Registration No :

Total Number of Pages : 02

B.Tech
PCS7D001

7^{th} Semester Regular Examination 2018-19
COMPUTATIONAL NUMBERS THEORY
BRANCH : CSE
Time : 3 Hours
Max Marks : 100
Q.CODE : E440

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

- **a)** Let $n = p^2 q$ with p, q distinct odd primes, p / (q − 1) and q / (p − 1). Prove that factoring n is polynomial-time equivalent to computing φ(n).
- **b)** Which of the polynomials $x^2 \pm 7$ is irreducible modulo 19? Justify
- **c)** What do you mean by primitive elements? Give two examples?
- **d)** What is the difference between polynomial basis and normal basis?
- **e)** What is Primality testing? List the various algorithms used for this?
- **f)** What do you mean by Montgomery Arithmetic?
- **g)** What is Elliptic Curves? How it relates to Finite fields?
- **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)** Factor number 299 using pollard's p-1 method of integer factoring?

Part- II

Q2 Focused-Short Answer Type Questions- (Answer Any EIGHT out of TWELVE) **(6 x 8)**

- **a)** Prove that the polynomial $x^2 + x + 2$ is irreducible modulo 3
- **b)** Represent F9 as F3(θ), where $\theta^2 + \theta + 2 = 0$.
  Find the roots of $x^2 + x + 2$ in F9.
- **c)** Represent F9 as F3(θ), where $\theta^2 + \theta + 2 = 0$.
  Prove that θ is a primitive element of F9.
- **d)** Let $a_1, a_2, \ldots, an$ be non-zero integers, and $d = \gcd(a_1, a2, \ldots, a_n)$. 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)** Let p be a prime > 3. Prove that 3 is a quadratic residue modulo p if and only if $p \equiv \pm 1 \pmod{12}$.
- **f)** 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.
- **g)** Let $n = p^2 q$ with p, q odd primes satisfying $q = 2p + 1$. Argue that one can factor n in polynomial time
- **h)** Conclude that if $u >= \sqrt{n}$, then n is prime
- **i)** Explain Algebraic coding theory?
- **j)** Describe the process of root finding and factorization of polynomials with one example?
- **k)** Describe AKS test with one example briefly?
- **l)** Describe pollard rho method of computing discreate algorithms over finite fields with one example briefly?

Part-III

Long Answer Type Questions (Answer Any TWO out of FOUR)

Q3 Compute all the simultaneous solutions of the following congruences. **(16)**
$5x \equiv 3 \pmod{47}$,
$3x^2 \equiv 5 \pmod{49}$.

Q4 a) Determine which of the following curves is/are non-singular (i.e., elliptic curves). **(10)**

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

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

b) Compute the complete factorization of $x^5 + 4x^3 + 4x^2 + 2$ in F7[x]. **(6)**

Q5 a) Let γ be a primitive element of the finite field F_q, and r ∈ N. Prove that the polynomial $x^r - \gamma$ has a root in Fq if and only if gcd(r, q − 1) = 1. **(10)**

b) Compute the continued fraction expansion of √ 5? **(6)**

Q6 **Short notes on any FOUR :** **(4 x 4)**

a) Cryptography

b) Index calculus methods

c) CFRAC method

d) Schoof's point counting algorithm

e) Hensel lifting

f) Chinese Remainder Theorem