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

SAINTGITS COLLEGE OF ENGINEERING (AUTONOMOUS)

(AFFILIATED TO APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY, THIRUVANANTHAPURAM)

FOURTH SEMESTER B.TECH DEGREE EXAMINATION (R), MAY 2024

(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. Define Bezout's identity with example.
2. Apply Euclid's algorithm to find GCD (2740, 1760).
3. Is 127 a Mersenne prime? Justify.
4. Solve $4^{532} \pmod{11}$ using Fermat's little theorem.
5. $5^i \pmod{13} = 8$. Determine i.
6. What are the three security goals?
7. Define the Legendre symbol with an example.
8. Show that $\sigma(n) = \sigma(n + 1)$ for n = 206.
9. Express 2104 as sum of three squares.
10. Every prime of the form 4k+1 can be represented uniquely as the sum of two squares. Justify.

PART B

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

MODULE I

11. a) Prove that if a|b and c|d then ac|bd. (5)
    b) Find general solutions of the Diophantine equation $1485x + 1745y = 15$. (9)

OR

12. a) Describe the properties of modular arithmetic. (5)
    b) Find the multiplicative inverse of 550 mod 1769 by applying extended Euclidean algorithm. (9)

MODULE II

13. a) Solve the linear congruence $14x \equiv 30 \pmod{100}$. (6)
    b) Explain Fermat's primality testing and factorization method with example. (8)

OR

14. a) Applying Wilson' theorem, prove that (13-1)! ≡ -1 (mod 13). (5)
    b) Explain Chinese remainder theorem and solve the system of congruences x ≡ 2(mod3), x ≡ 3(mod5), x ≡ 2(mod7). (9)

MODULE III

15. a) Show that $2^{341} \equiv 2 \pmod{341}$ (5)
    b) What are Carmichael numbers? Show that 1729 is a Carmichael number. (9)

OR

16. a) Find the last two decimal digits of 3^{256}. (6)
    b) Differentiate between symmetric and asymmetric encryption techniques. (8)

MODULE IV

17. a) Define quadratic residue. Determine the quadratic residues and non-residues of modulo 11. (7)
    b) Solve the quadratic congruence $2x^2 + 3x + 1 \equiv 0 \pmod{7}$ (7)

OR

18. a) Define Dirichlet product with an example. Describe its properties. (7)
    b) Verify that $\tau(n) = \tau(n + 1) = \tau(n + 2) = \tau(n + 3)$ holds for $n = 4503$. (7)

MODULE V

19. a) Show that sums of two squares is closed under multiplication. Express the product (13*17) as the sums of two squares. (7)
    b) Define Gaussian integers. Factorize the Gaussian integer $440 - 55i$. (7)

OR

20. a) Define Pell's equation. Solve the Pell's equation $x^2 - 2y^2 = 1$. (7)
    b) Express $\frac{227}{157}$ as a finite simple continued fraction. (7)

****