H1 **02000CST292062201** **Pages: 2**

Reg No.:_____ Name:_____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

Fourth Semester B.Tech (Honours) Degree Examination June 2023 (2021 Admission)

Course Code: CST292

Course Name: Number Theory

Max. Marks: 100 Duration: 3 Hours

PART A

(Answer all questions; each question carries 3 marks) Marks

1		State the principle of well ordering.	3
2		Apply Euclidean Algorithm to compute the GCD of (270,192).	3
3		Define Fermat prime and Mersenne prime with example.	3
4		Use Fermat's little theorem to find: 29^{25} mod 11.	3
5		Outline the concept of Carmichael number. Give an example.	3
6		List out the applications of primitive roots.	3
7		Define Mobius inversion formula.	3
8		Define quadratic residues and non-residues modulo a prime p. Find all quadratic residues modulo 11.	3
9		Explain the theorem for sum of two squares and sum of three squares.	3
10		State Pell's equation.	3

PART B

(Answer one full question from each module, each question carries 14 marks)

Module -1

11	a)	Summarize the properties of Modulo arithmetic and Modulo operator.	7
	b)	Apply Euclidean algorithm to find out the GCD(1492,1066) and express it in terms of Bezout's identity.	7
12	a)	Find all the solutions of 5x+3y=4, using Linear Diophantine equations.	7
	b)	State the relationship between GCD, LCM and product of two numbers a and b. Use it to find the LCM of [1050,2574]	7

Module -2

13	a)	Use Chinese Reminder Theorem to solve the simultaneous congruence: $x\equiv6 \pmod{11}$, $x\equiv13 \pmod{16}$, $x\equiv9 \pmod{21}$, $x\equiv19 \pmod{25}$	9
	b)	State Wilson's Theorem. Compute the value of (97!) mod 101 using Wilson's theorem.	5
14	a)	Explain the concept of Fermat's factorization theorem and use it to factorize the number 5959	7

b) State Fermat's Little theorem. Show how computations can be simplified using Fermat's Little theorem by computing the value of 2^{35} mod 7. 7

Module -3

15 a) With the aid of a figure, explain the concept of Symmetric key Encryption. Also mention it pros and cons. 10

b) What are the challenges faced in public key crypto systems? 4

16 a) When can we say that an integer n is a pseudoprime? Check whether the number 341 is pseudo prime number. 6

b) Explain Euler Totient function with example. What is the value of $\phi(n)$ when n is a composite number and use it to compute (i)ϕ (240) (ii) ϕ (49). 8

Module -4

17 a) State the generalised law of Quadratic reciprocity and hence evaluate the Jacobi symbol $\left(\frac{221}{399}\right)$ 8

b) Prove that 45 is not a quadratic residue modulo of 47. 6

18 a) State and prove the properties of Legendre Symbol. 6

b) Find the following values of the Legendre symbols: (113/127), (113/131), (113/137), (210/229) 8

Module -5

19 a) Express 28 as a sum of four squares. 6

b) Apply the theorem of Gaussian Integer unique factorization for the numbers 45 and 65 to count in how many different ways can it be written as a sum of two squares? 8

20 a) Using the theory of Pell's equation and understanding the fact that, $3+2\sqrt{2}$ yields the least solution of $x^2 - 2y^2 = 1$, explaining the method illustrate how to find the two new solutions for the same. 8

b) Express $\sqrt{13}$ as an infinite simple continued fraction. 6

*****