SRM VALLIAMMAI ENGINEERING COLLEGE

(An Autonomous Institution)

S.R.M.Nagar, Kattankulathur, 603203

DEPARTMENT OF MATHEMATICS

QUESTION BANK

V SEMESTER

B. E- CYBER SECURITY

1918501- MATHEMATICAL FOUNDATION FOR CYBER SECURITY SYSTEM

Regulation – 2019

Academic Year – 2022 - 2023

Prepared by

Dr. T.ISAIYARASI , Assistant Professor / Mathematics

SRM VALLIAMMAI ENGNIEERING COLLEGE

(An Autonomous Institution)

SRM Nagar, Kattankulathur – 603203.

DEPARTMENT OF MATHEMATICS

SUBJECT: 1918501- Mathematical Foundation for Cyber Security System

SEM / YEAR: V / III Year B.E. CYBER SECURITY

UNIT I - GROUPS AND RINGS Algebra: groups, cyclic groups, rings, fields, finite fields and their applications to cryptography			
Q.No.	**Question**	**BT Level**	**Competence**
	PART – A		
1.	Define group and State any two properties of a group	BTL -1	Remembering
2.	Define a cyclic group and give an example	BTL -1	Remembering
3.	Define cosets of a group	BTL -1	Remembering
4.	Prove that identity element in a group is unique	BTL -2	Understanding
5.	Prove that the inverse of each element of the group (G,*) is unique	BTL -3	Applying
6	Let Z be a group of integers with binary operation * defined by $a * b = a + b - 2$ for all $a, b \in Z$. Find the identity element of the group$\langle Z, * \rangle$	BTL -3	Applying
7.	In a group $(G,*)$, $prove\ that\ (a * b)^{-1} = b^{-1} * a^{-1}$for all $a, b \in G$	BTL -2	Understanding
8	Show that the cancellation laws are true in a group $(G,*)$	BTL -2	Understanding
9.	Prove that every cyclic group is abelian	BTL -3	Applying
10	If $(G,*)$ is a group for any $a \in G$ prove that $(a^{-1})^{-1} = a$	BTL -2	Understanding
11.	If $(G,*)$ is a group infer that the only idempotent element of a is the identity element	BTL -4	Analyzing
12.	Show that $(Z_5, +_5)$ is a cyclic group	BTL -3	Applying
13.	Prove that the order of an element a of a group G is the same as that of its inverse (a^{-1})	BTL -4	Analyzing
14.	Prove that if G is abelian group then for all $a, b \in G, (a * b)^2 = a^2 * b^2$	BTL -2	Understanding
15.	If a is a generator of a cyclic group$G$, then show that a^{-1} is also a generator of G	BTL -4	Analyzing
16.	State Lagrange's theorem	BTL -1	Remembering
17.	Find the left cosets of {[0], [3]} in the addition modulo group $(Z_6, +_6)$	BTL -4	Analyzing
18.	If G is a group of order n and $a \in G$, prove that $a^n = e$	BTL -2	Understanding
19.	Give an example of a ring which is not a field	BTL -4	Analyzing
20.	Discuss a ring and give an example	BTL -3	Applying
21.	Discuss a sub ring with example	BTL -2	Understanding
22.	Define integral domain and give an example.	BTL -4	Analyzing
23.	Define a field with example	BTL -1	Remembering
24.	Define conjugacy search problem in a group	BTL -1	Remembering
25.	Define discrete logarithm problem in a group	BTL -1	Remembering
	PART – B		

1.	Prove that $G = \left\{\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}, \begin{pmatrix}-1 & 0\\0 & 1\end{pmatrix}, \begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}, \begin{pmatrix}-1 & 0\\0 & -1\end{pmatrix}\right\}$ forms an abelian group under matrix multiplication	BTL -3	Applying
2.(a)	Prove that in a group G the equations $a * x = b$ and $y * a = b$ have unique solutions for the unknowns x and y as $x = a^{-1} * b, y = b * a^{-1}$ when $a, b \in G$	BTL -2	Understanding
2.(b)	Evaluate that the set of all matrices $\begin{bmatrix}a & b\\-b & a\end{bmatrix}$forms an abelian group with respect to matrix multiplication	BTL -5	Evaluating
3.	Apply the definition of a group to Prove that $(G,*)$ is a non-abelian group where $G = R^* \times R$ and the binary operation * is defined as $(a, b) * (c, d) = (ac, bc + d)$	BTL -3	Applying
4.(a)	If $(G,*)$ is an abelian group and if $\forall\ a, b \in G$. Show that $(a * b)^n = a^n * b^{\ n}, for\ every\ integer\ n$	BTL -3	Applying
4.(b)	Show that$(Q^+,*)$ is an abelian group where $*$ is defined as $a * b = ab/2, \forall a, b \in Q^+$	BTL -3	Applying
5.	Show that the union of two subgroups of a group G is again a subgroup of G if and only if one is contained in the other	BTL -3	Applying
6.(a)	Prove that the intersection of two subgroups of a group G is again a subgroup of G	BTL -3	Applying
6.(b)	Prove that the set $\{1, -1, i, -i\}$ is a finite abelian group with respect to the multiplication of complex numbers	BTL -3	Applying
7.	If (G, *) is a finite cyclic group generated by ab element $a \epsilon G$ and is of order n then $a^n = e$ so that $G = \{a, a^2, \ldots a^n (= e)\}$. Also, n is the least positive integer for which $a^n = e$	BTL -1	Remembering
8.(a)	Prove that the necessary and sufficient condition for a non-empty subset Hof a group $(G,*)$to be a subgroup is $a, b \in H \Rightarrow a * b^{-1} \in H$	BTL -4	Analyzing
8.(b)	Prove that every subgroup of a cyclic group is cyclic.	BTL -3	Applying
9.	Show that group homomorphism preserves identity, inverse, and subgroup	BTL -5	Evaluating
10.(a)	Let G be a group and $a \in G$. Let $f: G \to G$ be given by $f(x) = axa^{-1}, \forall\ x \in G$. Prove that f is an isomorphism of G onto G	BTL -6	Creating
10.(b)	Show that the group $(\{1, 2, 3, 4\}, X_5)$ is cyclic	BTL -3	Applying
11.	Analyze that $Z_n$is a field if and only if n is prime	BTL -4	Analyzing
12.(a)	Let $f: G,*) \to (H,\triangle)$ be group homomorphism then show that $Ker(f)$ is a normal subgroup	BTL -3	Applying
12.(b)	Show that M_2, the set of all $2X2$ nonsingular matrices over R is a group under usual matrix multiplication. Is it abelian?	BTL -3	Applying
13.	Prove that in a Ring (R,+,.) (a) The zero element is unique (b) The additive inverse of each ring element is unique (c) If R has a unity then it is unique (d) If R has a unity, x is a unit of R then the multiplicative inverse of x is unique	BTL -4	Analyzing
14.(a)	If G is a group of prime order, then G has no proper subgroups	BTL -3	Applying
14.(b)	Determine whether $H_1 = \{0, 5, 10\}$ and $H_2 = \{0, 4, 8, 12\}$are subgroups of Z_{15}	BTL -3	Applying
15.	Prove that every field is an integral domain and every finite integral	BTL -4	Analyzing

