

Enrolment No./Seat No _____

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER-IV (NEW) EXAMINATION – SUMMER 2024

Subject Code:3144803

Date:03-07-2024

Subject Name: Number Theory

Time:10:30 AM TO 01:00 PM

Total Marks:70

Instructions:

1. Attempt all questions.
2. Make suitable assumptions wherever necessary.
3. Figures to the right indicate full marks.
4. Simple and non-programmable scientific calculators are allowed.

		Marks
Q.1	(a) What are Mersenne numbers? Explain with example.	03
	(b) Find out multiplicative Inverse of 550 in GF (1579)	04
	(c) State and prove Wilson's Theorem and its converse.	07
Q.2	(a) Find the GCF of 67 and 194 using the prime factorisation method.	03
	(b) Find the GCD of (2740,1760) using Euclid's Algorithm.	04
	(c) Prove that the linear Diophantine equation: $ax + by = c$ has a solution iff $d c$, where a , b and c be given integer with a and b not both zero, and $d = (a,b)$. Also, if (x_0, y_0) is one solution of this equation, then show that all the solution are given by $x = x_0 + (b/d)t$, $y = y_0 - (a/d)t$, $t = 0, \pm 1, \pm 2, \dots$	07
	OR	
	(c) Determine all solutions in the positive integers of the following Diophantine equation $158x - 57y = 7$.	07
Q.3	(a) Find all the primitive root of 17.	03
	(b) Explain Fermat - Kraitchik Factorization Method.	04
	(c) Explain Knapsack Cryptosystem.	07
	OR	
Q.3	(a) What is primitive root? Is 5 a primitive root of 13?	03
	(b) Define Euler's phi-function. Find the value of $\phi(180)$.	04
	(c) Explain Euler's solvability criterion with one example. Also write down Mobius inversion formula.	07
Q.4	(a) What is Caesar Cipher? Why it is easy to crack cipher generated through this method?	03
	(b) Find the remainder when 250 is divisible by 7	04
	(c) Solve the system of congruences $x \equiv 5 \pmod{11}$ $x \equiv 4 \pmod{29}$ $x \equiv 15 \pmod{31}$	07
	OR	
Q.4	(a) Evaluate Legendre Symbol: $(19/23)$	03
	(b) What is complete residue system? State Fermat's little theorem.	04
	(c) State Chinese Remainder theorem and find the value of X for the given set of congruent equations using Chinese Remainder theorem. $X \equiv 1 \pmod{5}$ $X \equiv 2 \pmod{7}$ $X \equiv 3 \pmod{9}$ $X \equiv 4 \pmod{11}$	07

- Q.5** (a) Explain Asymmetric key Encryption with Private Key. **03**
(b) State and prove Quadratic Reciprocity Law. **04**
(c) For $p = 11$ and $q = 19$ and choose $d = 17$. Apply RSA algorithm where Cipher message = 80 and thus find the plain text. **07**

OR

- Q.5** (a) Explain Asymmetric key Encryption with Public Key. **03**
(b) What is Jacobi symbol? State and explain its properties. **04**
(c) P and Q are two prime numbers. $P=7$, and $Q=17$. Take public key $E=5$. If plain text value is 10, then what will be cipher text value according to RSA algorithm? **07**
