are infinitely many primes of the form 3n+2. **(8)**
11. (a) Find positive integers a and b satisfying the equations (a,b)=10 and [a,b]=100 simultaneously. Find all solutions. **(8)**
    (b) Prove that (a, b)=a, b, a+b) and more generally that (a, b)=(a, b, ax+by) for all integers x, y. **(8)**
12. (a) Prove that (a, a+k)/k for all integers a, k not both zero **(8)**
    (b) Prove that (a, a+2) =1 or 2 for every integer a. **(8)**
13. (a) Prove that an integer is divisible by 3 if and only if the sum of it digits is divisible by 3. Prove that an integer is divisible by 9 if and only if the sum of its digits is divisible by 9. **(8)**
    (b) Prove that an integer is divisible by 11 if and only if the difference between the sum of the digits in the odd places and the sum of the digits in the even places is divisible by 11. **(8)**
14. (a) Prove that any prime of the form 3k+1 is of the form 6k+1. **(8)**
    (b) If x and y are odd, prove that x^2+y^2 cannot be a perfect square. **(8)**
15. (a) If x and y are prime to 3, prove that x^2+y^2 cannot be a perfect square. **(8)**
    (b) Show that n/(n-1)! For all composite n>4. **(8)**

UNIT IV
DIOPHANTINE QUATIONS AND CONGRUENCES
PART A

1. **Define linear Diophantine equation.**
   Any linear equation in two variables having integral coefficients can be put in the form ax + by = c where a, b, c are given integers.
2. **State about the solution of linear Diophantine equation.**
   Consider the equation ax + by = c ----(1), in which x and y are integers. If a=b=c=0, then every pair (x, y) of integers is a solution of (1), whereas if a = b = 0 and c ≠ 0, then (1) has no

solution. Now suppose that at least one of a and b is nonzero, and let g = gcd (a, b). If g/c then (1)has no solution.

3. Write the solution of ax + by =c.

If the pair (x_1, y_1) is one integral solution, then all others are of the form $x = x_1 + kb/g$, $y = y_1 = ka/g$ where k is an integer and g=gcd (a, b)

4. Define unimodular with example.

A square matrix U with integral elements is called unimodular if det(U)=±1.Eg: Identity matrix

5. Define Pythagorean triangle.

We wish to solve the equation $x^2+y^2=z^2$ in positive integers. The two most familiar solutions are 3,4,5 and 5,12,13. We refer to such a triple of positive integers as a Pythagorean triple or a Pythagorean triangle, since in geometric terms x and y are the legs of a right triangle with hypotenuse z.

6. Write the legs of the Pythagorean triangles.

The legs of the Pythagorean triangles.

$X=r^2-s^2$

$Y=2rs$

$Z=r^2+s^2$

7. Define congruent and not congruent.

If an d integer m, not zero, divides the difference a-b, we say that a is congruent to b modulo m and write $a \equiv b(\text{mod } m)$. If a-b is not divisible by m, we say that a is not congruent to b modulo m, and in this case we write $a \neq b(\text{mod } m)$.

8. Define residue.

If $x \equiv y(\text{mod } m)$ then y is called a residue of x modulo m.

9. Define complete residue

A set $x_1, x_2, \ldots, x_m$ is called a complete residue system modulo m if for every integer y there is one and only one x_j such that $y \equiv x_j(\text{mod } m)$.

10. State Chinese Remainder Theorem.

Let $m_1, m_2, \ldots, m_r$ denote r positive integers that are relatively prime in pairs, and let $a_1, a_2, \ldots, a_r$ denote any r integers. Then the congruences

$x \equiv a_1(\text{mod } m_1)$

$x \equiv a_2(\text{mod } m_2)$

……

……

$x \equiv a_r(\text{mod } m_r)$

have common solutions. If x_0 is one such solution, then an integer x satisfies the congruences the above equations iff x is of the form $x=x_0+km$ for some integer k. Here $m=m_1m_2\ldots m_r$.

11. Define n-th power residue modulo p.

If (a, p)=1 and $x_n \equiv a$ (mod p) has a solution, then a is called an n-th power residue modulo p.

12. Define Euler's criterion.

If p is an odd prime and (q, p)=1, then $x^2 \equiv a(\text{mod } p)$ has two solutions or no solution according as $a^{(p-1)/2} \equiv$ or $\equiv -1$ (mod p).