	domain is a field. Give an example for an integral domain which is nor a field		
16.(a)	Define a cyclic group. Prove that any group of prime order is cyclic	BTL -4	Analyzing
16.(b)	Find the left cosets of the subgroup $H = \{[0],[3]\}$ of the group $[Z_6, +_6]$	BTL -3	Applying
17.	Analyze whether $(Z, \oplus, \odot)$ is a ring with the binary operation $x \oplus y = x + y - 1, x \odot y = x + y - xy$ for all $x, y \in Z$	BTL -4	Analyzing
18.(a)	Let $(H, \cdot)$be a subgroup of $(G, \cdot)$. Let $N = \{x \ / x \in G, xHx^{-1} = H\}$. Show that $(N, \cdot)$is a subgroup of G.	BTL -3	Applying
18.(b)	Show that $(Z_{5,} +_5, \cdot_5)$ is a field	BTL -3	Applying
	PART – C		
1.	Prove that every finite group of order n is isomorphic to a permutation group of degree n	BTL -4	Analyzing
2.	Discuss and show that the order of a subgroup of a finite group divides the order of the group	BTL -4	Analyzing
3.	Determine whether $(Q, \oplus, \odot)$is a ring with the binary operations $x \oplus y = x + y + 7, x \odot y = x + y + \frac{xy}{7}$ for all $x, y \in Q$	BTL -2	Understanding
4.	Prove that the set $Z_4 = \{0,1,2,3\}$ is a commutative ring with respct ot the binary operation $+_4$ *and* $\times_4$	BTL -2	Understanding
5.	Discuss the application of discrete logarithm problem in Diffie-Hellman key exchange	BTL -3	Applying

UNIT II - FINITE FIELDS AND POLYNOMIALS

Rings – Polynomial rings – Irreducible polynomials over finite fields – Factorization of polynomials over finite fields

Q.No.	Question	BT Level	Competence
	PART – A		
1.	Define polynomial	BTL -1	Remembering
2.	Define root of a polynomial	BTL -1	Remembering
3.	Find the roots for the function $f(x) = x^2 + 3x + 2 \in \mathbb{Z}_6[x]$	BTL -1	Remembering
4.	What are the roots of $f(x) = x^2 - 6x + 9 \in \mathbb{R}[x]$	BTL -2	Understanding
5.	Find the roots for the function $f(x) = x^2 - 2 \ in \ R[x] and \ Q[x]$	BTL -3	Applying
6	How many polynomials in $\mathbb{Z}_5$ has degree 3?	BTL -3	Applying
7.	How many polynomials in $\mathbb{Z}_7$ has degree 5?	BTL -2	Understanding
8	If $f(x) = 7x^4 + 4x^3 + 3x^2 + x + 4$ & $g(x) = 3x^3 + 5x^2 + 6x + 1, f(x), g(x) \in Z_7[x]$, then find $f(x) + g(x)$ & $\deg(f(x) + g(x))$	BTL -2	Understanding
9.	Determine all polynomials of degree 2 in $\mathbb{Z}_2[x]$	BTL -3	Applying
10	Define irreducible polynomial	BTL -2	Understanding
11.	Determine whether $x^2 + 1$ is an irreducible polynomial over the field {0,1}	BTL -4	Analyzing
12.	Show that $x^2 + x + 1$ is irreducible over Z_5	BTL -3	Applying
13.	Show that $x^2 + 1$ is irreducible in $\mathbb{Z}_3[x]$	BTL -4	Analyzing
14.	Obtain reducible polynomial of degree six with no roots in$\mathbb{Z}_2$	BTL -2	Understanding
15.	Does the set $F = \{0,1,2,3)$ form a filed with respect to addition modulo 4 and multiplication modulo 4? Why?	BTL -4	Analyzing

