Midterm 1 for CS 170

PRINT your name: ,

(last) (first)

SIGN your name:

WRITE your section number (e.g., 101):

WRITE your SID:

One page of notes is permitted. No electronic devices, e.g. cell phones and calculators, are permitted. Do all your work on the pages of this examination. If you need more space, you may use the reverse side of the page, but try to use the reverse of the same page where the problem is stated.

You have 80 minutes. The questions are of varying difficulty, so avoid spending too long on any one question.

In all algorithm design problems, you may use high-level pseudocode.

DO NOT TURN THE PAGE UNTIL YOU ARE TOLD TO DO SO.

Problem	Score/Points
Name/Section/etc.	
1	/60
2	/10
3	/10
4	/10
5	/10
Total	/100

Problem 1 [60 points] True (always) or False (on occasion) or short answer. Justify.

1. $n \log n = O(n^2)$. [T/F]

2. $n^2 = O(n \log n)$. [T/F]

3. $2^{c \log_2 n} = \Theta(n^c)$. [T/F]

4. $2^{O(\log_2 n)} = O(n^3)$. [T/F]

5. If $T(n) = 50000T(n/100) + O(n)$, then $T(n) = O(n^{2.5})$. [T/F]

6. If $T(n) = 50000T(n/100) + O(n)$, then $T(n) = \Omega(n^{2.5})$. [T/F]

7. If $T(n) = 3T(n/3) + O(n)$, then what is $T(n)$? [Short answer]

8. The number 3 has a multiplicative inverse **mod** 8? [T/F]

9. There is no solution to the equation $4x = 1$ **mod** 8? [T/F]

10. The probability that an n-bit integer is prime is $O(1/n)$? [T/F]

11. The probability that an n-bit integer is prime is asymptotically $\Omega(1/n)$? [T/F]

12. The lowest post order number of a depth first search of a DAG corresponds to a sink? [T/F]. (A sink is a node with no outgoing arcs.) (If false, give a counterexample.)

13. The lowest post order number of a depth first search of a graph is in a sink strongly connected component. [T/F] (If false, give a counterexample.)

14. How much stack space would one need to run depth first search in the worst case on an n node m edge graph? (Asymptotic notation.)

15. How much stack space would one need to run depth first search on a complete binary tree with n leaves? Note that a complete binary tree has two equal sized subtrees at each internal node. (Asymptotic notation.)

Problem 2. (10 points.)

1. What is the decryption key for RSA when the public key is $(N = 77, e = 7)$? Show your work if you want partial credit.

2. Why did I not choose $e = 3$?

Problem 3. (10 points.)

1. What are the fourth roots of unity?
2. What is the Fourier transform of the sequence $[0, 1, 0, 0]$?
3. What is the *inverse* Fourier transform of the sequence $[1, 0, 0, 0]$?

Problem 4. (10 points.)

1. Give a method that given the pre and post order numbers of all the neighbors of u for a call to explore(u) on an *undirected graph* determines whether u is on a cycle. (A cycle in an undirected graph is a sequence of distinct edges $e_0 = (v_0, v_1), e_1 = (v_1, v_2), \ldots, e_k = (v_k, v_0)$.) (Short answer.)

2. Prove that when pre,post intervals of two nodes u and v in a *directed* graph are disjoint then they are in different strongly connected components. (Short proof.)

Problem 5. (10 points.)

You are given a set of n distinct numbers. You divide them into groups of five, let S be the set of consisting of the median of each group, and let x be the median of these numbers. Notice that x will larger than $3n/10$ of the numbers and lower than $3n/10$ of the numbers.

(a) Sketch a recursive deterministic algorithm for selecting the kth largest element using the above idea. Write out a recurrence bounding its runtime. (You will primarily be graded on the recurrence.)

(b) Give an asymptotic upper bound on your recurrence.