Discrete Structures (MA5.101)

End Semester Examination (Monsoon 2021)

International Institute of Information Technology, Hyderabad

Time: 120 Minutes Total Marks: 50

Instructions: This is online examination.

Write at the top of your answer book the following:

Discrete Structures (MA5.101)

End Semester Examination (Monsoon 2021)

Date: 8-Mar-2022

Name:

Roll Number:

Submit your scanned hand-written answer script in the moodle with the file name: RollNo_EndSem_SecNo_8Mar2022.pdf

NOTE: No email submissions for the answer scripts are allowed.

8 Mar 2022

1. (a) If X is a normal (μ, σ) variate, then prove that

   (i) $P(a < X < b) = \phi\left(\frac{b-\mu}{\sigma}\right) - \phi\left(\frac{a-\mu}{\sigma}\right)$

   (ii) $P(|X - \mu| > a\sigma) = 2[1 - \phi(a)]$

   where $\phi(x)$ denotes the standard normal distribution function.

   (b) A point P is chosen at random on a circle of radius a and A is a fixed point on the circle. Derive the probability that the chord AP will exceed the length of the side of an equilateral triangle inscribed in the circle.

   [(2.5 + 2.5) + 5 = 10]

2. (a) A ring element a is called an idempotent if $a^2 = a$.

   (i) Prove that the only idempotents in an integral domain are 0 and 1.

   (ii) Let a and b be idempotents in a commutative ring. Show that $a + b - 2ab$ is also an idempotent.

   (b) Using the extended Euclid gcd algorithm, find the multiplicative inverse of 1234 in the finite field $GF(4321)$.

   [(2.5 + 2.5) + 5 = 10]

3. (a) Compute the product of bytes $\{d3\}.\{8f\}$ with respect to an irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$ in $GF(2^8)$.

(b) Find all the irreducible polynomials of degree 3 in $GF(2^3)$.

[5 + 5 = 10]

4. (a) Prove that the set of all morphisms of any monoid $M = [S, \circ]$ (from S to itself) is a submonoid of $[S^S, \circ]$, where S^S represents the set of all functions from S to itself.

   (b) In a group G, the center $C(G)$ of the group is the subset of elements of G that commute with every element of G. That is, $C(G) = \{h | g \circ h = h \circ g, \forall g \in G\}$, where $\circ$ is the operation defined in G. Prove that $C(G)$ is a normal subgroup of G.

[5 + 5 = 10]

5. (a) Show that a group G is abelian (commutative) if and only if $(ab)^2 = a^2b^2$, $\forall a, b \in G$, where the group composition being ordinary multiplication.

   (b) Prove that a group code can correct all combinations of t or fewer errors and can detect all combinations of $(t+1)$ to d errors, where $t \leq d$, if and only if it has a minimum Hamming distance of at least $(t + d + 1)$.

[5 + 5 = 10]

**************** **End of Question Paper** *******************