16.	If $f(x) = x^5 - 2x^2 + 5x - 3 \; and \; g(x) = x^4 - 5x^3 + 7x$are polynomials in Q[x], determine $q(x)$ and $r(x)$ such that $f(x) = q(x)g(x) + r(x)$	BTL -1	Remembering
17.	Find quotient and reminder when g(x) = 2x-1 divides $f(x) = 2x^4 + 5x^3 - 7x^2 + 4x + 8$, where f(x) and g(x) are polynomials over Q[x]	BTL -4	Analyzing
18.	What is the remainder when $f(x) = x^7 - 6x^5 + 4x^4 - x^2 + 3x - 7 \in \mathbb{Q}[x]$ is divided by $x - 2$.	BTL -2	Understanding
19.	State division algorithm for polynomials.	BTL -4	Analyzing
20.	State Remainder theorem.	BTL -3	Applying
21.	Define characteristics of a field.	BTL -2	Understanding
22.	State Euclidean algorithm.	BTL -4	Analyzing
23.	Find two non-zero polynomials $f(x)$ and $g(x)$ in $Z_6[x]$ such that $f(x)g(x) = 0$	BTL -3	Applying
24.	Check the reducibility of $f(x) = x^2 + 3x - 1$ in Q[x], R[x] and C[x]	BTL -2	Understanding
25.	Check the reducibility of $f(x) = x^3 - 1$ in Q[x], R[x] and C[x]	BTL -4	Analyzing
	PART – B		
1.	Let $\mathbb{R}[x]$ be a polynomial ring, then Prove the following (a) If $\mathbb{R}$ is commutative then $\mathbb{R}[x]$ is commutative. (b) If $\mathbb{R}$ is a ring with unity then $\mathbb{R}[x]$ is a ring with unity. (c) $\mathbb{R}[x]$ is an integral domain if and only if $\mathbb{R}$ is an integral domain.	BTL -3	Applying
2.(a)	Find $f(x) + g(x), f(x) - g(x) \; and \; f(x)\, g(x)$ such that $f(x) = x^4 + x^3 + x + 1, g(x) = x^3 + x^2 + x + 1$ over $\mathbb{Z}_2[x]$	BTL -5	Evaluating
2.(b)	Find all the roots of $f(x) = x^5 - x$ in $\mathbb{Z}_5[x]$ and then write $f(x)$ as a product of first degree polynomials	BTL -5	Evaluating
3.	If $\mathbb{R}$ is a ring then prove that $(\mathbb{R}[x], +, \; .)$ is a ring called a polynomial ring over $\mathbb{R}$	BTL -3	Applying
4.(a)	Let $(\mathbb{R}, +, .)$ be a commutative ring with unity u. Then $\mathbb{R}$ is an integral domain iff for all $f(x), g(x) \in \mathbb{R}[x]$, if neither $f(x)$ nor $g(x)$ is the zero polynomial, then prove that degree of $f(x)g(x) = degree f(x) + degree g(x)$	BTL -3	Applying
4.(b)	Find the remainder when $g(x) = 7x^3 - 2x^2 + 5x - 2$ is divided by $f(x) = x - 3$ and $f(x), g(x) \in \mathbb{Z}[x]$	BTL -3	Applying
5.	State and Prove (i) Remainder Theorem (ii) Factor theorem	BTL -3	Applying
6.(a)	Find all roots of $f(x) = x^2 + 4x$ if $f(x) \in Z_{12}$.	BTL -3	Applying
6.(b)	If $g(x) = x^5 - 2x^2 + 5x - 3$ & $f(x) = x^4 - 5x^3 + 7x$ Find $q(x), r(x)$ $such \; that \; g(x) = f(x)q(x) + r(x)$.	BTL -3	Applying
7.	(i) Check whether $f(x) = x^4 + x^3 + x^2 + x + 1 \in Z_2[x]$ is irreducible or not? (ii) Discuss whether $x^4 + x^3 + 1$ is reducible over Z_2	BTL -1	Remembering
8.(a)	If F is a field and $f(x) \in F[x]$ has degree ≥ 1, then prove that $f(x)$ has at most n roots in F	BTL -4	Analyzing
8.(b)	If $(x) = 3x^5 - 8x^4 + x^3 - x^2 + 4x - 7, g(x) = x + 9 \; and$, $f(x), g(x) \in \mathbb{Z}_{11}[x]$ find the remainder when $f(x)$ is divided by $g(x)$	BTL -3	Applying

