CS 4050 Test 1 Name ______________________

Each problem is worth 8 test points (purely for assigning a score out of 100% on the test), and some problems have several unrelated parts worth the points indicated.

Please write your answers on these sheets or your own paper and send me either one PDF file for your entire test or a separate file for each problem.

You may use any of our course materials: the written chapter documents, the videos, and your Exercise work. Other than accessing those allowed materials, you *may not* run any programs, including any Web browser or communication software, to help you on any questions, or communicate with anyone other than me about the test questions or course material. You may use a standard calculator (no special programs used).

1. The Sum of Subsets problem gives a set of positive numbers S (with no repeats for simplicity) and a target number T and asks for all the different subsets of S whose items add up to T.

For example, if $S = \{1, 2, 5, 6, 9\}$ and $T = 15$ then the answer is $\{1, 5, 9\}$ and $\{6, 9\}$.

Your job on this problem is to demonstrate a brute force approach to this problem by drawing the possibilities tree for this problem on the instance with $S = \{2, 5, 7, 8\}$ and $T = 15$, using the following rules: for each node of the tree, all child nodes should be generated using items of S that are larger than the last item used in the node, and each node should be pruned (draw an "X" under it) when its total is greater than the target or when there are no more items to be added, and nodes that have total equal to the target should be circled (and of course have no child nodes generated).

Each node should contain just the list of items being used (we probably should store the total of those items in each node, but it is trivial to add them up for this example, so don't bother).

Note that you will be scored based on how well you follow these rules—if your tree is just done in some other way, you will be penalized.

2. For each part, you will be asked to formally prove a O fact.

a. [4 points] Prove that $3n^2 + 59n \in O(n^2)$ by finding—and writing in the blank provided—a value for what we usually call "N" such that the statement below is true for the allowed values of n, and justify, either by writing down some experimental values or doing some algebra, that your inequality is true. Note that you are being required to use $c = 5$ (ordinarily in proving a big-O fact, you get to pick both N and c, but for the purposes of assessing your understanding, here you are being forced to use $c = 5$).

For all $n \geq$ ______,

$$3n^2 + 59n \leq 5n^2$$

Show the work you did to convince yourself that your inequality is true for the specified values of n:

b. [4 points] Prove that $100n^3 \in O(3^n)$ by finding—and writing in the blanks provided—a value for what we usually call c such that the statement below is true, and justify, either by writing down some experimental values or some algebra, that your inequality is true (note that here you are being forced to use $N = 6$).

For all $n \geq 6$,

$$100n^3 \leq \text{\_\_\_\_\_\_}\ 3^n$$

Show the work you did to convince yourself that your inequality is true for the specified values of n:

3. Consider the recurrence relation

$$T(n) = 5T\left(\frac{n}{2}\right) + n^3,$$

where we only care about $n = 2^m$, and $T(1) = 3$.

Showing all your steps, use our usual technique of repeated substitution—finish the first substitution, simplify, and do at least one more substitution step before extrapolating, and then somehow handle the geometric series that you get to find the Θ efficiency category for $T(n)$, expressed in terms of n to a constant power, or whatever it turns out to be in terms of n.

Note that $n^3 = (2^m)^3 = 8^m$.

$T(2^m) = 5T(2^{m-1}) + 8^m$

$= 5\left[5T(2^{m-2}) + 8^{m-1}\right] + 8^m =$

$=$

4. Demonstrate Karatsuba's algorithm for multiplying integers using just three half-size multiplications as detailed below.

Assume that you can use a calculator to do all operations (half-size (2 or 3 digit) multiplication, and adding, subtracting, and shifting of any size), but write down everything you do. (you are also encouraged to use a calculator to *check* your process by doing the 4-digit multiplication directly).

Suppose we want to multiply $3275 \cdot 2876$.

Write here the three half-size products that you are using:

Show how you can combine (adding or subtracting) some of these products to obtain whatever else you need:

Show how you can do shifting and adding to obtain the final answer:

5. For this problem and the next one do all your calculations in Z_{13}. For your convenience, here is the multiplication table in Z_{13} and a bunch of multiples of 13:

	0	1	2	3	4	5	6	7	8	9	10	11	12
0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12
2	0	2	4	6	8	10	12	1	3	5	7	9	11
3	0	3	6	9	12	2	5	8	11	1	4	7	10
4	0	4	8	12	3	7	11	2	6	10	1	5	9
5	0	5	10	2	7	12	4	9	1	6	11	3	8
6	0	6	12	5	11	4	10	3	9	2	8	1	7
7	0	7	1	8	2	9	3	10	4	11	5	12	6
8	0	8	3	11	6	1	9	4	12	7	2	10	5
9	0	9	5	1	10	6	2	11	7	3	12	8	4
10	0	10	7	4	1	11	8	5	2	12	9	6	3
11	0	11	9	7	5	3	1	12	10	8	6	4	2
12	0	12	11	10	9	8	7	6	5	4	3	2	1

```
0,  13,  26,  39,  52,  65,  78,  91,
104,  117,  130, 143,  156,  169
```

Here is the Fourier matrix F_4 for $\alpha = 8$, working in Z_{13}:

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 8 & 12 & 5 \\ 1 & 12 & 1 & 12 \\ 1 & 5 & 12 & 8 \end{bmatrix}.$$

Demonstrate how to multiply this matrix times $c = \begin{bmatrix} 5 \\ 3 \\ 2 \\ 7 \end{bmatrix}$ by the fast Fourier method, using just two products of 2 by 2 matrices times 2-vectors (do those products by hand/calculator, not by recursively doing the fast Fourier method). Show clearly what two 2 by 2 matrix products you perform and how you combine (adding vectors, multiplying rows of vectors by numbers) those products to get the desired answer. Since you can easily compute the product F_4c by the usual approach, you will be penalized if your demonstration doesn't produce the correct answer.

6. Complete the demonstration of how to efficiently compute a^e in Z_n for $a = 367$, $e = 23$, and $n = 2501$, using a calculator to do the arithmetic.

Some of the work has been done below, for the standard efficient algorithm—if you don't realize how to use what is given and waste time, that will be unfortunate.

367	23	
2136	11	
672	5	

7. Complete the demonstration of the extended GCD algorithm for computing the greatest common divisor of a and b, and producing s and t such that $sa + tb$ equals the GCD, with $t > 0$, for $a = 3671$ and $b = 215$.

Be sure to verify that your final values of s and t do what you want, namely $sa + tb = 1$, with $t > 0$.

a	b	r	q	s	t
3671	215	16	17		
215	16	7	13		

8. Suppose the public information for an RSA encryption scheme is $n = 247$ and $e = 31$. Suppose further that you intercept the encrypted message $c = 239$, which you know is a^e in Z_{241} for the original message a.

Show all the details to break this encryption.

Be sure to state the original message a and show all your steps—no credit for just pulling a out of thin air! If you have the energy, you might want to check your answer by encrypting the a you get to verify that this gives you 239.

Note that $247 = 13 \cdot 19$.