NAME: SID:

Problem 1: For each pseudocode below, give the number of letters printed as a function of n, using the Θ-notation. For the first three programs give a recurrence and its solution. For the last two programs, give the solution and a brief justification (at most 20 words).

<table>
<tr><th>pseudocode</th><th>Solution and recurrence or justification</th></tr>
<tr><td>procedure PrintAs(n)
  if $n > 1$ then
    print("A")
    PrintAs($n/3$)</td><td>$A(n) = A(n/3) + 1$

$A(n) = \Theta(\log n)$</td></tr>
<tr><td>procedure PrintBs(n)
  if $n > 1$ then
    for $j \leftarrow 1$ to $4n$
      do print("B")
    PrintBs($n/3$)
    PrintBs($n/3$)</td><td>$B(n) = 2B(n/3) + 4n$

$B(n) = \Theta(n)$</td></tr>
<tr><td>procedure PrintCs(n)
  if $n > 1$ then
    for $j \leftarrow 1$ to n^2
      do print("C")
    for $i \leftarrow 1$ to 5 do
      PrintCs($n/2$)</td><td>$C(n) = 5C(n/2) + n^2$

$C(n) = \Theta(n^{\log 5})$</td></tr>
<tr><td>procedure PrintDs(n)
  for $j \leftarrow 1$ to n do
    $k \leftarrow 1$
    while $k < n$ do
      print("D")
      $k \leftarrow 2k$</td><td>$D(n) = \Theta(n \log n)$

internal loop makes $\Theta(\log n)$ iterations
because k doubles at each step</td></tr>
<tr><td>procedure PrintEs(n)
  for $i \leftarrow 1$ to n^2 do
    for $j \leftarrow 1$ to $2n$ do
      print("E")</td><td>$E(n) = \Theta(n^3)$

for each of n^2 iterations of external loop
internal loop makes $2n$ iterations</td></tr>
</table>

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 1 and n that is relatively prime to $\phi(n)$, and $d = e^{-1} \pmod{\phi(n)}$
	Public and secret keys:	$P = (n, e)$, $S = d$

Encryption:	$E(M) = M^e \pmod n$	Decryption:	$D(C) = C^d \pmod n$

(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 an encoding of $M = 3$. If not, give a brief justification (at most 10 words).

p	q	e	d	correct?	justify if not correct / encode $M = 3$ if correct
5	7	5	5	Y	Computing modulo 35: $3^5 = 243 = 33$
11	27	13	55	N	27 is not a prime
17	5	5	13	Y	Computing modulo 85: $3^5 = 243 = 73$
11	11	3	67	N	p and q cannot be equal
7	11	5	27	N	$5^{-1} \not\equiv 27 \pmod{60}$

[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.

Theorem: Let p be a prime number and $a \in \{1, 2, ..., p-1\}$. Then $a^{p-1} \equiv 1 \pmod{p}$.

(b) Use Fermat's Little Theorem to compute the following values. In the second example, show your work.

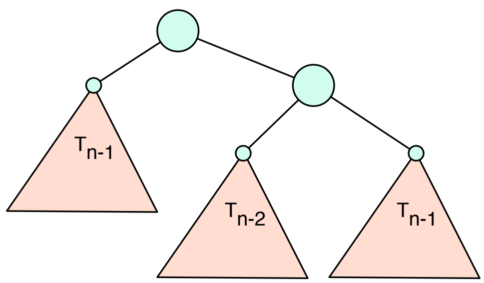
$35^{130} \,\mathrm{rem}\, 131 \; = \; 1$

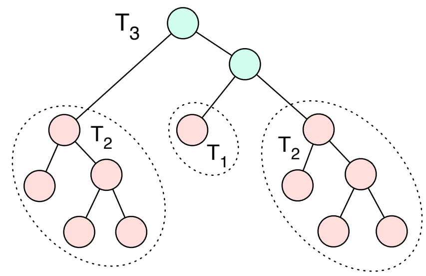
$3^{14074} \,\mathrm{rem}\, 71 \; = \; 10$

Computing modulo 71: $3^{14074} = 3^{14070} \cdot 3^4 = 1 \cdot 81 = 10$.

NAME: SID:

Problem 4: For each $n \geq 0$ we define a binary tree T_n as follows. T_0 is a single node and T_1 is also a single node. For $n \geq 2$, T_n is obtained by creating two new nodes and adding copies of T_{n-1} and T_{n-2} as their subtrees, as in the picture below on the left:





The picture on the right shows tree T_3 (with subtrees T_2 and T_1 marked).