PART-B

1. (a) Find all solutions of 10x -7y=17. **(8)**
   (b)Prove that 101x+37y=3819 has a positive solution in integers. **(8)**
2. (a) Find all solution in integers of 2x+3y+4z=5. **(8)**
   (b) Find all solution in integers of the simultaneous equations. 20x+44y+50z=10.
   17x+13y+11z=19. **(8)**
3. (a) Find all solutions of the simultaneous congruence's $3x+z \equiv 1(\text{mod}(5), 4x-y+z \equiv 3(\text{mod}5)$ **(8)**
   (b) For what integers a, b, and c does the system of equations x+2y+3z+4w=a. x+4y+9z+16w=b.
   x+8y+27z+64w=c.have a solution in integers? What are the solutions if a=b=c=1? **(8)**
4. (a) The equation $15x^2-7y^2=9$ has no solution in integers. **(8)**
   (b) let f denote a polynomial with integral coefficients. If a $a \equiv b(\text{mod } m)$ then $f(a) \equiv f(b) \text{mod } m$ **(8)**
5. If $x \equiv y(\text{mod } m)$, then y is called a residue of x modulo m, a set $x_1, x_2, \ldots x_n$. is called a complete

residue system modulo m if for every integer there is one and only one x_j such that $y \equiv x_j \pmod m$ **(16)**

6. (a) If p is a prime number and $p \equiv 1 \pmod 4$ then there exist positive integer a and b such that $a^2+b^2=p$. **(8)**
   (b) Let q be a prime factor of a^2+b^2. If $q \equiv 3 \pmod 4$ then $q \mid a$ and $q \mid b$. **(8)**
7. (a) Find the least positive integer x such that $x \equiv 5 \pmod 7$. $x \equiv 7 \pmod{11}$, and $x \equiv 3 \pmod{13}$ **(8)**
   (b) Show that there is no x for which both $x \equiv 29 \pmod{52}$ and $x \equiv 19 \pmod{72}$. **(8)**
8. (a) Determine whether the system $x \equiv 3 \pmod{10}$, $x \equiv 8 \pmod{15}$, $x \equiv 5 \pmod{84}$ has no solution, and find them all, if any exist. **(8)**
   (b) Exhibit the foregoing one to one correspondence explicitly, when $m_1=7$, $m_2=9$, $m=63$. **(8)**
9. (a) Let $f(x) = x^2+x+7$. Find all roots of congruence $f(x) \equiv 0 \pmod{15}$ **(8)**
   (b) Solve the set of congruence's: $x \equiv 1 \pmod 4$, $x \equiv 0 \pmod 3$, $x \equiv 5 \pmod 7$ **(8)**
10. (a)Find all the integers that satisfy simultaneously: $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 1 \pmod 7$ **(8)**
    (b)Find all the integers that give the remainders 1,2,3 when divided by 3,4,5 respectively. **(8)**
11. (a)Find the number of positive integers≤7200 that are prime to 3600. **(8)**
    (b)Solve the congruence $x^3+4x+8 \equiv 0 \pmod{15}$ **(8)**
12. (a)Solve the congruence $x^3-9x^2+23x-15 \equiv 0 \pmod{503}$ **(8)**
    (b)For any integer x, (a,b)=(b,a)=(a,-b)=(a,b+ax) **(8)**
13. (a)If (a,m)=(b,m)=1, then (ab,m)=1. **(8)**
    (b)If $b \equiv c \pmod m$, then $(b, m) = (c, m)$ **(8)**

UNIT V
CLASSICAL THEOREMS AND MULTIPLICATIVE FUNCTIONS
PART A

1. **State Wilson's theorem**
   The Wilson's theorem states that, if p is a prime, then $(p-1)! \equiv -1 \pmod p$
2. **State Fermat's theorem.**
   Let p denote a prime. If p/a then $a^{p-1} \equiv 1 \pmod p$. For every integer a, $a^p \equiv a \pmod p$.
3. **State Euler's generalization of Fermat's theorem.**
   If (a, m)=1, then $a\phi(m) \equiv 1 \pmod m$.
4. **State Fermat's little theorem**
   If p is a prime and $a \not\equiv 0 \pmod p$, then $a^{p-1} \equiv 1 \pmod p$
5. **Explain the Exponent of an integer modulo n.**
   Let n be a natural number >1 and a an integer prime to n. if the infinite sequence $a, a^2, a^3, \ldots \equiv 1 \pmod n$. Suppose that a^δ is the first number in the sequence $\equiv 1 \pmod n$. then a is said to belong to the Exponent of an integer modulo n
6. **Define improper divisor of n**
   Every integer n is a divisor of itself. It is called the improper divisor of n . All other divisors of n are called proper divisors .
7. **Define Eulers Phi function**
   $\phi(n)$ is the number of non-negative integers less than n that are relatively prime to n. In other words, if $n>1$ then $\phi(n)$ is the number of elements in Un, and $\phi(1)=1$.
8. **If p is a prime, the only elements of Up which are their own inverses are [1] and $[p-1]=[-1]$.**
   Note that $[n]$ is its own inverse if and only if $[n2]=[n]2=[1]$ if and only if $n2 \equiv 1 \pmod p$ if and only if $p|(n2-1)=(n-1)(n+1)$. This is true if and only if $p|(n-1)$ or $p|(n+1)$. In the first case, $n \equiv 1 \pmod p$, i.e., $[n]=[1]$. In the second case, $n \equiv -1 \equiv p-1 \pmod p$, i.e., $[n]=[p-1]$.
9. **Find the remainder of 97! When divided by 101.**

First we will apply Wilson's theorem to note that 100! ≡ −1 (mod101). When we decompose the factorial, we get that: (100)(99)(98)(97!)≡−1(mod101). Now we note that 100 ≡ −1(mod101), 99 ≡ −2 (mod101), and 98 ≡ −3 (mod101).

