Registration No : | | | | | | | | | | |

Total Number of Pages : 02 **B.Tech**
PCS7D001

7th Semester Regular Examination 2019-20
COMPUTATIONAL NUMBERS THEORY
BRANCH : CSE
Max Marks : 100
Time : 3 Hours
Q.CODE : HR345

Answer Question No.1 (Part-1) which is compulsory, any EIGHT from Part-II and any TWO from Part-III.
The figures in the right hand margin indicate marks.

Part- I

Q1 **Only Short Answer Type Questions (Answer All-10)** **(2 x 10)**

a) Define Algebraic coding theory.
b) Define Hensel lifting.
c) What is the difference between polynomial basis and normal basis?
d) What is complete factorization?
e) What is Primality testing?
f) What do you mean by Montgomery Arithmetic?
g) Define Chinese Remainder Theorem.
h) What is the time complexity of Chinese remainder theorem?
i) What is hensel lifting and how it can be used for polynomial division?
j) How Elliptic Curves relates to Finite fields?

Part- II

Q2 **Only Focused-Short Answer Type Questions- (Answer Any Eight out of Twelve)** **(6 x 8)**

a) Find all the points at infinity on the following curves.
The ellipse $X^2/a^2 + Y^2/b^2 = 1$ with a, b real and positive, treated as a curve over C.
b) Represent F9 as F3(θ), where $\theta^4 + \theta + 2 = 0$.
Find the roots of $x^4 + x + 2$ in F9.
c) Let p be a prime number and greater than 11. Prove that 11 is a quadratic residue modulo p if and only if $p \equiv \pm 1 \pmod{12}$.
d) Let $a_1, a_2, \ldots, a_n$ be non-zero integers, and $d = \gcd(a_1, a_2, \ldots, a_n)$. Prove that there exist integers $u_1, u_2, \ldots, u_n$ with the property that $u_1a_1 + u_2a_2 + \cdots + u_na_n = d$.
e) Represent F9 as F3(θ), where $\theta^2 - 2 = 0$. Prove that θ is a primitive element of F9.
f) The polynomial $x^2 + x + 2$ is reducible modulo 3 (True/False). Justify your answer.
g) Let $n = x^2 y$ where x, y distinct odd primes, $x / (y - 1)$ and $x / (y - 1)$. Prove that factoring n is polynomial-time equivalent to computing φ(n).
h) Is $u >= \sqrt{n}$, then n is prime. If yes, then justify your answer
i) Describe the process of root finding with one example.
j) Describe pollard rho method of computing discreate algorithms over finite fields with one example briefly?
k) Write short note on Cryptography
l) Write short notes on factorization of polynomials

Part-III

Only Long Answer Type Questions (Answer Any Two out of Four)

Q3 List the various algorithms used in Primality testing. Discuss them in details. **(16)**

Q4 Determine which of the following curves is/are non-singular. **(16)**

a) C1 : $y^2 + 4y = x^3 - 3x - 6$ defined over Q.

b) C2 : $y^2 + 4y = x^3 - 3x + 6$ defined over F7.

Q5 **a)** Compute the complete factorization of $x^5 + 4x^3 + 4x^2 + 2$ in F7[x]. **(8)**

b) Compute the continued fraction expansion of $\sqrt{5}$? **(8)**

Q6 **Short notes on any FOUR** **(4 × 4)**

a) AKS test.

b) Index calculus methods

c) CFRAC method

d) Schoof's point counting algorithm

e) pollard's p-1