## CS/MATH 111 Winter 2011 Final Test

- The test is 2 hours and 30 minutes long, starting at 8:10AM and ending at 10:40AM
- 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 your student ID on each page

Problem 1: For each pseudo-code below, tell what is the number of words printed if the input is $n$. Give a recurrence and then its solution (expressed using the $\Theta()$ notation.)

| Pseudo-code | Recurrence and solution |
| :---: | :---: |
| procedure Geez ( $n$ ) if $n>1$ then print("geez") print("geez") Geez(2n/3) |  |
| procedure Caramba ( $n$ ) <br> if $n>1$ then <br> for $j \leftarrow 1$ to $3 n$ do print("caramba") <br> Caramba ( $n / 4$ ) <br> Caramba ( $n / 4$ ) |  |
| ```procedure \(\operatorname{Bummer}(n)\) if \(n>1\) then for \(j \leftarrow 1\) to \(n / 2\) do print("bummer") Bummer ( \(n / 3\) ) \(\operatorname{Bummer}(n / 3)\) Bummer ( \(n / 3\) )``` |  |
| procedure $\operatorname{Darn}(n)$ <br> if $n>1$ then <br> for $j \leftarrow 1$ to $n$ do print("darn") <br> for $j \leftarrow 1$ to 4 do $\operatorname{Darn}(n / 2)$ |  |

NAME:
SID:

Problem 2: Prove by induction that $1^{2}+2^{2}+\ldots .+n^{2}=n(n+1)(2 n+1) / 6$.

NAME: SID:

Problem 3: (a) Explain how the RSA cryptosystem works.

| Initialization: |  |
| :--- | :--- |
|  |  |
|  |  |
|  |  |
|  |  |
| Encryption: |  |
| Decryption: |  |

(b) Suppose that $p=3, q=29$, and $e=9$. Determine $d$. Compute the encryption of $M=3$.

Problem 4: We construct recursively binary trees $T_{0}, T_{1}, T_{2}, \ldots$, as follows. Both $T_{0}$ and $T_{1}$ consist of a single node. For $n \geq 2$, to obtain $T_{n}$, we link one copy of $T_{n-1}$ and three copies of $T_{n-2}$, as in the figure below:


Let $\ell_{n}$ be the number of leaves in $T_{n}$. For example, $\ell_{0}=1, \ell_{1}=1, \ell_{2}=4$. Give the formula for $\ell_{n}$. Show your work. The solution must consist of the following steps: (i) Set up a recurrence equation. (ii) Determine the characteristic equation and solve it. (iii) Give the general form of the solution. (iv) Compute the final answer.

Problem 5: (a) Give a complete statement of Hall's Theorem.
(b) For the two graphs below, tell whether they have a perfect matching or not. Justify your answer: either show the matching (say, by marking its edges in the picture or listing its edges) or use Hall's theorem to prove that it does not exist.


NAME:
SID:

Problem 6: Prove that each planar graph can be colored with at most 6 colors.

Problem 7: (a) Give a complete statement of the Inclusion-Exclusion principle.
(b) Things are not going well on Capitol Hill. The special prosecutor indicted 49 congressmen on various charges.

- Among them: 26 congressmen were indicted for bribery, 29 for fraud, and 19 for perjury.
- We further know that: $\mathbf{1 2}$ congressmen received indictments for bribery and fraud, $\mathbf{1 1}$ congressmen received indictments for bribery and perjury, and $\mathbf{9}$ congressmen received indictments for fraud and perjury.

Determine how many congressmen were indicted on all three charges? Show your work.

## NAME:

## SID:

Problem 8: Below you are given three relations on a set $X$. For each, determine whether it is (i) reflexive, (ii) symmetric, (iii) transitive, and (iv) antisymmetric. Then tell whether the relation is an equivalence relation or a partial order. If it is an equivalence relation, determine its equivalence classes. (You don't have to give proofs.)
(a) $X=\{a, b, c, d\}$ and $R$ is given by the following matrix:

|  | a | b | c | d |
| :---: | :---: | :---: | :---: | :---: |
| a | 1 | 1 | 0 | 0 |
| b | 0 | 1 | 0 | 0 |
| c | 1 | 1 | 1 | 0 |
| d | 1 | 1 | 0 | 1 |


| property | $\mathrm{Y} / \mathrm{N}$ |
| :--- | :--- |
| reflexive |  |
| symmetric |  |
| transitive |  |
| antisymmetric |  |

(b) $X=\{1,2,3,4,5,6\}$, and $x R y$ if and only if $x=y$ or $x^{2}+x \leq y^{2}+y$.

| property | $\mathrm{Y} / \mathrm{N}$ |
| :--- | :--- |
| reflexive |  |
| symmetric |  |
| transitive |  |
| antisymmetric |  |

(c) $X=\{2,3,4,5,8,24,27,128\}$, and $x R y$ if and only if $x$ and $y$ have exactly the same prime factors. (For example, $1183 R 637$, because $1183=7 \cdot 13^{2}, 637=7^{2} \cdot 13$.)

| property | $\mathrm{Y} / \mathrm{N}$ |
| :--- | :--- |
| reflexive |  |
| symmetric |  |
| transitive |  |
| antisymmetric |  |

