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

Assume that $a \geq$ __1__ , $b >$ __1__, $c >$ __0__ and $d \geq$ __0__, and that $T(n)$ satisfies the recurrence $T(n) = aT(n/b) + cn^d$. Then

$$T(n) = \begin{cases} \underline{\Theta(n^{\log_b a})} & \text{if } \underline{a > b^d} \\ \underline{\Theta(n^d \log n)} & \text{if } \underline{a = b^d} \\ \underline{\Theta(n^d)} & \text{if } \underline{a < b^d} \end{cases}$$

(b) Give asymptotic solutions for the following recurrences:

recurrence	solution
$f(n) = 4f(n/2) + n^3$	$f(n) = \Theta(n^3)$
$f(n) = 4f(n/2) + 3n$	$f(n) = \Theta(n^2)$
$f(n) = 4f(n/2) + 5n^2$	$f(n) = \Theta(n^2 \log n)$
$f(n) = f(n/3) + 5$	$f(n) = \Theta(\log n)$
$f(n) = 2f(n/3) + 4$	$f(n) = \Theta(n^{\log_3 2})$

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:	p, q are different primes and $n = pq$
	Formula for $\phi(n)$:	$\phi(n) = (p-1)(q-1)$
	Determine e and d:	e can be any number between 2 and $n-1$ that is relatively prime to $\phi(n)$, and $d = e^{-1} \pmod{\phi(n)}$
	Public and secret keys:	$P = (n, e)$, $S = d$

Encryption:	$E(M) = M^e \operatorname{rem} n$	Decryption:	$D(C) = C^d \operatorname{rem} n$

(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
5	21	7	43	N	21 is not prime
19	5	31	7	Y	$2^7 \operatorname{rem} 95 = 33$
13	13	5	29	N	p cannot be equal to q
13	7	5	31	N	d is not the inverse of e modulo 72
11	7	11	11	Y	$2^{11} \operatorname{rem} 77 = 46$

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

NAME: SID:

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

If p is prime and $a \in \{1, 2, ..., p-1\}$ then $a^{p-1} \equiv 1 \pmod{p}$.

(b) Use Fermat's Little Theorem to compute $6^{-1} \pmod{13}$. (You will receive credit only if you use this theorem). Show your work.

Computing modulo 13, we have

$$\begin{aligned} 6^{-1} &= 6^{11} = 6 \cdot (6^2)^5 = 6 \cdot 10^5 = 6 \cdot 10 \cdot (10^2)^2 \\ &= 8 \cdot 9^2 = 11. \end{aligned}$$

(c) Solve the congruence $6x \equiv 11 \pmod{13}$. Show your work.

Since $6^{-1} \pmod{13} = 11$, computing modulo 13 we get $x = 11 \cdot 6^{-1} = 11 \cdot 11 = 4$.

(d) Use Fermat's Little Theorem to compute $2^{229368} \pmod{11}$. Show your work.

Computing modulo 13, we have $2^{229368} = (2^{10})^{22936} \cdot 2^8 = 2^8 = 4^4 = 16^2 = 5^2 = 3$.

NAME: SID:

Problem 4: We have five types of blocks with letters: BY , DU , NA , RAN and KAL. Let L_n denote the number of different words of length n that can be formed from these blocks. For example, for $n = 5$ we have $L_5 = 12$ because we can form 12 words of length 5:

BY|RAN BY|KAL DU|RAN DU|KAL NA|RAN NA|KAL

RAN|BY KAL|BY RAN|DU KAL|DU RAN|NA KAL|NA

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

Consider valid strings of length n. Each such string ends with a block of length 2 or 3, and for each string the last block is uniquely determined (because all blocks end with different letters). For each of the three blocks with two letters, there are L_{n-2} strings ending with this block. For each of the two blocks with three letters, there are L_{n-3} strings ending with this block.

