Reg No.:_____ Name:_____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

Fourth Semester B.Tech (Hons) Degree Examination July 2021 (2019 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 Well ordering Principle.	3
2		Apply the Euclidean algorithm to find gcd(4076, 1024).	3
3		Define Mersenne primes with an example.	3
4		Show that $2^{314} \equiv 2(mod\ 341)$	3
5		Verify that 2 is a primitive root modulo 9.	3
6		Explain Euler Totient function with example	3
7		Define Jacobi symbol	3
8		State the law of quadratic reciprocity	3
9		Define Pell's equation.	3
10		Show that 23 cannot be represented as a sum of two squares.	3

PART B

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

Module - 1

11	a)	Explain Extended Euclidean algorithm.	7
	b)	Find gcd(1914,899) using Euclidean algorithm and express in terms of Bezout's identity (ax+by=d).	7

OR

12	a)	Let a,b and c be integers with a≠0 and b≠0. Prove that If a|b and b|c then a|c.	7
	b)	Describe the properties of modular arithmetic and modulo operator.	7

Module - 2

13	a)	Let P be a prime and 'a' any positive integers. Then prove that $a^p \equiv a(mod p)$	7
	b)	Find all the solutions of 24x + 34y = 6.	7

OR

14 a) Define Fermat primes. Show that any two distinct Fermat numbers are Relatively prime. 7

b) Explain Chinese remainder theorem and solve the system of congruences, 7
$x \equiv 2(\text{mod}3)$, $x \equiv 3(\text{mod}5)$, $x \equiv 2(\text{mod}7)$

Module - 3

15 a) If m is relatively prime to n, show that $\Phi(mn) = \Phi(m)\Phi(n)$. 7

b) Distinguish between public key encryption and private key encryption techniques. Also mention merits and demerits of both. 7

OR

16 a) Let a be a positive integer such that (a,m) = 1 and $ord_m a = e$. Then prove that $a^n \equiv 1 \pmod{m}$ if and only if e|n. 7

b) Define Carmichael number and show that a 561 is a Carmichael number. 7

Module - 4

17 a) State and prove properties of Legendre's symbol. 7

b) Define Quadratic Residue and find the quadratic residue and non-residue of modulo 13. 7

OR

18 a) Define Mobius function. Prove that the function 'μ' is multiplicative. 7

b) Solve the quadratic congruence $2x^2 + 3x + 1 \equiv 0(mod7)$ 7

Module -5

19 a) Show that sums of two squares is closed under multiplication and express the product (13*7) as the sums of two squares. 7

b) Solve the Pell's equation $x^2 - 2y^2 = 1$ 7

OR

20 a) Express $\frac{227}{157}$ as a finite simple continued fraction. 7

b) Show that Gaussian integers is closed under addition, subtraction and multiplication 7

*****