International Institute of Information Technology Hyderabad

Discrete Structures (MA5.101)

Assignment 5
Total Marks: 190

Ring and Field

1. A non-empty subset S of a ring $(R, +, .)$ will form a sub-ring of R, if and only if, for any two elements x and y of S,

   $$x - y \in S \text{ and } x.y \in S, \forall x, y \in S.$$

   (i) Prove that the intersection of two sub-rings is a ring.

   (ii) The center of a ring R is defines to be

   $$\{a \in R | ax = xa, \forall x \in R\}.$$

   Show that the center of the ring R is a sub-ring of R.

   [10 + 10 = 20]

2. If $a^2 = a$, for every element a in a ring R, then show that $b = -b$, for every $b \in R$.

   [10]

3. Prove that the set of all 2×2 real matrices of the form:

   $$\begin{bmatrix} x & y \\ -y & x \end{bmatrix}$$

   forms a field with respect to matrix addition and multiplication.

   [10]

4. Given two elements a, b in a field $\langle F, +, \times \rangle$ and $b \neq 0$. Prove that $a = 1$ if $(a \times b)^2 = a \times b^2 + b \times a \times b - b^2$.

   [10]

5. Prove that a finite integral domain is a field.

   [10]

6. Compute

$$\{a4\}.\{8d\}$$

in $GF(2^8)$ with respect to an irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$.

[10]

7. Find the multiplicative inverse of $(x^5 + x^3 + x^2 + 1) \mod (x^8 + x^4 + x^3 + x + 1)$ in $GF(2^8)$.

[10]

Group Code

8. Given the following parity-check matrix, H:

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

(i) Encode the message $\langle$ 1 0 1 1 $\rangle$ using H.
(ii) Decode the received tuple $\langle$ 1 1 0 0 0 1 1 $\rangle$ assuming that error, if any, is a single-error.

[5 + (3+ 2) = 10]

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

[10]

Pigeonhole Principle

10. Show that if seven numbers from 1 to 12 are chosen, then two of them will add up to 13.

[10]

11. Given a set of sixteen natural numbers, none having a prime factor > 7, show that either some number is a perfect square or, the product of some two distinct numbers is a perfect square.

[Use the fundamental theorem of arithmetic and the canonical representation of a number $n > 1$].

[10]

12. Prove that among 100,000 people there are two who were born in exactly the same time (hour, minute and second).

[10]

Graph Theory

13. The Fibonacci sequence $f_1, f_2, f_3 \ldots$ is defined as follows.

$$f_1 = f_2 = 1$$
$$f_r = f_{r-1} + f_{r-2} \; \forall \, r \geq 3$$

Prove that the following propositions hold for all positive integers n.

(a) $f_{n+1}f_{n-1} - f_n^2 = (-1)^n$

(b) $f_{n+1}^2 + f_n^2 = f_{2n+1}$

(c) For any positive integers m and n, show that $f_{n+m} = f_m f_{n+1} + f_{m-1} f_n$

[18]

14. For any set T whose elements are positive integers, define $\phi(T)$ to be the square of the product of the elements of T. For example, if $T = \{1, 2, 5, 6\}$, then $\phi(T) = (1 \cdot 2 \cdot 5 \cdot 6)^2 = 60^2 = 3600$. For any positive integer n, consider all nonempty subsets S of $\{1, 2, \ldots, n\}$ that do not contain two consecutive integers. Prove that Σ, the sum of all the $\phi(S)$'s of these subsets is given as

$$\Sigma = (n + 1)! - 1.$$

[10]

15. Prove the following

   (a) The sum of all degrees of an undirected graph is even.

   (b) In a graph $G = (V, D)$, let $d(u, v)$ be the length of shortest path connecting the two vertices u and v. Prove that the function d satisfies the following:
   $d(u, v) + d(v, w) \geq d(u, w)$ where $u, v, w \in V$.

[10]

16. For a **simple** undirected graph $G = (V, D)$, Let n be the number of vertices and x_i be the degree of the vertex v_i. For the given series of $(x_1, x_2, \ldots, x_n)$, sketch a graph with the given degrees. If not possible, explain why.

   (a) (4, 3, 2, 2)

   (b) (2, 1, 1, 0)

   (c) (4, 4, 4, 4, 2)

   (d) (4, 2, 2, 1, 1)

   (e) (3, 2, 1)

[10]

17. On an 8*8 chessboard, A new piece, "Jack", is proposed. Jack can move either (3 squares vertically and 2 squares horizontally) or (2 squares vertically and 3 squares horizontally)

   (a) Define a relation that relates all squares to the squares Jack can go to in a single move

   (b) Show that Jack can move to any square of the same color

   (c) Show that Jack can move from any square of the board to any other square

   You can consider the chessboard as a set of coordinate pairs:

$$V = \{(x, y) | x, y \in \mathbb{N} \text{ and } 0 \leq x, y \leq 7\}.$$

   Adjacent squares have different colors (basically a conventional chessboard)

[12]

All the best!!!