H 678A1 Total Pages: 2

Dogiston No.	Mamai	
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(2⁷)
- 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 $G = \langle Z_8^*, x \rangle$, prove that it is an Abelian group. Also show the result of 5 x 7 and $7 \div 5$.
 - b) Solve the linear Diophantine equation $40 \times 16 y = 88$.

OR

(7)

(7)

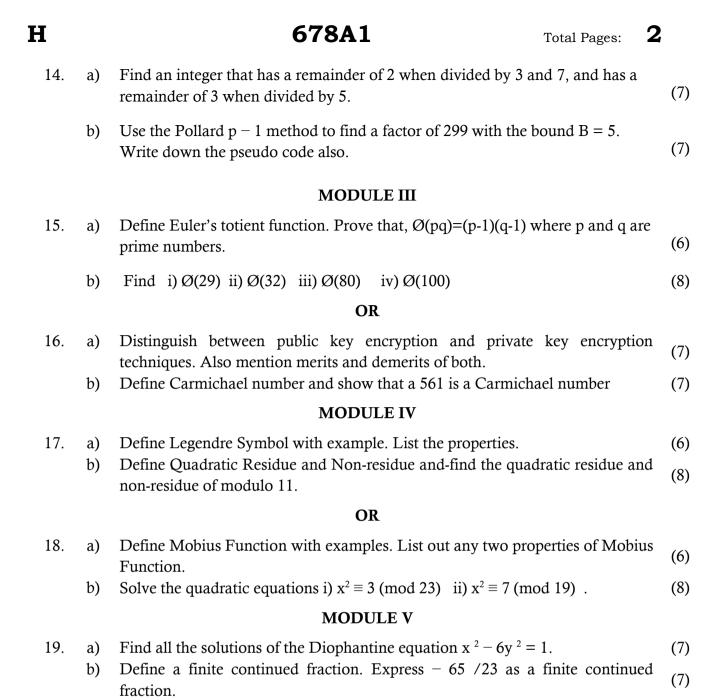
(8)

- 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} .

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.

OR



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

20.

a)

b)

Define a Gaussian integer. Factorize the Gaussian integer 440 – 55i.

OR

(6)

(8)