For $n = 0$, we have only the empty string. For $n = 1$, there are no valid strings. For $n = 2$ we have three strings, each formed from one block. So the recurrence is

$$\begin{aligned} L_n &= 3L_{n-2} + 2L_{n-3} \\ L_0 &= 1 \\ L_1 &= 0 \\ L_2 &= 3 \end{aligned}$$

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

The characteristic equation is $x^3 - 3x - 2 = 0$. As usual with cubic equations, the first thing to do is to see whether there are integral roots. The only candidates are 1, -1 and 2. Indeed, both -1 and 2 are roots. The polynomial factors into $(x + 1)^2(x - 2)$, so we have roots $r_1 = -1$ with multiplicity 2 and $r_2 = 2$ with multiplicity 1.

This gives us the general form

$$L_n = \alpha_1 \cdot (-1)^n + \alpha_2 \cdot n \cdot (-1)^n + \alpha_3 \cdot 2^n.$$

After plugging into the initial conditions, we get

$$\begin{aligned} \alpha_1 + \alpha_3 &= 1 \\ -\alpha_1 - \alpha_2 + 2\alpha_3 &= 0 \\ \alpha_1 + 2\alpha_2 + 4\alpha_3 &= 3 \end{aligned}$$

The solution of these equations is $\alpha_1 = \frac{5}{9}$, $\alpha_2 = \frac{1}{3}$, and $\alpha_3 = \frac{4}{9}$. So the final answer is

$$L_n = \frac{5}{9} \cdot (-1)^n + \frac{1}{3} \cdot n \cdot (-1)^n + \frac{4}{9} \cdot 2^n.$$

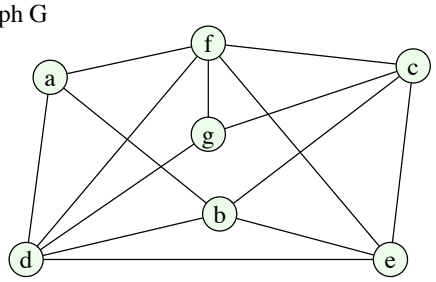
NAME: SID:

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

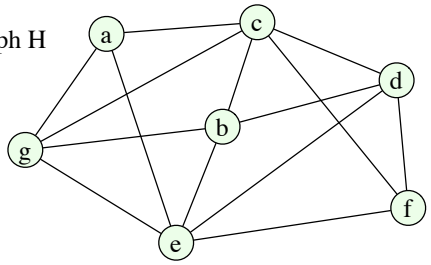
A graph is planar if and only if it does not contain a subgraph that is a sub-division of K_5 or $K_{3,3}$

(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.)

Graph G

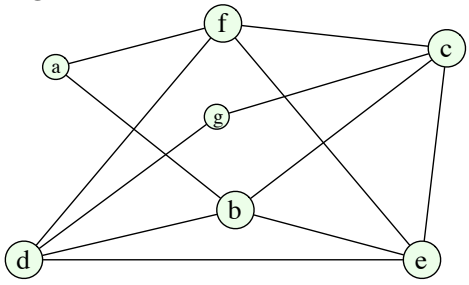


Graph H

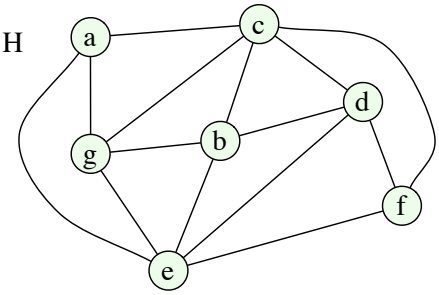


Graph G is not planar. A subdivision of K_5 in G is shown on the left. Graph H is planar. It's planar drawing is on the right.

Graph G



Graph H



NAME: SID:

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

$$\begin{aligned} U_0 &= 1 \\ U_1 &= 1 \\ U_n &= \tfrac{1}{8} \cdot U_{n-1}^2 + \tfrac{1}{8} \cdot U_{n-2} + 1 \quad \text{for all } n \geq 2 \end{aligned}$$

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

Base case: for $n = 0$ we have $U_0 = 1 < 2$ and for $n = 1$ we have $U_1 = 1 < 2$. So the claim holds in the base case.