9.	(i) Determine whether the given polynomial is irreducible or not? $f(x) = x^2 + x + 1$ over Z_3, Z_5, Z_7 (ii) Find four distinct linear polynomials $g(x)\ , h(x)\ , s(x),$ $t(x) \in Z_{12}[x]$ so that $f(x) = g(x)h(x) = s(x)t(x)$.	BTL -5	Evaluating
10.(a)	Give an example of polynomial $f(x) \in F(x)$, where $f(x)$ has degree 8 and degree 6, it is reducible but it has no real roots.	BTL -6	Creating
10.(b)	Discuss whether $x^4 - 2$ is reducible over $\mathbb{Q}\ , \mathbb{R}\ , \mathbb{C}$	BTL -3	Applying
11.	Let (F, +, ·) be a field. If Char (F) > 0, then prove that Char (F) must be Prime	BTL -4	Analyzing
12.(a)	Check whether $f(x) = x^4 + x^3 + x^2 + x + 1 \in Z_2[x]$ is irreducible or not?	BTL -3	Applying
12.(b)	Find four distinct linear polynomials $g(x)\ , h(x)\ , s(x), t(x) \in Z_{12}[x]$ so that $f(x) = g(x)h(x) = s(x)t(x)$	BTL -3	Applying
13.	Identify the equivalence classes of $Z_2[x]$ with $S(x) = x^2 + x + 1$	BTL -4	Analyzing
14.(a)	Write $f(x) = (2x^2 + 1)(5x^3 - 5x + 3)(4x - 3) \in Z_7[x]$ as a product of the unit and three Monic polynomial	BTL -3	Applying
14.(b)	Determine whether the following polynomial is irreducible or not? $f(x) = x^2 + 3x - 1$ in $\mathbb{R}[x]\ , \mathbb{Q}[x],\ \mathbb{C}[x]$	BTL -3	Applying
15.	Determine whether the given polynomial is irreducible or not? $f(x) = x^3 + 3x + 2$ over Z_3, Z_5, Z_7	BTL -4	Analyzing
16.(a)	If $f(x) = 4x^2 + 1\ , g(x) = 2x + 3, f(x), g(x) \in Z_8[x]$. Then show that deg $f(x)g(x) = degf(x) + degg(x)$.	BTL -4	Analyzing
16.(b)	If $f(x) = 2x^4 + 5x^2 + 2\ , g(x) = 6x^2 + 4$, then determine $q(x) and\ r(x) in\ \mathbb{Z}_7[x]$, where $f(x)$ is divided by $g(x)$.	BTL -3	Applying
17.	Analyze the GCD of (i) $4x^3 - 2x^2 - 3x + 1$ and $2x^2 - x - 2$ in Q[x] (ii) $x^5 + x^4 + 2x^2 - x - 1$and $x^3 + x^2 - x$ in Q[x]	BTL -4	Analyzing
18.(a)	Find the remainder when $g(x) = 6x^4 + 4x^3 + 5x^2 + 3x + 1$ is divided by $f(x) = 3x^2 + 4x + 2$ over polynomials in $\mathbb{Z}_7[x]$	BTL -3	Applying
18.(b)	Find the g.c.d of $x^4 + x^3 + 2x^2 + x + 1$ and $x^3 - 1$ over Q.	BTL -3	Applying
PART – C			
1.	Prove that a finite field F has order p^t, where p is a prime and $t \in Z^+$	BTL -4	Analyzing
2.	Infer the equivalence classes of $Z_2[x]$ with $S(x) = x^3 + x + 1$	BTL -4	Analyzing
3.	Obtain the equivalence classes of $Z_3[x]$ with $S(x) = x^2 + 1$	BTL -2	Understanding
4.	Show that $Z_2[x]/x^3 + x + 1$ forms a field	BTL -2	Understanding
5.	Show that $Z_2[x]/x^3 + x^2 + 1$ forms a field	BTL -3	Applying
UNIT III - ANALYTIC NUMBER THEORY Division algorithm – Base – b representations – Number patterns – Prime and composite numbers – GCD – Euclidean algorithm – Fundamental theorem of arithmetic – LCM			
Q.No.	**Question**	**BT Level**	**Competence**
PART – A			
1.	State divisible algorithm	BTL -1	Remembering
2.	State pigeon hole principle	BTL -1	Remembering
3.	State principle of inclusion and exclusion	BTL -1	Remembering
4.	Find the number of positive integers ≤ 2076 that are divisible by 19	BTL -2	Understanding

5.	Find the number of positive integers ≤ 3076 that are not divisible by 17	BTL -3	Applying
6	Find the number of positive integers ≤ 3076 that are divisible by 19	BTL -3	Applying
7.	Prove that if n is odd then $n^2 - 1$ is divisible by 8	BTL -2	Understanding
8	Express $(10110)_2$ in base 10 and express $(1076)_{10}$ in base two	BTL -2	Understanding
9.	Express $(1776)_8$ in base 10 and express $(676)_{10}$ as octagonal	BTL -3	Applying
10	Express $(1976)_{16}$ in base 10 and express $(2076)_{10}$ as hexadecimal	BTL -2	Understanding
11.	Find the six consecutive integers that are composite	BTL -4	Analyzing
12.	Express $(12,15,21)$ as a linear combination of 12,15,and 21	BTL -3	Applying
13.	Prove that the product of any two integers of the form 4n+1 is also the same form	BTL -4	Analyzing
14.	Use canonical decomposition to Evaluate the GCD of 168 and 180	BTL -2	Understanding
15.	Use canonical decomposition to evaluate LCM of 1050 and 2574	BTL -4	Analyzing
16.	Find the canonical decomposition of 2520	BTL -1	Remembering
17.	Find the prime factorization of 420, 135, 1925	BTL -4	Analyzing
18.	Using $(252,360)$ construct $[252,360]$	BTL -2	Understanding
19.	Using recursion evaluate $[24,28,36,40]$	BTL -4	Analyzing
20.	Using recursion evaluate $(18,30,60,75,132)$	BTL -3	Applying
21.	Find the GCD (414,662) using Euclidean algorithm	BTL -2	Understanding
22.	Find the LCM (120.500)	BTL -4	Analyzing
23.	Find the canonical decomposition of 1976	BTL -3	Applying
24.	Use canonical decomposition to Evaluate the GCD of 72 and 108	BTL -2	Understanding
25.	Use canonical decomposition to Evaluate the LCM of 110 and 210	BTL -4	Analyzing
	PART – B		
1.	If $a, b, c \in Z$ then (i) $a/a\,, for\ all\ a \neq 0\ \in Z$ (ii) $a/b\ and\ b/c\ then\ a/c\,, \forall\ a, b \neq 0, c \neq 0\ \in Z$ (iii) $a/b\ then\ a/b\,c, \forall a \neq 0, b \in Z$ $(iv)\ a/b\ and\ a/c\ then\ a/(xb + yc)\,, \forall\ x, y \in Z, a \neq 0 \in Z$	BTL -3	Applying
2.(a)	State and Prove Euclidean algorithm	BTL -5	Evaluating
2.(b)	Find the number of positive integers ≤ 3000 divisible by 3, 5 or 7	BTL -5	Evaluating
3.	Prove that (i) If p is a prime and p/ab then p/a or p/b (ii) If p is a prime and $p/a_1a_2a_3 \cdots a_n$, where $a_{1,}a_{2,}a_{3,} \cdots, a_n$ are positive integers then p/a_i for some i, $1 \leq i \leq n$	BTL -3	Applying
4.(a)	Prove that the GCD of two positive integers a and b is a linear combination of a and b	BTL -3	Applying
4.(b)	Find the number of positive integers in the range 1976 through 3776 that are divisible by 13 and not divisible by 17	BTL -3	Applying
5. (a)	Prove that (i) Every integer $n \geq 2$ has a prime factor.	BTL -3	Applying
5. (b)	Find the number of integers from 1 to 250 that are divisible by any of the integers 2,3,5,7		

