CS/MATH 111 Winter 2013
Final Test

- The test is 2 hours and 30 minutes long, starting at **7PM** and ending at **9:30PM**
- 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) For each pseudo-code below, give the *exact formula* for the number of words printed if the input is n (where $n \geq 1$), and then give its asymptotic value (using the Θ-notation.)

Pseudo-code	Formula	Asympt. value

procedure Ahem(n)
  for $j \leftarrow 1$ **to** $n+1$
    for $i \leftarrow 1$ **to** j
      do print("ahem")		

procedure Geez(n)
  if $n = 1$ **then**
   print("geez geez")
  else
    for $i \leftarrow 1$ **to** 3 **do**
      Geez($n-1$)		

(b) For each pseudo-code below, give a recurrence for the asymptotic value for the number of words printed if the input is n (where $n \geq 1$) and then its solution (using the Θ-notation.)

Pseudo-code	Recurrence	Solution

procedure Oops(n)
  if $n > 2$ **then**
    print("oops")
    Oops($n/3$)
    Oops($n/3$)		

procedure Eeek(n)
  if $n > 2$ **then**
    for $j \leftarrow 1$ **to** n
      do print("eeek")
    for $k \leftarrow 1$ **to** 4
      do Eeek($n/2$)		

procedure Whew(n)
  if $n > 1$ **then**
    for $j \leftarrow 1$ **to** n^2
      do print("whew")
    for $k \leftarrow 1$ **to** 5
      do Whew($n/2$)		

NAME: SID:

Problem 2: (a) Explain how the RSA cryptosystem works.

Initialization:	
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 not, give a brief justification (at most 10 words).

p	q	e	d	correct?	justify if not correct
23	51	18	89		
23	11	33	103		
3	7	5	5		
17	17	3	171		
11	7	13	37		

[1]For correctness it is only required that the decryption function is the inverse of the encryption function.

NAME: SID:

Problem 3: (a) Give a complete statement of the principle of inclusion-exclusion.

(b) We have three sets A, B, C that satisfy

- $|A| = |B| = 14$ and $|C| = 19$,
- $|A \cap B| = |A \cap C| = \frac{3}{14}|A \cup B \cup C|$ and $|B \cap C| = 8$,
- $|A \cap B \cap C| = 1$.

Determine the cardinality of $A \cup B \cup C$.

NAME: SID:

Problem 4: (a) Give a complete statement of Fermat's Little Theorem.

(b) Use Fermat's Little Theorem to compute the following values:

$78^{112} \pmod{113} =$

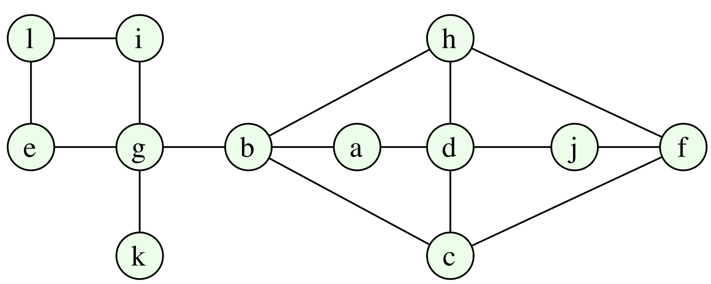
$3^{39635} \pmod{31} =$

NAME: SID:

Problem 5: (a) Give a complete definition of a perfect matching in a bipartite graph.

(b) State Hall's Theorem.

(c) Determine whether the graph below is bipartite and if it is, whether it has a perfect matching. You must give a complete justification for your answer.



NAME: SID:

Problem 6: (a) Prove or disprove the following statement: "If a graph G has an Euler tour then G also has a Hamiltonian cycle".

(b) Prove or disprove the following statement: "If a bipartite graph G has a Hamiltonian cycle then G has a perfect matching".

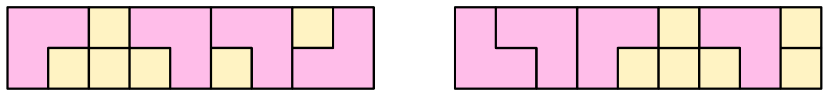
Problem 7: Using mathematical induction prove that

$$\sum_{i=0}^{n} 5^i \;=\; \frac{1}{4}(5^{n+1} - 1).$$

(Only proofs by induction will be accepted.)

NAME: SID:

Problem 8: We want to tile a $2 \times n$ strip with 1×1 tiles and L-shaped tiles of width and height 2. Here are two examples of such a tiling of a 2×9 strip:



Let $A(n)$ be the number of such tilings. (a) Give a recurrence relation for $A(n)$ and justify it. (b) Solve the recurrence to compute $A(n)$.