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.	/5
1	/20
2	/20
3	/20
4	/20
5	/15
Total	/100

1. True/False. No need to justify your answer. [2 points per problem]

Answer true or false for each. Scoring is 2 points for correct answer and -2 points for incorrect.

1. $2^n = \Omega(n!)$.
2. $3^{\log \sqrt{n}} = \Theta(\sqrt{n})$.
3. If $f(n) = O(g(n))$, then $g(n) = \Omega(f(n))$.
4. $\sum_{j=1}^{n} j = O(n \log n)$.
5. If $T(n) = 4T(n/2) + O(n)$ then $T(n) = O(n^3)$.
6. If $T(n) = 4T(n/2) + O(n)$ then $T(n) = O(n^2 \log n)$.
7. If $a^{n-1} \equiv 1 \bmod n$ for all positive integers $a < n$, then n is prime.
8. The probability that an n-bit integer is prime is roughly 2^{-n}.
9. Any DAG with a unique source and sink has a unique topological ordering.
10. Breadth first search and depth first search produces the same tree on connected undirected graphs if and only if the graph is a tree.

2. Number Theoretical Algorithms (20 points)

1. Give an asymptotic upper bound on the number of bits in a number a^b if a and b are both n-bit numbers? How about a^{b^c}, when c is an n-bit number.

2. Given n-bit primes p and q, and public key (e, pq).

   (a) What is d the secret key and how long does it take to find?

   (b) How long does it take to compute the encoding of an n-bit message?

3. Algorithm Design and FFT.

1. Given k sorted arrays of length l, sketch an algorithm for finding the median element of all the kl elements. Justify the correctness and give and justify running time bounds. (We are looking for a solution that takes $o(kl)$ time.)

2. What is the FFT matrix for a four point FFT? What is the FFT of (0,0,0,1)? of (1,0,0,0)?

4. Depth first Search. 20 points.

Given only the ability to run DFS on a graph from any starting point u and obtaining the resulting pre and post order numbers. (You never get to see an edge.) (Remark: these are pretty easy so don't worry if it seems so.)

1. Show how to find a pair of vertices that is in a cycle in a directed graph if there is one. (You can call DFS as many times as you like on different starting point.)

2. If for some DFS $[pre(u), post(u)]$ is disjoint from $[pre[v], post(v)]$, what is the relative order of the intervals if u is reachable from v?

3. For a connected undirected graph where the starting point is on a cycle, what is the pre and post numbers of the starting point in terms of the number of nodes in the graph. What if the graph is not connected?

5. Shortest paths. (15 points)

Give as fast an algorithm as you can that indicates whether or not there is a negative cycle in a strongly connected graph $G = (V, E)$ with at most k negative edges. Justify both the correctness and the running time of your algorithm(s). (Remark: An $O(k(m + n \log n))$ gets you full credit. An $O(k^3 + k(m + n \log n))$ time gets you 3/4 credit where $n = |V|$ and $m = |E|$.)