6.(a)	Prove that there are infinitely many primes.	BTL -3	Applying
6.(b)	Prove that $(a, a-b) = 1$ if and only if $(a, b) = 1$	BTL -3	Applying
7.	State and prove Fundamental Theorem of Arithmetic.	BTL -1	Remembering
8.(a)	Evaluate $(625{,}1000)$ by using canonical decomposition	BTL -4	Analyzing
8.(b)	Use Euclidean algorithm to find the GCD of $(1819, 3587)$. Also express the GCD as a linear combination of the given numbers	BTL -3	Applying
9.	State and Prove Euclid theorem	BTL -5	Evaluating
10.(a)	Prove that there are infinitely many primes of the form $4n+3$	BTL -6	Creating
10.(b)	Use Euclidean algorithm to find the GCD of $(12345{,}54321)$. Also express the GCD as a linear combination of the given numbers	BTL -3	Applying
11.(a)	If a and b are positive integers then prove that (i) $[a, b] = \frac{a.b}{(a,b)}$	BTL -4	Analyzing
11.(b)	Use Euclidean algorithm to find the GCD of (2076, 1776). Also express the GCD as a linear combination of the given numbers	BTL -3	Applying
12.(a)	Prove that every composite number n has prime factor $\leq \left[\sqrt{n}\right]$	BTL -3	Applying
12.(b)	Prove that two positive integers a and b are relatively prime iff [a,b]= ab	BTL -3	Applying
13.	Use Euclidean algorithm to evaluate the GCD of (2024, 1024). Also express the GCD as a linear combination of the given numbers	BTL -4	Analyzing
14.(a)	Prove that for every positive integer n there are n consecutive integers that are composite numbers	BTL -3	Applying
14.(b)	Use Euclidean algorithm to find the GCD of (4076, 1024). Also express the GCD as a linear combination of the given numbers	BTL -3	Applying
15.	(i)If $d = (a, b)$ and d' is any common divisor of a and b then d'/d (ii) For any positive integer m prove that $(ma, mb) = m(a, b)$ (iii) If $d = (a, b)$, then $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$	BTL -4	Analyzing
16.(a)	Construct the canonical decomposition of 23!	BTL -4	Analyzing
16.(b)	Use Euclidean algorithm to find the GCD of (3076, 1976). Also express the GCD as a linear combination of the given numbers	BTL -3	Applying
17.	If $d = (a, b)$ then $(i)(a, a-b) = d$ (ii)For any integer x then $(a, b) = (a, b+ax)$	BTL -4	Analyzing
18.(a)	Construct the canonical decomposition of 23!	BTL -3	Applying
18.(b)	Use Euclidean algorithm to find the GCD of (3076, 1976). Also express the GCD as a linear combination of the given numbers	BTL -3	Applying
PART – C			
1.	Prove the following If (i)$(a, m) = 1$and $(a, m) = 1$, then $(ab, m) = 1$ (ii)If a/c and b/c and $(a, b) = 1$, then ab/c	BTL -4	Analyzing
2.	A total of 1232 students have taken a course in Spanish, 879 have taken a course in French and 114 have taken a course in Russian. Further 103 have taken courses in both Spanish and French, 23 have taken courses in both Spanish and Russian and 14 have taken courses in both French and Russian. If 2092	BTL -4	Analyzing

	students have taken at least one Spanish, French and Russian, how students have taken a course in all three languages?		
3.	There are 250 students in an Engineering college, of the 188 have taken a course in Fortran, 100 have taken a course in C and 35 have taken a course in Java. Further 88 have taken courses in both Fortran and C, 23 have taken courses in both C and Java and 29 have taken courses in both Fortran and Java . If 19 of of these students have taken all the three course, how many of these 250 students have not taken a course in any of these three programming languages?	BTL -2	Understanding
4.(a)	Prove that in a group of six people at least three must be mutual friends or at least three must be mutual strangers	BTL -2	Understanding
4.(b)	If we select ten points in the interior of an equilateral triangle of side 1 , show that there must be at least two points whose distance apart less than $1/3$	BTL -3	Applying
5.	Apply Euclidean algorithm find the GCD of (i)2024,1024 (ii)4076,2076 Also express the GCD as a linear combination of the given numbers	BTL -3	Applying

UNIT IV - DIOPHANTINE EQUATIONS AND CONGRUENCES

Linear Diophantine equations – Congruence's – Linear Congruence's – Applications: Divisibility tests – Modular exponentiation–Chinese remainder theorem – 2 X2 linear system

