CS/MATH 111 Winter 2018
Final Test

- The test is 2 hours and 30 minutes long, starting at **8AM** and ending at **10:30AM**
- There are **8** problems on the test. Each problem is worth 10 points.
- Write legibly. What can't be read won't be credited.
- **Before** you start:
  - Make sure that your final has all 8 problems
  - Put your name and SID on the front page below and on top of *each* page

Name	SID

problem	1	2	3	4	5	6	7	8	total
score									

NAME: SID:

Problem 1: (a) Complete the statement of the Master Theorem by filling in the blanks.

Assume that $a \geq$ _____ , $b >$ _____, $c >$ _____ and $d \geq$ _____, and that $T(n)$ satisfies the recurrence $T(n) = aT(n/b) + cn^d$. Then

$$T(n) = \begin{cases} \_\_\_\_\_\_\_\_ & \text{if} \quad \_\_\_\_\_\_\_\_ \\ \_\_\_\_\_\_\_\_ & \text{if} \quad \_\_\_\_\_\_\_\_ \\ \_\_\_\_\_\_\_\_ & \text{if} \quad \_\_\_\_\_\_\_\_ \end{cases}$$

(b) Give asymptotic solutions for the following recurrences:

recurrence	solution
$f(n) = 4f(n/2) + 3n$	
$f(n) = 4f(n/2) + 5n^2$	
$f(n) = 4f(n/2) + n^3$	
$f(n) = 2f(n/3) + 4$	
$f(n) = f(n/3) + 5$	

Note: You must use correct notation.

NAME: SID:

Problem 2: (a) Explain how the RSA cryptosystem works by filling in the table below.

Initialization	Determine p, q, and n:	
	Formula for $\phi(n)$:	
	Determine e and d:	
	Public and secret keys:	

Encryption:		Decryption:	

(b) Below you are given five choices of parameters p, q, e, d of RSA. For each choice tell whether these parameters are correct[1] (write YES/NO). If yes, give a decryption of $C = 2$. If not, give a brief justification (at most 10 words).

p	q	e	d	correct?	justify if not correct / decrypt $C = 2$ if correct
11	7	11	11		
21	5	7	43		
5	19	31	7		
13	13	5	29		
7	13	5	31		

[1]o clarify, correctness refers to whether these parameters satisfy the conditions specified in the algorithm.

NAME: SID:

Problem 3: (a) Give a complete statement of Fermat's Little Theorem.

(b) Use Fermat's Little Theorem to compute $10^{-1} \pmod{13}$. (You will receive credit only if you use this theorem). Show your work.

(c) Solve the congruence $10x \equiv 5 \pmod{13}$. Show your work.

(d) Use Fermat's Little Theorem to compute $3^{229367} \pmod{11}$. Show your work.

NAME: SID:

Problem 4: We have five types of blocks with letters: `TA`, `JU`, `CO`, `GOR` and `SAC`. Let B_n denote the number of different words of length n that can be formed from these blocks. For example, for $n = 5$ we have $B_5 = 12$ because we can form 12 words of length 5:

TA|GOR	TA|SAC	JU|GOR	JU|SAC	CO|GOR	CO|SAC
GOR|TA	SAC|TA	GOR|JU	SAC|JU	GOR|CO	SAC|CO

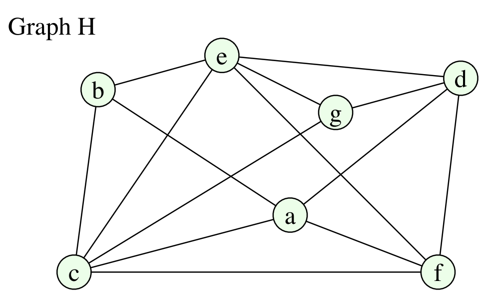
(a) Set up a recurrence for B_n and justify it.

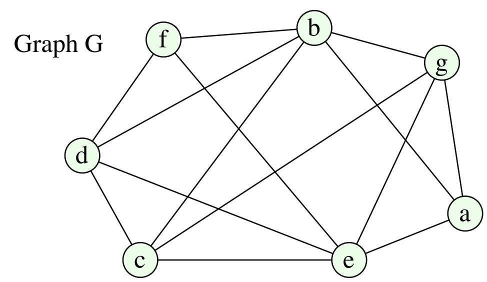
(b) Solve this recurrence to find a formula for B_n.

NAME: SID:

Problem 5: (a) Give a complete statement of Kuratowski's Theorem.

(b) Determine whether the two graphs below are planar or not. To show planarity, give a planar embedding. To show that a graph is not planar, use Kuratowski's theorem. (No credit without justification.)





NAME: SID:

Problem 6: We define a sequence of numbers A_n recursively as follows:

$$A_0 = 1$$
$$A_1 = 1$$
$$A_n = \frac{1}{8} \cdot A_{n-1}^2 + \frac{1}{8} \cdot A_{n-2} + 1 \quad \text{for all } n \geq 2$$

Use mathematical induction to prove that $A_n < 2$ for all $n \geq 0$.

NAME: SID:

Problem 7: (a) Complete the statement of the inclusion-exclusion principle below:

Let $S_1, S_2, ..., S_k$ be finite sets. Then

$$\left|\bigcup_{i=1}^{k} S_i\right| =$$

(b) We have three sets A, B, C that satisfy the following conditions:

$$|A| = 11 \qquad |B| = 12 \qquad |C| = 16$$

$$|A \cap B \cap C| = 1$$

$$|A \cap C| = |B \cap C| = \tfrac{5}{3} \cdot |A \cap B|$$

$$|A \cup B \cup C| = 9 \cdot |A \cap B|$$

Compute $|A \cup B \cup C|$. You need to use the inclusion-exclusion principle. Show your work.

NAME: SID:

Problem 8: Let T be a tree with n vertices. Denote by $T - \{u\}$ the graph obtained from T by removing a vertex u. A vertex v of T is called a *centroid* if each connected component of $T - \{v\}$ has at most $n/2$ vertices. Prove that each tree has a centroid.

Example: The figure below shows a tree T with $n = 11$ vertices. Vertex 5 is a centroid, because removing this vertex partitions the tree into subtrees of sizes 2, 3, and 5, all of size at most $11/2$.