Roll No. ☐☐☐☐☐☐☐☐☐☐☐☐ **Total No. of Pages : 02**

Total No. of Questions : 07

B.Sc.(Computer Science) (2013 & Onwards) (Sem.–4)

NUMBER THEORY

Subject Code : BCS-401

M.Code : 72317

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. Answer the followings in short :

a) Prove that $3a^2 - 1$ is never a perfect square.

b) Show that **any two** consecutive Fibonacci number are relatively primes.

c) State fundamental theorem of Arithmetic. Also prove number of primes are infinite.

d) Find all primitive Pythagorean triples for x = 40.

e) If (x, y, z) is primitive solution of $x^2 + y^2 = z^2$ then show $(x, y) = (y, z) = (z, x) = 1$.

f) Show that $2^{37} - 1$ is divisible by 233.

g) Find all integers n such that $\phi(n) = \phi(2n)$

h) State Fermat's Theorem. Show that 1763 is a composite number.

i) Using Wilson's Theorem, show that 17 is a prime number,

j) Prove that $\phi(p^a) = p^a - p^{a-1}$ for prime p and $\alpha \geq 1$.

SECTION-B

Q2. State and prove division algorithm. Show that the square of any integer is either of the forms $3k$, or $3k + 1$ using it.

Q3. Show that the positive primitive solutions of $x^2 + y^2 = z^2$ with x as even are given by $x = 2ab$, $y = a^2 - b^2$, $z = a^2 + b^2$ where a and b are integers of opposite parity and $(a, b) = 1$ and $a > b > 0$.

Q4. Let p be a prime number. Prove that $x^2 \equiv -1 (\text{mod } p)$ has a solution iff $p = 2$ or $p \equiv 1 (\text{mod } 4)$.

Q5. Derive a relation between Mobius and Euler- Totient function. Also verify Mobius inversion formula for $n = 20$.

Q6. Let p be a prime. Then prove that

(i) $(p - 1)! \equiv -1 (\text{mod } p)$

(ii) $a^p \equiv a (\text{mod } p)$ for every integer a.

Q7. State and prove Chinese Remainder Theorem. Also find the least positive integer that give remainder 1, 2, 3 when divided by 3, 4, 5 respectively.

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