H **921A2** Total Pages: **2**

Register No.: .... Name: ....

SAINTGITS COLLEGE OF ENGINEERING (AUTONOMOUS)

(AFFILIATED TO APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY, THIRUVANANTHAPURAM)

FOURTH SEMESTER B.TECH DEGREE EXAMINATION (R), MAY 2023

(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. State and prove Well Ordering principle.
2. Find gcd (2322,654) using Euclid's algorithm.
3. Solve the linear congruence equation 12 x ≡ 48 (mod 18).
4. Use Fermat's Little theorem to show that 91 is not a prime.
5. Find the value of
   a. Ø(29) b. Ø(32)
6. Calculate 4^{99} (mod 35).
7. Define Dirichlet Product.
8. Define Jacobi Symbol with example.
9. Define Pell's equation
10. Show that 23 cannot be represented as a sum of two squares.

PART B

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

MODULE I

11. a) State Euclidean Theorem and its extension. Express gcd (252,198) as a linear combination of 252 and 198 (8)

    b) Prove that for a positive integer m, if a ≡ b (mod m) and c ≡ d (mod m) then a+c ≡ b+d (mod m) and ac ≡ bd (mod m) (6)

OR

12. a) Determine all solutions in the positive integers for the given Diophantine equation 172 x +20 y =1000 (9)

    b) Define (5)
       a. Group
       b. Field

MODULE II

13. a) Explain Fermat's factorization algorithm and use this algorithm to factorize 809009. (8)

b) State and prove Fermat's theorem. (6)

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. (8)

b) Prove if a ≡ b (mod n) and b ≡ c (mod n) then a ≡ c mod n) (6)

MODULE III

15. a) Define Carmichael number and show that a 561 is a Carmichael number (5)

b) Distinguish between public key encryption and private key encryption techniques. Also mention merits and demerits of both. (9)

OR

16. a) Find the unit digit of 3^{100} by means of Euler's theorem. (7)

b) Check there exists primitive roots for G=<Z_7^* , X>. (7)

MODULE IV

17. a) Define Quadratic Residue and find the quadratic residue and non-residue of modulo 13. (8)

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

OR

18. a) Define Mobius function and prove Mobius function is a multiplicative. (5)

b) Solve the quadratic congruence equation (9)

a. $y^2 \equiv 10$ (mod 13)

b. $x^2 - 5$ x + 6 ≡ 0 (mod 11)

c. x^2 + 8x + 6 ≡ 0 (mod 13)

MODULE V

19. a) Solve the Pell's equation x^2 - $6y^2$ = 1. (7)

b) Define a finite continued fraction. Express 89 /37 as a finite continued fraction. (7)

OR

20. a) Show that Gaussian integers is closed under addition, subtraction and multiplication. (7)

b) If m and n can be expressed as sum of four squares, then show that mn can also be expressed the sum of four squares. (7)

****