# CS/MATH 111 SPRING 2015
# Final Test

- The test is 2 hours and 30 minutes long, starting at **8:00AM** 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.
- Calculators are not allowed.
- **Before** you start:
  - Make sure that your final has all 8 problems
  - Put your name and your student ID on *each* page

NAME: SID:

**Problem 1:** For each pseudo-code below, give the number of letters printed as a function of $n$, using the $\Theta$-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).

| Pseudo-code | Solution and recurrence or justification |
|---|---|
| **procedure** PrintAs($n$)<br>  **if** $n > 1$ **then**<br>  print("A")<br>  PrintAs($n/3$) | |
| **procedure** PrintBs($n$)<br>  **if** $n > 1$ **then**<br>  **for** $j \leftarrow 1$ **to** $4n$<br>  **do** print("B")<br>  PrintBs($n/3$)<br>  PrintBs($n/3$) | |
| **procedure** PrintCs($n$)<br>  **if** $n > 1$ **then**<br>  **for** $j \leftarrow 1$ **to** $n^2$<br>  **do** print("C")<br>  **for** $i \leftarrow 1$ **to** 5 **do**<br>  PrintCs($n/2$) | |
| **procedure** PrintDs($n$)<br>  **for** $j \leftarrow 1$ **to** $n$ **do**<br>  $k \leftarrow 1$<br>  **while** $k < n$ **do**<br>  print("D")<br>  $k \leftarrow 2k$ | |
| **procedure** PrintEs($n$)<br>  **for** $i \leftarrow 1$ **to** $n^2$ **do**<br>  **for** $j \leftarrow 1$ **to** $2n$ **do**<br>  print("E") | |

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 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 | | |
| 11 | 27 | 13 | 55 | | |
| 17 | 5 | 5 | 13 | | |
| 11 | 11 | 3 | 67 | | |
| 7 | 11 | 5 | 27 | | |

[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.

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

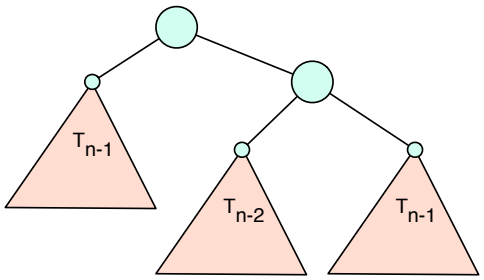
$35^{130} \operatorname{rem} 131 \; =$

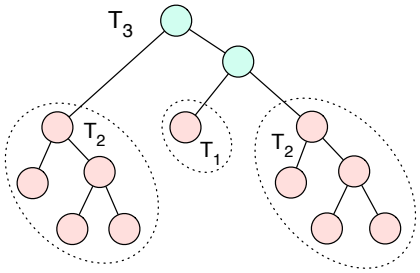
$3^{14074} \operatorname{rem} 71 \; =$

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.

NAME: SID:

---

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

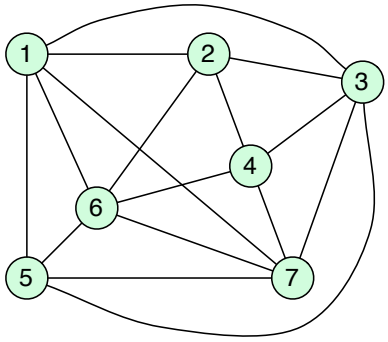
- at least 2 blue t-shirts,
- at least 5 red t-shirts,
- at least 1 pink t-shirt, and
- at least 2 and not more than 10 yellow t-shirts.

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

NAME: SID:

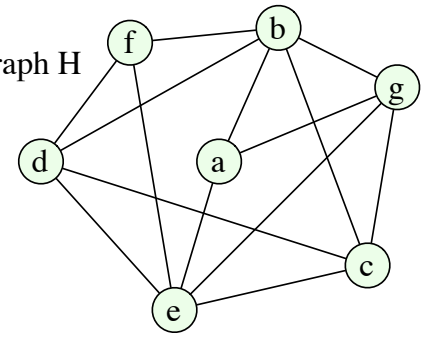
---

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

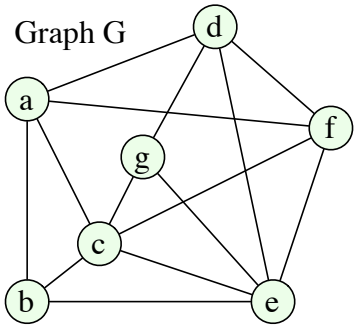



(b) Determine which of the following two graphs are planar. Justify your answer and show your work.

Graph H




Graph G



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 $n \geq 1$.

NAME: SID:

---

**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.