Inductive step: Let $k \geq 2$ and assume now that the claim holds for all values $n < k$. In particular, it means that $U_{k-1} < 2$ and $U_{k-2} < 2$. We want to show that it also holds for $n = k$, that is $U_k < 2$. For $n = k$ we have

$$\begin{aligned} U_k &= \tfrac{1}{8} \cdot U_{k-1}^2 + \tfrac{1}{8} \cdot U_{k-2} + 1 \\ &< \tfrac{1}{8} \cdot 2^2 + \tfrac{1}{8} \cdot 2 + 1 \\ &= \tfrac{7}{4} \ < \ 2. \end{aligned}$$

Thus $U_k < 2$, completing the inductive step and the whole proof.

NAME: SID:

Problem 7: Nick is planning a 48-day vacation, to visit Afghanistan, Libya and Syria (in this order). He wants to spend at most 20 days in Afghanistan and at most 24 days in Libya. Compute the number of possible itineraries that satisfy these conditions. (Hint: use the method for computing the number of integer partitions, combined with the inclusion-exclusion formula.)

Denoting by a, l, s the number of days in Afghanistan, Libya and Syria, respectively, we need to compute the number of non-negative integer solutions of

$$\begin{aligned} a + l + s &= 48 \\ a &\leq 20 \\ l &\leq 24 \end{aligned}$$

As in class, let S denote the total number of non-negative solutions of $a + l + s = 48$ and $S(P)$ denote the number of solutions that satisfy some condition P. We need to compute $S(a \leq 20 \wedge l \leq 24)$.

We start by computing the number of itineraries that *do not* satisfy the required condition, and to compute this number we apply the inclusion-exclusion principle:

$$\begin{aligned} S(a \geq 21 \vee l \geq 25) &= S(a \geq 21) + S(l \geq 25) - S(a \geq 21 \wedge l \geq 25) \\ &= \binom{48-21+2}{2} + \binom{48-25+2}{2} - \binom{48-21-25+2}{2} \\ &= \binom{29}{2} + \binom{25}{2} - \binom{4}{2} \\ &= 406 + 300 - 6 = 700. \end{aligned}$$

The number of all solutions is

$$S = \binom{48+2}{2} = \binom{50}{2} = 1225.$$

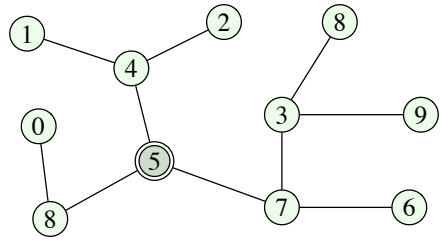
Then

$$\begin{aligned} S(a \leq 20 \wedge l \leq 24) &= S - S(a \geq 21 \vee l \geq 25) \\ &= 1225 - 700 = 525. \end{aligned}$$

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 $11/2$.



The proof is constructive, that is, we show an algorithm that guarantees to find a centroid in T. The idea is to start with v being any vertex in T and then iteratively moving v towards the "center" of the tree, until v becomes the centroid.

If T has just one vertex then this vertex is itself a centroid. If T has two vertices, then any of these two vertices can be chosen as a centroid. So from now on we can assume that $n \geq 3$.

Start with v being any vertex of T. Removing v partitions T into subtrees $T_1, T_2, ..., T_d$, where d is the degree of v. Let $s(v)$ denote the maximum size of these subtrees, that is $s(v) = \max_i |T_i|$. If $s(v) \leq n/2$ then v is a centroid, and we are done.

So suppose that $s(v) > n/2$, that is, there is some T_j for which $|T_j| > n/2$. (See the figure below, on the left.) There could only be one such T_j, because otherwise the total number of vertices would exceed n. Let x be the neighbor of v in this T_j. Consider the subtrees of T obtained after removing x. The subtree that contains v consists exactly of the set of vertices that are not in T_j, so its size is strictly less than $n/2$. All other subtrees are contained in T_j and do not include x, so their size is strictly less than the size of T_j. Therefore $s(x) < s(v)$.

We can thus move v to x, and this will decrease the value of $s(v)$. Therefore in each step, we either have that v is a centroid, or $s(v)$ decreases by at least 1. So after at most n steps this process needs to complete.