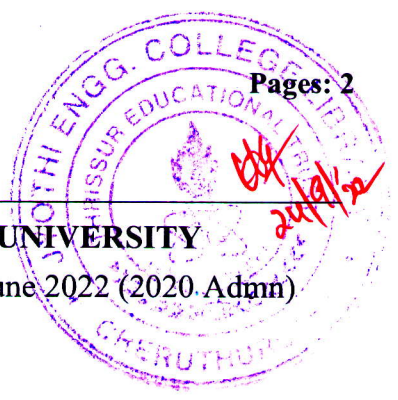


Reg No.: _____

Name: _____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

Fourth Semester B.Tech (Hons) Degree Examination June 2022 (2020 Admn)

**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 | Show that Z_2 forms a field | (3) |
| 2 | Find LCM of 1240 and 5300 using GCD | (3) |
| 3 | Define Fermat and Mersenne primes with example. | (3) |
| 4 | Solve the congruence equation $17X \equiv 3 \pmod{29}$ | (3) |
| 5 | Define Carmichael Number and use the definition to show that 561 is a Carmichael number | (3) |
| 6 | Define Euler's Totient function $\phi(n)$ and using prime factorization compute $\phi(60)$. | (3) |
| 7 | Describe Dirichlet product and its properties. | (3) |
| 8 | Compute $\left(\frac{31}{103}\right)$ | (3) |
| 9 | Express 180 as a sum of two squares. | (3) |
| 10 | Find a continued fraction expansion for $\frac{47}{17}$ | (3) |

PART B*(Answer one full question from each module, each question carries 14 marks)***Module -1**

- 11 a) Find gcd of $a=299$ and $b=221$ and express d as $ax + by$ where x and y are integers. (7)
- b) State and prove division algorithm. (7)

OR

- 12 a) Describe the properties of modular arithmetic and congruence. (7)
- b) Explain Extended Euclidean algorithm. Find the multiplicative inverse of 23 mod 100. (7)

Module -2

- 13 a) Recall the use of Miller -Rabin Test for Primality. Check whether 561 is prime or composite. (7)
- b) Find the remainder when $18!$ is divided by 23 (7)

OR

- 14 a) Explain fermat's factorization method and use it to factor 5959. (7)
- b) Solve the system of congruences using Chinese remainder theorem, (7)
- $$x \equiv 2 \pmod{3}, x \equiv 5 \pmod{4}, x \equiv -3 \pmod{7}$$

Module -3

- 15 a) Define a pseudo prime. Show that 561 is an absolute pseudoprime. (7)
- b) Solve the polynomial power congruence $x^3 + 4x \equiv 4 \pmod{343}$ (hint: $343=7^3$) (7)

OR

- 16 a) Explain Set of Units U_n in $\mathbb{Z}_n$ with example. Determine if 5 is a primitive root of 107. (8)
- b) Differentiate public key encryption from private key encryption. (6)

Module -4

- 17 a) Define Quadratic Residues. Find quadratic residues of 11 (7)
- b) Outline the Quadratic law of reciprocity for Jacobi symbols. (7)

OR

- 18 a) Illustrate that Mobius function is a multiplicative function. (7)
- b) State and prove properties of Legendre's symbol. (7)

Module -5

- 19 a) State and prove Legendre's Three-Square theorem. (7)
- b) Define a Gaussian integer. Factorize the Gaussian integer $(-19 + 43i)$ (7)

OR

- 20 a) State and prove Fermat's Theorem on the Sum of Two Squares (7)
- b) Define Infinite continued fraction. Compute c_4 for $[1,2,1,2,1]$ (7)
