Reg. No.																

Question Paper Code	12841

B.E. / B.Tech. - DEGREE EXAMINATIONS, APRIL / MAY 2024

Third Semester

Computer Science and Engineering (Cyber Security)

20BSMA309 - NUMBER THEORY

Regulations - 2020

Duration: 3 Hours | Max. Marks: 100

PART - A ($10 \times 2 = 20$ Marks)

Answer ALL Questions

	Question	Marks	K – Level	CO
1.	Express $(10110)_2$ in base 10 and express $(1076)_{10}$ in base two.	2	K1	CO1
2.	Find the six consecutive integers that are composite.	2	K1	CO1
3.	Determine whether the congruence $8x \equiv 10(mod\ 6)$ is solvable.	2	K2	CO2
4.	How many solutions are there for $5x^2 + 10x + 15 \equiv 0(mod5)$?	2	K2	CO2
5.	What are quadratic residues? Give examples.	2	K1	CO3
6.	Define the Jacobi symbol.	2	K1	CO3
7.	Discuss whether $6x + 8y = 25$ is solvable.	2	K1	CO4
8.	Express 169 as the sum of four squares.	2	K2	CO4
9.	Show that 11 is self-invertible.	2	K2	CO5
10.	Find $\emptyset\,(11)\ \ and\ \ \emptyset(18)$.	2	K2	CO5

PART - B ($5 \times 16 = 80$ Marks)

Answer ALL Questions

		Question	Marks	K – Level	CO
11.	a)	State and prove Fundamental Theorem of Arithmetic.	16	K2	CO1
		OR			
	b) i)	Prove that there are infinitely many primes.	8	K2	CO1
	ii)	Use Euclidean algorithm to find the GCD of (2076, 1776). Also express the GCD as a linear combination of the given numbers.	8	K2	CO1
12.	a) i)	Find the roots of the congruence . $x^2 \equiv 43(\mathrm{mod}\, 97)$.	8	K3	CO2
	ii)	Reduce the congruence $4x^2 + 2x + 1 \equiv 0(\mathrm{mod}\, p)$ to the form $x^2 \equiv a(\mathrm{mod}\, p)$.	8	K3	CO2
		OR			
	b) i)	Solve $x^2 + x + 7(\mathrm{mod}\, 81)$.	8	K3	CO2
	ii)	Prove that the congruence $f(x) \equiv 0(\mathrm{mod}\, p)$ of degree n has at most n solutions.	8	K3	CO2

13.	a) i) Determine whether 7411 is a residue modulo the prime 9283.	8	K3	CO3
	ii) List the quadratic residues of each of the primes 7, 13, 17, 29.	8	K3	CO3
	OR			
	b) i) Evaluate: $\left(\frac{-23}{83}\right), \left(\frac{51}{71}\right), \left(\frac{71}{73}\right)$	8	K3	CO3
	ii) Prove that $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$	8	K3	CO3
14.	a) Prove that a positive integer n is properly representable as a sum of two squares if and only if the prime factors of n are all of the form 4k + 1, except for the prime 2, which may occur to at most the first power.	16	K4	CO4
	OR			
	b) State and prove Chinese remainder theorem.	16	K3	CO4
15.	a) i) Evaluate $\tau(n)$ and $\sigma(n)$ for each $n = 43, 1560, 44982$ and 496	8	K4	CO5
	ii) Find the remainder when 15^{1976} is divided by 23.	8	K4	CO5
	OR			
	b) i) Let $n = p_1^{e_1} p_2^{e_2}, \ldots, p_k^{e_k}$ be the canonical decomposition of a positive integer n. Then Prove that $\emptyset(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right), \ldots, \left(1-\frac{1}{p_k}\right)$	8	K4	CO5
	ii) State and prove Wilson's Theorem.	8	K4	CO5