Q.No.	Question	BT Level	Competence
	PART – A		
1.	Define linear Diophantine Equation in two variables	BTL -1	Remembering
2.	Discuss whether $6x + 8y = 25$ is solvable	BTL -1	Remembering
3.	Discuss whether 12x+18y=30 is solvable	BTL -1	Remembering
4.	Is 6x+12y+15z=10 solvable?	BTL -2	Understanding
5.	Prove that $9^{100} - 1$ is divisible by 10	BTL -3	Applying
6	Prove that $a \equiv b(mod\ m)$ if and only if $a = b + km\ for\ some\ integer\ k$	BTL -3	Applying
7.	Find the least residue of 23 modulo 5 , -3 modulo 5.	BTL -2	Understanding
8	Define complete sets of residues modulo m.	BTL -2	Understanding
9.	Find the Congruence classes modulo 5.	BTL -3	Applying
10	Find the remainder when $1! + 2! + \cdots + 100!$ is divided by 15	BTL -2	Understanding
11.	Find the remainder when $1! + 2! + \cdots + 1000!$ is divided by 10	BTL -4	Analyzing
12.	Find the remainder when $1! + 2! + \cdots + 1000!$ is divided by 12	BTL -3	Applying
13.	If $a \equiv b(mod\ m)$, then prove that $a^n \equiv b^n(mod\ m)$ for any positive integer n	BTL -4	Analyzing
14.	If $ac \equiv bc(mod\ m)$ and $(c\ ,m) = 1\ ,then\ \ a \equiv b(mod\ m)$	BTL -2	Understanding
15.	If $ac \equiv bc(mod\ m)$ and $(c\ ,m) = d\ ,then\ \ a \equiv b\left(mod\ \frac{m}{d}\right)$	BTL -4	Analyzing
16.	Determine whether the congruence $8x \equiv 10(mod\ 6)$ is solvable	BTL -1	Remembering
17.	Determine whether the congruence $2x \equiv 3(mod\ 4)$ is solvable	BTL -4	Analyzing
18.	Determine whether the congruence $4x \equiv 7(mod\ 5)$ is solvable	BTL -2	Understanding
19.	Determine whether the congruence $8x \equiv 10(mod6)$ is	BTL -4	Analyzing

	solvable		
20.	Using Chinese Remainder theorem, determine whether the linear system is solvable $x \equiv 7(mod\ 9)$, $x \equiv 11(mod\ 12)$	BTL -3	Applying
21.	Using Chinese Remainder theorem, determine whether the linear system is solvable $x \equiv 3(mod\ 6)$, $x \equiv 5(mod\ 8)$	BTL -2	Understanding
22.	Using Chinese Remainder theorem, determine whether the linear system is solvable $x \equiv 2(mod\ 10)$, $x \equiv 7(mod\ 15)$	BTL -4	Analyzing
23.	Define 2x2 linear system	BTL -3	Applying
24.	State Chinese Remainder Theorem	BTL -2	Understanding
25.	Define Congruence and incongruence solution	BTL -4	Analyzing
	PART – B		
1.	Prove that the linear Diophantine equation $ax + by = c$ is solvable if and only if d/c, where $d = (a, b)$. If x_0 and y_0 is a particular solution of the linear Diophantine equation , then all its solutions are given by $x = x_0 + \frac{dt}{d}, y = y_0 - \frac{at}{d}$ where t is an arbitrary integer	BTL -3	Applying
2.(a)	Solve $71x - 50y = 1$	BTL -2	Understanding
2.(b)	Find the remainder when 16^{53} is divided by 7	BTL -5	Evaluating
3.	Solve $1776x + 1976y = 4152$	BTL -3	Applying
4.(a)	Solve $93x - 81y = 3$	BTL -3	Applying
4.(b)	Find the remainder when $(n^2 + n + 41)^2$ is divided by 12	BTL -3	Applying
5.	Find the general solution of the linear Diophantine equation $6x + 8y + 12z = 10$	BTL -3	Applying
6.(a)	Determine if each linear Diophantine equation is solvable $(i)12x + 16y = 18$ $(ii)28x + 91y = 119$, $(iii)1776x + 1976y = 4152$ $(iv)1076x + 2076y = 1155$	BTL -3	Applying
6.(b)	Find the least positive integer that leaves the remainder 3 when divided by 7,4 when divided by 9 and 8 when divided by 11	BTL -3	Applying
7.	Prove that (i) $a \equiv b(modm)$ if and only if $a = b + km$ for some integer k (ii) Prove that the relation $' \equiv '$ (congruence) is an equivalence relation	BTL -1	Remembering
8.(a)	Prove that $a \equiv b(modm)$ iff a and b leave the same remainder when divided by m	BTL -4	Analyzing
8.(b)	Solve $3x + 13y \equiv 8(mod\ 55), 5x + 21y \equiv 34(mod\ 55)$	BTL -3	Applying
9.	Prove that the integer r is the remainder when a is divided by m iff $a \equiv r(modm) where\ 0 \le r < m$	BTL -5	Evaluating
10.(a)	Solve $x \equiv 1(mod\ 3)$, $x \equiv 2(mod\ 5), x \equiv 3(mod\ 7)$	BTL -6	Creating
10.(b)	Solve $x \equiv 1(mod\ 3)$, $x \equiv 2(mod\ 4), x \equiv 3(mod\ 5)$	BTL -3	Applying
11.	Prove that, let $a \equiv b(modm) and\ c \equiv d(modm)$ then $(i) a + c \equiv b + d(modm)$ $(ii) ac \equiv bd(modm)$ (iii) $a^n \equiv b^n(modm)$ for any positive integer n	BTL -4	Analyzing
12.(a)	Solve $2x + 3y \equiv 4(mod\ 13)$, $3x + 4y \equiv 5(mod\ 13)$	BTL -3	Applying
12.(b)	Show that every integer is congruent to exactly one of the least residues $0,1,2, \cdots, (m-1) modulo\ m$	BTL -3	Applying
13.	State and prove Chinese remainder theorem	BTL -4	Analyzing
14.(a)	Verify that whether the number of prime of the form $4n + 3$	BTL -3	Applying

