Department of Computer Science and Engineering

Mid-Semester Examination

Course No.: CS 207 Course Name: Discrete Structures

Date: 13/9/2017 Time: 11-00 to 13-00 Marks: 30

NOTE: You can use any result done in class/homework but state it clearly. Do NOT ask for any clarifications.

Q1. In a RSA cryptosystem, the public-key is specified by $n = 143$ and $e = 53$. What is the private-key? Equivalently, find a positive number d such that $a^{53d} \equiv a \bmod 143$ for all a with $gcd(a, 143) = 1$. (3)

Q2. Let A be a finite set with $n \geq 1$ elements, and $\preceq$ a partial order on A.

(a) Show that there exists a minimal element in A, that is, an element x such that for all $y \in A$, $y \preceq x$ implies $y = x$. (2)

(b) Show that there is a total order $\leq$ on A that contains the partial order $\preceq$. A total order is a partial order such that for any two elements x, y, either $x \leq y$ or $y \leq x$. (2)

(c) Prove that $\preceq$ can be written as the intersection of n total orders on A. (3)

(d) The dimension of a partial order is the minimum number of total orders whose intersection is the given partial order. Prove that the dimension of the partial order on 2^A defined by the subset relation is n. (6)

Q3. A function f from a set A to itself is said to be idempotent if $f.f. = f$, that is $f(f(x)) = f(x)$ for all $x \in A$. Write down the simplest possible expression for the number of idempotent functions from $[n]$ to $[n]$. Explain how you got the answer. (5)

Q4 (a) A $2 \times n$ matrix is said to be in standard form if it contains all numbers from 1 to $2n$ and both rows and all columns are strictly increasing. Prove that the number of such matrices is the Catalan number $C_n = \binom{2n}{n}/(n+1)$. (3)

(b) A permutation p of $[n]$ can be written as a sequence of numbers $p_1, p_2, \ldots, p_n$ where $p_i = p(i)$. A subsequence of a permutation is a sequence of numbers $p_{i_1}, p_{i_2}, \ldots, p_{i_k}$ for some $1 \leq i_1 < i_2 < \cdots < i_k \leq n$. A permutation of $[2n]$ is said to be good if the longest increasing subsequence in the permutation has length n and the longest decreasing subsequence has length 2. Prove that the number of good permutations of $[2n]$ is C_n^2. Hint: Show a bijection from such permutations to pairs of $2 \times n$ matrices in standard form. (6)