Enrollment No: ______________________ **Exam Seat No:** ______________________

C. U. SHAH UNIVERSITY

Winter Examination-2022

Subject Name: Number Theory

Subject Code: 5SC04NUT1 **Branch: M.Sc. (Mathematics)**

Semester: 4 **Date: 21/09/2022** **Time: 02:30 To 05:30** **Marks: 70**

Instructions:

(1) Use of Programmable calculator and any other electronic instrument is prohibited.
(2) Instructions written on main answer book are strictly to be obeyed.
(3) Draw neat diagrams and figures (if necessary) at right places.
(4) Assume suitable data if needed.

SECTION – I

Q-1 **Attempt the following questions.** **(07)**

a. Calculate $\phi(16)$.
b. Check whether 28 is a perfect number or not.
c. If $n = 18$, then find $\tau(n)$.
d. Findlcm(a, b) if $a = 2^2 \cdot 3^1 \cdot 5^0,\ b = 2^1 \cdot 3^1 \cdot 5^1$.
e. Ifgcd$(a, n) = 1$, then the linear congruence $ax \equiv b\ (mod\ n)$ has a unique solution modulo n. (True/False)
f. If $ca \equiv cb\ (mod\ n)$ andgcd$(c, n) = 1$, then $a \equiv b\ (mod\ n)$. (True/False)
g. If p is a prime and $p|ab$, then $p|a$ or $p|b$. (True/False)

Q-2 **Attempt all questions.** **(14)**

A. State Chinese remainder theorem. Solve the system of three congruence **06**
$$x \equiv 1(mod\ 3), x \equiv 2(mod\ 5), x \equiv 3(mod\ 7).$$
B. Prove that given integers a and b, with $b > 0$, there exist unique integers q and r satisfying $a = qb + r,\ \ 0 \le r < b$. **06**
C. If $a \equiv b\ (mod\ n)$ and $c \equiv d\ (mod\ n)$, then show that $a + c \equiv b + d\ (mod\ n)$. **02**

OR

Q-2 **Attempt all questions.** **(14)**

A. Prove that every positive integer greater than one can be express uniquely as a product of prime, up to the order of the factor. **06**
B. In usual notations, prove that lcm(a, b) gcd$(a, b) = ab$. **06**
C. If $a \equiv b\ (mod\ n)$ and $c \equiv d\ (mod\ n)$, then show that $ac \equiv bd\ (mod\ n)$. **02**

Q-3 **Attempt all questions.** **(14)**

- **A.** Define: Mobious function. Show that Mobious function is multiplicative. **04**
- **B.** State and prove Euclid's lemma. **04**
- **C.** Prove that if $k > 0$, then $\gcd(ka, kb) = k\gcd(a, b)$. **03**
- **D.** Find the highest power of 3 dividing 1000!. **03**

OR

Q-3 **Attempt all questions.** **(14)**

- **A.** Show that the functions τ and σ are both multiplicative functions. **04**
- **B.** Compute $\gcd(26,118)$ and express it in the form $26x + 118y$, where $x, y \in \mathbb{Z}$. **04**
- **C.** Show that $\left[\frac{[x]}{n}\right] = \left[\frac{x}{n}\right]$ if n is a positive integer. **03**
- **D.** Prove that 41 divides $2^{20} - 1$. **03**

SECTION – II

Q-4 **Attempt the following questions.** **(07)**

- **a.** Find two primitive roots of 10.
- **b.** Write Pell's equation.
- **c.** Define: Periodic continued fraction.
- **d.** Every Euclidean quadratic field has unique factorization property. (True/False)
- **e.** If $n \geq 1$ and $\gcd(a, n) \neq 1$, then $a^{\phi(n)} \equiv 1 \ (mod\ n)$. (True/False)
- **f.** A linear Diophantine equation $12x + 8y = 199$ has no solution. (True/False)
- **g.** Define: Algebraic number.

Q-5 **Attempt all questions.** **(14)**

- **A.** Express the rational number $\frac{19}{51}$ in finite simple continue fraction. **02**
- **B.** Solve the linear Diophantine equation $525\,x + 231y = 42$. **05**
- **C.** State and prove Wilson's theorem. **07**

OR

Q-5 **Attempt all questions.** **(14)**

- **A.** Find first three positive solution of the equation $x^2 - 7y^2 = 1$. **07**
- **B.** State and prove Lagrange's theorem. **07**

Q-6 **Attempt all questions.** **(14)**

- **A.** Find order of 2 modulo 7. **02**
- **B.** Compute the convergents of the simple continued fraction $[1; 2,3,3,2,1]$. **05**
- **C.** Determine the infinite continued fraction representation of irrational number $\sqrt{23}$. **07**

OR

Q-6 **Attempt all questions.** **(14)**

- **A.** Find a primitive root modulo 4. **02**
- **B.** Determine the unique irrational number represented by the infinite continued fraction $x = [3; 6, \overline{1,4}]$. **05**
- **C.** State and prove the Fermat's last theorem. **07**