	be expressed as the sum of two squares		
14.(b)	Compute the remainder when 3^{247} is divided by 25	BTL -3	Applying
15.	The linear congruence $ax \equiv b(mod m)$ is solvable if and only if d/b, where $d = (a, m)$. If d/b, then it has d incongruent solutions	BTL -4	Analyzing
16.(a)	Compute the remainder when 5^{31} is divided by 12	BTL -4	Analyzing
16.(b)	Verify that whether the number of integer of the form $8n + 7$ be expressed as the sum of three squares	BTL -3	Applying
17.	If n is any integer then show that $(i) n^2 + n \equiv 0(mod 2)$ $(ii) n^4 + 2n^3 + n^2 \equiv 0(mod 4)$ $(iii) 2n^3 + 3n^2 + n \equiv 0(mod 6)$	BTL -4	Analyzing
18.(a)	Compute the remainder when 23^{1001} is divided by 17	BTL -3	Applying
18.(b)	Find the incongruent solutions of $28x \equiv 119(mod\ 91)$	BTL -3	Applying
	PART – C		
1.	23 weary travelers entered the outskirts of a lush and beautiful forest. They found 63 equal heaps of plantains put together and seven single fruits are divided then equally. Find the number of fruits in each heap	BTL -4	Analyzing
2.	A fruit basket contains apples and oranges. Each apple cost 65 Rs. Each orange cost 45Rs. For a total of 810 Rs. Find the minimum possible numbers of apple in the basket.	BTL -4	Analyzing
3.	If a cock is worth five coins, a hen three coins and three chicks together one coin, how many cocks, hens and chicks, totally 100 can be bought for 100 coins	BTL -2	Understanding
4.	A child has some marbles in a box. If the marbles are grouped in sevens, there will be five left over; If they are grouped in elevens, there will be six left over; If they are grouped in thirteen , eight will be left over; Determine the latest number of marbles in the box	BTL -2	Understanding
5.	Find the least positive integer that leaves the reminder 2 when divided by 5, 4 when divided by 6 and 5 when divided by 11, and 6 when divided by 13	BTL -3	Applying

UNIT V - CLASSICAL THEOREMS AND MULTIPLICATIVE FUNCTIONS

Wilson‘s theorem – Fermat‘s little theorem – Euler‘s theorem – Euler‘s Phi functions – Tau and Sigma functions.

Q.No.	Question	BT Level	Competence
	PART – A		
1.	State Wilsons Theorem	BTL -1	Remembering
2.	State Fermat’s Theorem	BTL -1	Remembering
3.	State Euler’s Theorem	BTL -1	Remembering
4.	Define Euler Phi Function	BTL -2	Understanding
5.	Define Tau Function	BTL -3	Applying
6	Define Sigma Function	BTL -3	Applying
7.	Show that 11 is self invertible.	BTL -2	Understanding
8	Evaluate $\frac{(np)!}{n!\,p^n}$ if n=46, p=5	BTL -2	Understanding
9.	How many primes are there of the form m! + 1 when m≤ 100?	BTL -3	Applying

10	Find the self-invertible least residue modulo each prime 7 & 19	BTL -2	Understanding
11.	Solve $x^2 \equiv 1\ mod(6)$	BTL -4	Analyzing
12.	Find the least residues of $1,2,\dots,p-1\ modulo\ 7$	BTL -3	Applying
13.	Let p be a prime number and a any integer such that $p \nmid a$ then prove that a^{p-2} is an inverse of a modulo p	BTL -4	Analyzing
14.	Evaluate the inverse of 12 modulo 7	BTL -2	Understanding
15.	Solve the linear congruence of 12x ≡ 6 (mod 7)	BTL -4	Analyzing
16.	Solve the linear congruence of 24x ≡ 11 (mod 17)	BTL -1	Remembering
17.	Create $\emptyset\ (11)\ and\ \emptyset(18)$	BTL -4	Analyzing
18.	Solve the linear congruence of 35x ≡ 47 (mod 24)	BTL -2	Understanding
19.	Define Multiplication Theorem	BTL -4	Analyzing
20.	Compute $\emptyset\ (47), \emptyset\ (223), \emptyset\ (7919)$	BTL -3	Applying
21.	Compute $\emptyset\ (15{,}625)$	BTL -2	Understanding
22.	Find the twin primes p and q if $\emptyset\ (pq) = 288$	BTL -4	Analyzing
23.	Compute $\tau(81), \tau(2187)$	BTL -3	Applying
24.	Compute $\tau(1560), \tau(6120)$	BTL -2	Understanding
25.	Compute $\sigma(97), \sigma(36)$	BTL -4	Analyzing
	PART – B		
1.	Prove that a positive integer a is invertible modulo p iff a ≡ ±1 (mod P) and hence prove Wilson's Theorem.	BTL -3	Applying
2.(a)	Find the reminder of 13! When divided by 19	BTL -5	Evaluating
2.(b)	Find the remainder when 7^{1001} is divided by 17	BTL -5	Evaluating
3.	Verify $(p-1)! \equiv -1(modp)$, when p=13 (i)Without using Wilson's theorem (ii)Using Wilson's theorem	BTL -3	Applying
4.(a)	Find the reminder of 17! When divided by 23	BTL -3	Applying
4.(b)	Find the remainder when 24^{1947} is divided by 17	BTL -3	Applying
5.	Let p be a prime and a is any integer such that $p \nmid a$ then prove that the least residues of the integers $a, 2a, 3a, \dots,$ $(p-1)a\ modulo\ p$ are permutation of integers $1,2,3, \dots,$ $p-1$ and use it to prove Fermat's Little Theorem	BTL -3	Applying
6.(a)	If n is a positive integer such that$(n-1)! \equiv -1(modp)$	BTL -3	Applying
6.(b)	Find the remainder when 15^{1976} is divided by 23	BTL -3	Applying
7.	Let p be a prime and a any integer such that $p \nmid a$ then (i)prove that the solution of the linear congruence $ax \equiv b\ (mod\ p)$ is given by $x \equiv a^{p-2}\ b\ (modp)$ (ii) Let p be a prime and a any positive integer then show that $a^p = a\ (mod\ P)$	BTL -1	Remembering
8.(a)	Verify that $\sum_{\frac{d}{n}} \emptyset(d) = n$ for n=28	BTL -4	Analyzing
8.(b)	Find the remainder when 31^{1706} is divided by 23	BTL -3	Applying
9.(a)	State and prove fundamental theorem for multiplicative function	BTL -5	Evaluating
9.(b)	If f is a multiplicative function. Then show that $F(n) = \sum_d F(d)$ is also multiplicative		
10.(a)	Solve the linear congruence $5x \equiv 3(mod24)$	BTL -6	Creating
10.(b)	Let p and q are distinct prime then prove that $p^{q-1} + q^{p-1} \equiv 1modpq)$	BTL -3	Applying
11.	Prove that (i) A positive integer p is prime if and only if $\emptyset(p) = p-1$	BTL -4	Analyzing