Let A_n be the number of leaves in T_n. (For example, $A_0 = A_1 = 1$, $A_2 = 3$ and $A_3 = 7$, as can be seen in the picture above.) Give a formula for A_n. You need to show your work, all steps. First, give a recurrence equation with a brief justification. Then solve this recurrence. At each step explain what you are computing.

The recurrence is

$$\begin{aligned} A_n &= 2A_{n-1} + A_{n-2} \quad \text{for } n \geq 2 \\ A_0 &= 1 \\ A_1 &= 1 \end{aligned}$$

Justification for the recurrence: the leaves of T_n are either the leaves of two subtrees T_{n-1} or one subtree T_{n-2}.

The characteristic equation is $x^2 - 2x - 1 = 0$. The roots are $1 + \sqrt{2}$ and $1 - \sqrt{2}$. So the general solution is

$$A_n = \alpha_1(1 + \sqrt{2})^n + \alpha_2(1 - \sqrt{2})^n.$$

Using the initial conditions, we get equations:

$$\begin{aligned} \alpha_1 + \alpha_2 &= 1 \\ \alpha_1(1 + \sqrt{2}) + \alpha_2(1 - \sqrt{2}) &= 1 \end{aligned}$$

The solution is $\alpha_1 = \alpha_2 = \frac{1}{2}$. So the final solution is

$$A_n = \tfrac{1}{2}(1 + \sqrt{2})^n + \tfrac{1}{2}(1 - \sqrt{2})^n.$$

NAME: SID:

Problem 5: The Duggars are about to buy t-shirts for their 19 children, one for each. They need

- at least 2 blue t-shirts,
- at least 5 red t-shirts,
- at least 1 pink t-shirt, and
- at least 2 and not more than 10 yellow t-shirts.

How many different choices of t-shirt colors satisfy these requirements?

The answer is the number of non-negative integral solutions of

$$\begin{aligned} b + r + p + y &= 19 \\ 2 &\le b \\ 5 &\le r \\ 1 &\le p \\ 2 &\le y \le 10 \end{aligned}$$

After eliminating lower bounds (by substitutions), this reduces to computing the number of non-negative integral solutions of

$$\begin{aligned} b + r + p + y &= 9 \\ y &\le 8 \end{aligned}$$

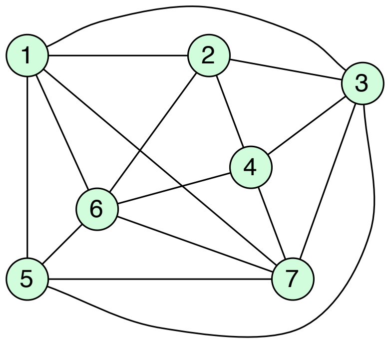
Let S be the number of all non-negative integral solutions and $S(P)$ the number of non-negative integral solutions that satisfy condition P. Then

$$S(y \le 8) = S - S(y \ge 9) = \binom{12}{3} - \binom{3}{3} = 220 - 1 = 119.$$

So the answer is 119.

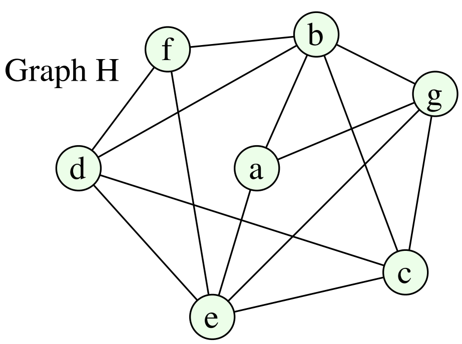
NAME: SID:

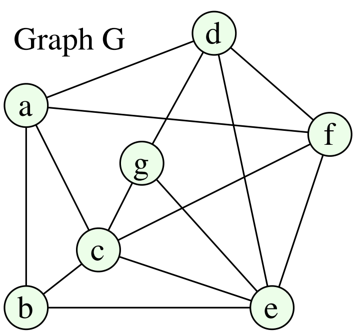
Problem 6: (a) Give Euler's inequality for planar graphs, and use it to show that the graph below is not planar.



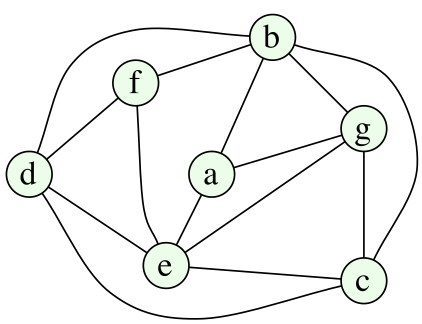
Euler's inequality: In a planar graph with $n \geq 3$ vertices the number of edges m satisfies $m \leq 3n - 6$.
In this graph we have $n = 7$ and $m = 16$. These numbers do not satisfy Euler's inequality, so G is not planar.

