Register No.: …… Name: ……..

SAINTGITS COLLEGE OF ENGINEERING (AUTONOMOUS)

(AFFILIATED TO APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY, THIRUVANANTHAPURAM)

FOURTH SEMESTER B.TECH DEGREE EXAMINATION (Regular), JULY 2022

(2020 SCHEME)

Course Code : **20CST292**

Course Name: **Number Theory**

Max. Marks : **100** **Duration: 3 Hours**

PART A

(Answer all questions. Each question carries 3 marks)

1. Find gcd (401,700) using Euclid's algorithm.
2. Find the 7- bit word that is represented by the polynomial $x^5+ x^3 +x^2 +1$ in GF(2^7)
3. Define Fermat's theorem. Prove the theorem.
4. Solve the congruence equation $14 x \equiv 12 \pmod{18}$
5. Find the result of 6^{29} mod 35.
6. Verify that 3 is a primitive root modulo 7.
7. Define Dirichlet Product.
8. Define Jacobi Symbol with example.
9. Define Pell's equation.
10. Express 221 as a sum of squares.

PART B

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

MODULE I

11. a) For the group G = $< Z_8^*, x>$, prove that it is an Abelian group. Also show the result of 5 x 7 and 7 ÷ 5. (7)

    b) Solve the linear Diophantine equation 40 x + 16 y =88. (7)

OR

12. a) Describe the properties of modular arithmetic and modulo operator (7)

    b) Explain Extended Euclid's algorithm. Using the algorithm find out the multiplicative inverse of 23 in Z_{100}. (7)

MODULE II

13. a) State Fermat Test. Prove that 17 is prime using Fermat Test. (6)

    b) Write down the pseudo code for Fermat factorization method and factorize N= 5959. (8)

OR

14. a) Find an integer that has a remainder of 2 when divided by 3 and 7, and has a remainder of 3 when divided by 5. (7)

b) Use the Pollard p − 1 method to find a factor of 299 with the bound B = 5. Write down the pseudo code also. (7)

MODULE III

15. a) Define Euler's totient function. Prove that, Ø(pq)=(p-1)(q-1) where p and q are prime numbers. (6)

b) Find i) Ø(29) ii) Ø(32) iii) Ø(80) iv) Ø(100) (8)

OR

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

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

MODULE IV

17. a) Define Legendre Symbol with example. List the properties. (6)

b) Define Quadratic Residue and Non-residue and-find the quadratic residue and non-residue of modulo 11. (8)

OR

18. a) Define Mobius Function with examples. List out any two properties of Mobius Function. (6)

b) Solve the quadratic equations i) $x^2 \equiv 3 \pmod{23}$ ii) $x^2 \equiv 7 \pmod{19}$. (8)

MODULE V

19. a) Find all the solutions of the Diophantine equation $x^2 - 6y^2 = 1$. (7)

b) Define a finite continued fraction. Express − 65 /23 as a finite continued fraction. (7)

OR

20. a) Show that every prime of the form 4k+3 cannot be represented as the sum of two squares with example. (6)

b) Define a Gaussian integer. Factorize the Gaussian integer 440 − 55i. (8)

****