

B.E. / B.Tech. - DEGREE EXAMINATIONS, NOV / DEC 2025
 Third Semester
Computer Science and Engineering (Cyber Security)
20BSMA309 - NUMBER THEORY
 Regulations - 2020

Duration: 3 Hours

Max. Marks: 100

PART - A (MCQ) (10 × 1 = 10 Marks)

Answer ALL Questions

- | | Marks | K-Level | CO |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|---------|-----|
| 1. The prime factorization of 104 is
$2 + 2 + 2 + 13$ (b) $2 \times 2 \times 2 \times 13$
$2 \times 2 \times 1 \times 3$ (d) $2 \times 2 \times 2 \times 3 \times 1$ | 1 | K2 | CO1 |
| 2. The value of $\pi(18.75)$ is
(a) 2,3,5,7,11,13,17 (b) 2,3,5,7,11,15,17
(c) 7 (d) 2,3,5,7,12,13,17 | 1 | K2 | CO1 |
| 3. The linear system of congruences $ax + by \equiv e \pmod{m}$ and $cx + dy \equiv f \pmod{m}$ has unique solution if and only if
(a) $(\Delta, m) = 1, \Delta = (ad - bc) \pmod{m}$. (b) $(\Delta, m) = 1, \Delta = -(ad - bc) \pmod{m}$.
(c) $(\Delta, m) = -1, \Delta = (ad - bc) \pmod{m}$. (d) None of the above | 1 | K1 | CO2 |
| 4. The incongruent solution of the linear congruence $5x \equiv 3 \pmod{6}$ is
(a) $x \equiv 3 \pmod{6}$ (b) $x \equiv 2 \pmod{6}$
(c) $x \equiv 5 \pmod{6}$ (d) $x \equiv 4 \pmod{6}$ | 1 | K2 | CO2 |
| 5. Gauss' Lemma. Let p be an odd prime and a an integer such that p does not divide a . Let γ denote the number of least positive residues of the integers $a, 2a, 3a, \dots, [(p-1)/2]a$ that exceeds $p/2$. Then
(a) $(a/p) = (-1)^\gamma$ (b) $(a/p) = (-1)^{-\gamma}$
(c) $(a/p) = (i)^\gamma$ (d) None of these | 1 | K1 | CO3 |
| 6. The Jacobi symbol is defined by
(a) $(a/m) = \prod_{i=1}^k (a/p_i)^{e_i}$ (b) $(a/m) \neq \prod_{i=1}^k (a/p_i)^{e_i}$
(c) $(a/p) = \prod_{i=1}^k (a/p_i)^{e_i}$ (d) none of these | 1 | K1 | CO3 |
| 7. The sum of four squares of 15795 is
(a) $18^2 + 27^2 + 36^2 + 9^2$ (b) $81^2 + 27^2 + 36^2 + 9^2$
(c) $81^2 + 72^2 + 63^2 - 9^2$ (d) $81^2 + 72^2 + 63^2 + 9^2$ | 1 | K2 | CO4 |
| 8. The linear system of $6x + 8y \equiv 10 \pmod{13}$ and $8x + 10y \equiv 12 \pmod{13}$ is solvable. Then the system has
(a) unique solution (b) infinitely many solution
(c) no solution (d) none of these. | 1 | K2 | CO4 |
| 9. Let m be a positive integer. Then Euler's Phi function $\phi(m)$ denotes
(a) the number of positive integers $\leq m$ and not relatively prime to m .
(b) the number of positive integers $\leq m$ and relatively prime to m .
(c) the number of positive integers $\geq m$ and relatively prime to m .
(d) none of these. | 1 | K1 | CO5 |
| 10. If $n \geq 3$, then $\phi(n)$
(a) is even (b) odd (c) prime (d) None of these. | 1 | K2 | CO5 |

PART - B (12 × 2 = 24 Marks)

Answer ALL Questions

- | | | | |
|--------------------------------------------------------------------------------|---|----|-----|
| 11. Write the division algorithm. | 2 | K1 | CO1 |
| 12. Represent 15036 in hexadecimal system. | 2 | K2 | CO1 |
| 13. Find the number of positive integers ≤ 2076 that are divisible by 19. | 2 | K2 | CO1 |

- | | | | |
|------------------------------------------------------------------|---|----|-----|
| 14. State any two properties of congruence relation. | 2 | K1 | CO2 |
| 15. Write the working procedure for Chenise Remainder Theorem. | 2 | K1 | CO2 |
| 16. Find the least residue of (i) 23 modulo 5, (ii) -3 modulo 5. | 2 | K2 | CO2 |
| 17. Define Legendre Symbol and give an example. | 2 | K1 | CO3 |
| 18. Write the relation between (p/q) and (q/p) . | 2 | K2 | CO3 |
| 19. Examine whether the LDE $12x + 16y = 18$ is solvable or not. | 2 | K2 | CO4 |
| 20. Express the prime 197 as the sum of four squares. | 2 | K2 | CO4 |
| 21. Define Euler Phi Function. | 2 | K1 | CO5 |
| 22. Show that 11 is self-invertible. | 2 | K1 | CO5 |