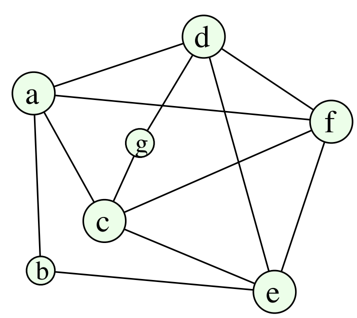
(b) Determine which of the following two graphs are planar. Justify your answer and show your work.





Graph H is planar. The picture below on the left shows a planar drawing of H. Graph G is not planar, because it contains a sub-division of K_5, shown below on the right.





NAME: SID:

Problem 7: Use induction to prove that $\sum_{k=1}^{n} k^3 = \frac{1}{4}n^2(n+1)^2$ for all integers $n \geq 1$.

Base case: For $n = 1$, the left-hand side is $\sum_{k=1}^{1} k^3 = 1$ and the right-hand side is $\frac{1}{4}1^2(1+1)^2 = 1$ as well.

Inductive step: Assume that $\sum_{k=1}^{n} k^3 = \frac{1}{4}n^2(n+1)^2$. We want to show that this equation holds for the next value of n, that is $\sum_{k=1}^{n+1} k^3 = \frac{1}{4}(n+1)^2(n+2)^2$. Starting from the left-hand side, and using the inductive assumption, we proceed as follows:

$$\begin{aligned}
\sum_{k=1}^{n+1} k^3 &= \sum_{k=1}^{n} k^3 + (n+1)^3 \\
&= \tfrac{1}{4}n^2(n+1)^2 + (n+1)^3 \\
&= \tfrac{1}{4}(n+1)^2[n^2 + 4(n+1)] \\
&= \tfrac{1}{4}(n+1)^2(n+2)^2.
\end{aligned}$$

as needed.

Problem 8: We have a set of $2n$ players in a chess tournament, where $n \geq 1$. Let $f(n)$ be the number of ways to divide them into pairs for the first round of the tournament. Prove that

$$f(n) = \frac{(2n)!}{2^n n!}.$$

For example, consider the case when $n = 2$, that is have four players. Lets call them A, B, C, D. There are three possible pairings: (AB, CD), (AC, BD), and (AD, BC). This agrees with the formula, because $f(2) = (2 \cdot 2)!/(2^2 \cdot 2!) = 4!/(4 \cdot 2) = 3$.

Hint: One way to approach this is to derive a recurrence equation for $f(n)$ and then prove that the above formula is its solution. Another way is to show a relation between pairings and permutations of the players.

Solution 1: For $n = 1$ we have two players and one pairing, so $f(1) = 1$. Consider some $n > 1$. The last player can be paired with any of the other $2n - 1$ players. Once we choose the pairing for the last player, the remaining players can be paired in $f(n-1)$ ways. Thus we have the recurrence

$$\begin{aligned} f(1) &= 1 \\ f(n) &= (2n-1)f(n-1) \end{aligned}$$

It remains to verify that the formula above satisfies this recurrence. Indeed:

$$\begin{aligned} (2n-1) \cdot f(n-1) &= (2n-1)\frac{(2(n-1))!}{2^{n-1}(n-1)!} \\ &= \frac{(2n-1)(2n-2)!}{2^{n-1}(n-1)!} = \frac{2n(2n-1)(2n-2)!}{2^n n!} = \frac{(2n)!}{2^n n!} = f(n), \end{aligned}$$

as claimed.

Solution 2: Consider any of the $(2n)!$ permutations of the players, say $x_1, x_2, ..., x_{2n}$. This permutation defines a pairing where each odd-numbered player is paired with the next player: $x_1x_2, x_3x_4, ..., x_{2n-1}x_{2n}$. However, each pairing can be obtained in many ways from this construction: in each pair the two players can be exchanged in two ways, for the total of 2^n ways, and the n pairs themselves can be obtained in any order, and there are $n!$ such orders. Therefore the number of pairings will be $(2n)!$ divided by $2^n n!$, which is exactly our formula.

Solution 3: Let's try brute force: pick the pairs one by one. The first pair can be selected in $\binom{2n}{2} = 2n(2n-1)/2$ ways. Once we choose this pair, the second pair can be chosen in $(2n-2)(2n-3)/2$ ways, and so on. This will give us

$$\frac{2n(2n-1)(2n-2)...1}{2^n} = \frac{(2n)!}{2^n}$$

ways to choose the pairings. However, the n pairs in each pairing can be selected in all possible orderings, and there are $n!$ such orderings. Thus we need to divide the above value by $n!$, which gives us $f(n) = (2n)!/(2^n n!)$.