	(ii) Let p be a prime and e any positive integer then prove that $\emptyset(p^e) = p^e - p^{e-1}$ (iii) Let $n = {p_1}^{e_1}{p_2}^{e_2}, \dots, {p_k}^{e_k}$ be the canonical decomposition of a positive integer n. Then Prove that $\emptyset(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right), \dots, \left(1-\frac{1}{p_k}\right)$		
12.(a)	Evaluate $\tau\ (n) and\ \sigma\ (n)$ for each $n = 43, 1560, 44982\ \&\ 496$	BTL -3	Applying
12.(b)	Create the remainder when 245^{1040} is divided by 18 and the remainder when 7^{1020} is divided by 15	BTL -6	Creating
13.(a)	Let n be a positive integer with canonical decomposition $n = {p_1}^{e_1}{p_2}^{e_2}, \dots, {p_k}^{e_k}$ then show that $\tau(n) = (e_1+1)(e_2+1), \dots, (e_k+1)$ $\sigma(n) = \frac{{p_1}^{e_1+1}-1}{p_1-1} \cdot \frac{{p_2}^{e_2+1}-1}{p_1-1}, \dots, \frac{{p_k}^{e_1+1}-1}{p_1-1}.$ Also compute $\tau(6120)\ and\ \sigma\ (6120)$.	BTL -4	Analyzing
13.(b)	Let p be a prime and e any positive integer then prove that $\tau(p^e) = e+1\ and\ \sigma\ (p^e) = \frac{p^{e+1}-1}{p-1}$. Also find $\tau(49)$	BTL -3	Applying
14.(a)	State and Prove Euler's Theorem.	BTL -3	Applying
14.(b)	Evaluate the remainder when 199^{2020} is divided by 28 and the remainder when 79^{1776} is divided by 24	BTL -3	Applying
15.	Show that the Euler's φ function is multiplicative function.	BTL -4	Analyzing
16.(a)	Find the remainder when $35^{32} + 51^{24}$ is divisible by 1785	BTL -4	Analyzing
16.(b)	Show that the Tau and Sigma functions are multiplicative function. Also compute $\tau(36)\ and\ \sigma\ (36)$	BTL -3	Applying
17.(a)	Let m be positive integer and a be any integer such that $(a,m) = 1$. Then prove that $a^{\emptyset(m)-1}$ is an inverse of a modulo m	BTL -4	Analyzing
17.(b)	Using Euler's Theorem, evaluate the ones digit in the decimal value of each (i) 17^{666} $(ii) 23^{7777}$	BTL -3	Applying
18.(a)	Let m be a positive integer and a be any integer with $(a,m) = 1$. Then the solution of the linear congruence $ax \equiv b\ (modm)$ is given by $x = a^{\emptyset(m)-1}b(modm)$	BTL -3	Applying
18.(b)	Solve the linear congruence $15x \equiv 7(mod13)$	BTL -3	Applying
PART – C			
1.	Using Fermat's theorem prove the following Let p and q are distinct prime then prove that (i) $p^q + q^p \equiv p + q(modpq)$ (ii)$(a+b)^p \equiv (a^p + b^q)(modp)$	BTL -4	Analyzing
2.	Apply Wilson's theorem to find the reminder of (i) 51! When divided by 91 (ii)67! When divided by71	BTL -3	Applying
3.	Evaluate the linear congruence equations (i)$8x \equiv 3(mod11)$ (ii)$12x \equiv 6(mod7)$ using Fermat's little theorem	BTL -5	Evaluating
4.	Create the reminder of (i)55^{1876} when divided by 12 (ii)25^{2550} when divided by 18	BTL -2	Understanding
5.	Compute (i) $\emptyset(7919), \emptyset(666), \emptyset(1976)$ (ii) $\tau(6491), \tau(2187), \tau(44982)$ (iii)$\sigma(331), \sigma(1024), \sigma(2187)$	BTL -3	Applying