PART - C (6 × 11 = 66 Marks)

Answer ALL Questions

- | | | | | |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|----|-----|
| 23. a) | From the pattern, write down the n^{th} row and prove the validity of the number pattern.
$1.9 + 2 = 11$
$12.9 + 3 = 111$
$123.9 + 4 = 1111$
$1234.9 + 5 = 11111$ and so on. | 11 | K3 | CO1 |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|----|-----|

OR

- | | | | | |
|--------|----------------------------------------------------------------------------------------|---|----|-----|
| b) (i) | Prove that the product of any two integers of the form $4n + 1$ is also the same form. | 6 | K3 | CO1 |
| (ii) | Use recursion to find [24,28,36,40]. | 5 | K3 | CO1 |

- | | | | | |
|--------|---------------------------------------------------------------------------------------------------------|----|----|-----|
| 24. a) | Solve the linear system of congruences :
$3x + 4y \equiv 5 \pmod{7}$; $4x + 5y \equiv 6 \pmod{7}$. | 11 | K3 | CO2 |
|--------|---------------------------------------------------------------------------------------------------------|----|----|-----|

OR

- | | | | | |
|----|-------------------------------------------------------------------------------------------------------------------------|----|----|-----|
| b) | Solve the system $x \equiv 1 \pmod{3}$, $x \equiv 2 \pmod{4}$, $x \equiv 3 \pmod{5}$ using Chinese Remainder Theorem. | 11 | K3 | CO2 |
|----|-------------------------------------------------------------------------------------------------------------------------|----|----|-----|

- | | | | | |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|----|-----|
| 25. a) | If f is a number theoretic function which is multiplicative and for any positive integer n , then prove that function $F(n) = \sum_{(d n)} f(d)$ is also multiplicative. | 11 | K3 | CO3 |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|----|-----|

OR

- | | | | | |
|----|-----------------------------------------------|----|----|-----|
| b) | State and prove Law of Quadratic Reciprocity. | 11 | K3 | CO3 |
|----|-----------------------------------------------|----|----|-----|

- | | | | | |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|----|----|-----|
| 26. a) | If cock is worth five coins, a hen three coins and three chicks together one coin, how many cocks, hence and chicks, totaling 100, can be bought for 100 coins? | 11 | K3 | CO4 |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|----|----|-----|

OR

- | | | | | |
|----|-------------------------------------------------------------------------------------------------------|----|----|-----|
| b) | Determine if the linear Diophantine Equation $12x + 18y = 30$ is solvable. If so, find the solutions. | 11 | K3 | CO4 |
|----|-------------------------------------------------------------------------------------------------------|----|----|-----|

- | | | | | |
|--------|-----------------------------------------------------------------------------------------------------------------|----|----|-----|
| 27. a) | Using Euler's Theorem, evaluate the ones digit in the decimal value of each
(i) 17^{666} (ii) 23^{777} . | 11 | K3 | CO5 |
|--------|-----------------------------------------------------------------------------------------------------------------|----|----|-----|

OR

- | | | | | |
|--------|-------------------------------------------------------|---|----|-----|
| b) (i) | State and Prove Fermat's Little Theorem. | 6 | K3 | CO5 |
| (ii) | Find the remainder when 15^{1976} is divided by 23. | 5 | K3 | CO5 |

- | | | | | |
|------------|-------------------------------------------------------------------------------------------------|---|----|-----|
| 28. a) (i) | Prove that the product of the sums of four squares can be expressed as the sum of four squares. | 6 | K3 | CO4 |
|------------|-------------------------------------------------------------------------------------------------|---|----|-----|

- | | | | | |
|------|---------------------------------------------------------------------------------------------------------------------|---|----|-----|
| (ii) | Let p be a prime and e any positive integer, prove that $\phi(p^e) = p^e - p^{e-1}$. Hence find $\phi(6125)$. | 5 | K3 | CO5 |
|------|---------------------------------------------------------------------------------------------------------------------|---|----|-----|

OR

- | | | | | |
|----|---------------------------------------------------------------------------------------------|----|----|-----|
| b) | Show that the Euler's ϕ function is multiplicative function. Hence find $\phi(1976)$. | 11 | K3 | CO5 |
|----|---------------------------------------------------------------------------------------------|----|----|-----|