Hence: (−1)(−2)(−3)(97!)≡−1(mod101)(−6)(97!)≡−1(mod101)(6)(97!)≡1(mod101). Now we want to find a modular inverse of 6 (mod 101). Using the division algorithm, we get that: 101=6(16)+56=5(1)+11=6+5(−1)1=6+[101+6(−16)](−1)1=101(−1)+6(17)

Hence, 17 can be used as an inverse for 6 (mod 101). It thus follows that: (17)(6)(97!)≡(17)1(mod101)97!≡17(mod101) Hence, 97! has a remainder of 17 when divided by 101.

10. For prime p≥5,determine the remainder when (p−4)!is divided by p.

By *Wilson*'s theorem, (p−1)!≡−1(modp). Therefore

−1≡(p−1)(p−2)(p−3)·(p−4)!≡−6·(p−4)!(modp).

If p=6k+1, multiplying both sides of the congruence by k gives (p−4)!≡−k=-(p-1)/6(modp).

If p=6k−1, multiplying both sides of the congruence by k gives (p−4)!≡k=(p+1)/6(modp).

11. Find the remainder of 53! when divided by 61.

We know that by Wilson's theorem 60!≡−1(mod61). Decomposing 60!, we get that: (60)(59)(58)(57)(56)(55)(54)(53)(52)51!≡−1(mod61)(−1)(−2)(−3)(−4)(−5)(−6)(−7)(−8)(−9) 51!≡ −1(mod61)(−362880)51!≡−1(mod61)(362880)51!≡1(mod61)(52)51!≡1(mod61) We will now use the division algorithm to find a modular inverse of 52 (mod 61): 61=52(1)+952=9(5)+79=7(1)+27=2(3)+11=7+2(−3)1=7+[9+7(−1)](−3)1=9(−3)+7(4)1=9(−3)+[52+9(−5)](4)1=52(4)+9(−23)1=52(4)+[61+52(−1)](−23)1=61(−23)+52(27) Hence 27 can be used as an inverse (mod 61). We thus get that: (27)(52)51!≡(27)1(mod61)51!≡27(mod61) Hence the remainder of 51! when divided by 61 is 2.

12. What is the remainder of 149! when divided by 139?

From Wilson's theorem we know that 138!≡−1(mod139). We are now going to multiply both sides of the congruence until we get up to 149!: 149!≡(149)(148)(147)(146)(145)(144)(143)(142)(141)(140)(139)(−1)(mod139)149!≡ (10)(9)(8)(7)(6)(5)(4)(3)(2)(1)(0)(−1)(mod139)149!≡0(mod139). Hence the remainder of 149! when divided by 139 is 0.

13. Define congruence in one variable

A congruence of the form $ax \equiv b \pmod m$ where x is an unknown integer is called a linear congruence in one variable.

14. Let p be a prime. A positive integer m is its own inverse modulo p iff p divides m + 1 or p divides m − 1.

Suppose that m is its own inverse. Thus $m.m \equiv 1 \pmod p$. Hence $p \mid m^2 - 1$.then $p \mid (m-1)$or $p \mid (m+1)$.

PART B

1. State and prove Wilson's theorem **(16)**
2. (a) For n>2, φ(n) is an even integer **(8)**
   (b)Verify the equality φ(n)=φ(n+1)=φ(n+2) holds when n=5186. **(8)**
3. (a) State and prove Euler's theorem **(8)**
   (b) If p is a prime, then $(p-1)! \equiv -1 \pmod p$ **(8)**
4. (a) If m and n are relatively prime positive integers, prove that $m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}$. **(8)**
   (b) For any integer a, show that a and a^{4n+1} have the same last digit. **(8)**
5. (a) Using Euler's theorem to evaluate $2^{100000} \pmod{77}$ **(8)**
   (b) Find the units digit of 3^{100} by means of Euler's theorem. **(8)**
6. For any prime p, establish each of assertions below **(16)**

   (i) τ(p!)=2τ((p-1)!)

   (ii) σ(p!)=(p+1)σ((p-1)!)

(iii) $\varphi(p!)=(p-1)\varphi((p-1)!)$

7. (a) If p is a prime and a is a positive integer, then $\phi(pa)=pa-pa-1$ **(8)**
   (b) If a and b are relatively prime and $n=ab$, then $\phi(n)=\phi(a)\phi(b)$. **(8)**

8. (a) State and prove Fermat's theorem **(8)**
   (b) Given integers a, b c, gcd(a, bc)=1 iff gcd(a,b)=1 and gcd(a,c)=1 **(8)**
9. State and prove Euler generalization of Fermat's theorem **(16)**
10. State and prove Fermat's little theorem. **(16)**
11. let p be a prime number. Then $x^2 \equiv 1(\text{mod } m)$ iff $x \equiv \pm 1(\text{mod } p)$. **(16)**
12. If p is a prime and k>0, then $\Phi(p^k) = p^k - p^{k-1} = p^k\left(1-\frac{1}{p}\right)$ **(16)**