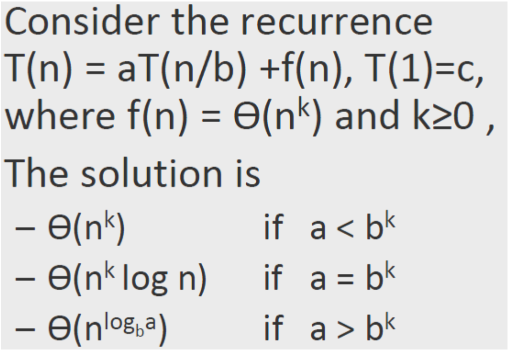
MA/CSSE 473 Exam #1 Fall, 2012 Name__________________________ Section 01__ 02__

Resources allowed: Textbook, calculator, one 8.5 x 11 sheet of paper.
Resources not allowed: Anything that can communicate or has headphones/earphones.

It is possible to get so caught up in getting all of the points for one problem and spend so much time on it that you do not get to the other problems. Don't do that! I will be generous with partial credit if you have the main ideas. You should first do the problems you are confident about, and then do the rest.

For Instructor use:

Problem	Possible	Earned
1	20	
2	20	
3	8	
4	15	
5	15	
6	5	
7	4	
8	8	
9	5	
Total	100	



Consider the recurrence $T(n) = aT(n/b) + f(n)$, $T(1)=c$, where $f(n) = \Theta(n^k)$ and $k \geq 0$,

The solution is

– $\Theta(n^k)$ if $a < b^k$
– $\Theta(n^k \log n)$ if $a = b^k$
– $\Theta(n^{\log_b a})$ if $a > b^k$

I chose small numbers for the first two problems, so that the arithmetic can be done with the assistance of a simple calculator. Because the possible answers come from a very small set, you *could* get the answers by trial and error. But I insist that you show me how you get your answers, in a way that demonstrates that you understand the algorithms.

1. (20) Show how to use the extended Euclid's algorithm to find the inverse of 5 (mod 48). Your answer should be a number in the range 1 … 47.

   Answer: __________

   How to get that answer::

2. (20) Bob has advertised his RSA public key as (N=65, e=29). Eve intercepts an encoded message that someone sends to Bob using this public key, and that encoded message is: 3

   What was the original message before it was encoded? __________

   Briefly show how you got your answer; you do not have to write a lot, but convince me that you understand RSA.

3. (8) T/F/IDK. Below you will find two statements. A statement is true (T) if it is always true. It is false (F) if there is at least one counterexample (i.e. sometimes false). You may also choose IDK to indicate that you do not know the answer. Point values: Correct answer: 4, incorrect answer: -1, IDK: 2, blank: 0.
   Circle one answer for each part.

   a. T F IDK f(n) + g(n) is O(max(f(n), g(n))).

   b. T F IDK If f(n) is $\Theta(g(n))$, then $2^{f(n)}$ is $\Theta(2^{g(n)})$.

4. (15) Use mathematical induction to show that for all n≥1, $\sum_{i=1}^{n} i(i!) = (n+1)! - 1$.
   Be sure to indicate the step that uses the induction assumption.

5. (15) Suppose we have N points in two dimensions. Consider the recursive algorithm for finding the smallest distance between two of those points. We said that the number of comparisons between pairs of points is given by the recurrence T(N) = 2T(N/2) + O(N). Explain how we can guarantee that the "overhead", i.e. the work done in addition to the recursive calls, can be O(N).

6. (5) If G is a directed graph with n vertices, what is the maximum number of distinct vertex orders that can comprise a topological sort of G?

7. (4) Name a software system that was invented by Donald Knuth. ____________________

8. (8) If we use brute force integer multiplication and addition, and brute-force matrix multiplication, what is the big-theta running time (in terms of *n*) for multiplying *n* *n*-by-*n* matrices whose entries are *n*-bit integers? Circle one of the choices below. Briefly show how you get your answer

$\Theta(n^2)$ $\Theta(n^3)$ $\Theta(n^4)$ $\Theta(n^5)$ $\Theta(n^6)$ $\Theta(n^7)$ $\Theta(n^8)$ $\Theta(n^9)$ $\Theta(n^{10})$ $\Theta(n^{11})$ $\Theta(n^{12})$

9. (5) Find the big-theta solution of $T(N) = 8T(N/4) + 5N^2$

Answer: $T(N) \in \Theta(\qquad)$