Roll No. [ ] **Total No. of Pages : 02**

Total No. of Questions : 07

B.Sc. (CS) (Sem.–4)

NUMBER THEORY

Subject Code : BCS-401

M.Code : 72317

Date of Examination : 05-07-22

Time : 3 Hrs. **Max. Marks : 60**

INSTRUCTIONS TO CANDIDATES :

1. **SECTION-A is COMPULSORY consisting of TEN questions carrying TWO marks each.**
2. **SECTION-B contains SIX questions carrying TEN marks each and students have to attempt any FOUR questions.**

SECTION-A

1. Write briefly :

(a) Define Well Ordering Principle.

(b) Find gcd(272,1479).

(c) Find lcm(56,72).

(d) Check the consistency of the Diophantine equation : $13x + 117y = 91$.

(e) Find all prime numbers that divide 40!

(f) Show that $[x + n] = [x] + n$, for any positive integer n.

(g) State Möbius inversion formula.

(h) Find $\phi(22750)$.

(i) State Euler's Theorem.

(j) Derive Fermat's theorem from Euler's theorem.

SECTION-B

2. (a) If $bd = bd'(\text{mod m})$ and $g = \gcd(b,m) \neq 1$, then prove that $d' = d$ $d'\left(\text{mod}\frac{m}{g}\right)$

(b) If $m > 0$, prove that $\text{lcm}[ma, mb) = m\ \text{lcm}[a, b]$ and $\text{lcm}[a, b], gcd(a, b) = |ab|$.

3. (a) Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$ be a polynomial with $(n + 1)$ integral coefficients a_i; $1 \leq i \leq n$. If $a \equiv b(\text{mod } m)$, then prove that $f(a) = f(b)(\text{mod } m)$.

(b) If $\gcd(a, b) = 1$, then prove that. $\gcd(a + b, ab) = 1$.

4. State and prove fundamental theorem of arithmetic.

5. Find the least positive solution of the congruence $3x = 11$ (mod 2275).

6. (a) If a and b are prime to each other, show that $(b - 1)!\ (a^{b-1} - 1) = 0(\text{mod } b)$.

(b) Prove that $\{n, \phi(n)\}$ is a Möbius pair.

7. (a) If $2n + 1$ is prime, then prove that $(n!)^2 \equiv (-1)^{n+1}(\text{mod } 2n + 1)$.

(b) Prove that Euler's ϕ function is multiplicative.

NOTE : Disclosure of Identity by writing Mobile No. or Marking of passing request on any paper of Answer Sheet will lead to UMC against the Student.