Algorithms CMSC-37000 Fourth Quiz. February 27, 2007
Instructor: László Babai

Name: ______________________________________

Show all your work. **Do not use book, notes, or scrap paper.** Write your answers in the space provided. When describing an algorithm in pseudocode, **explain the meaning of your variables** (in English). This quiz contributes 6% to your course grade.

1. (3+9 points) (a) Given the positive integers x and y, prove that x^y cannot be computed in polynomial time. (b) Given the positive integers x, y, m, compute the quantity $z = (x^y \bmod m)$ in polynomial time. Here $0 \le z \le m - 1$. Your algorithm should be direct, no recursive calls to itself. Give your solution in pseudocode. Use as few arithmetic operations as possible. Assuming each of x, y, m have n digits, estimate the number of multiplications/divisions of $O(n)$-digit integers required by your algorithm.

2. (3+9 points) Let $L_1 \subseteq \Sigma_1^*$ and $L_2 \subseteq \Sigma_2^*$ be two languages. (a) Define, what is a Karp-reduction from L_1 to L_2. (b) Let k-COL denote the set of k-colorable graphs (encoded in some natural way over a finite alphabet). Assuming 3-COL is NP-complete, prove that 4-COL is NP-complete. State what it is that you are reducing to what.

3. (2+6+7 points) (a) Define the CLIQUE language. (This language corresponds to the decision version of the "maximum clique" problem.) (b) Give a Karp-reduction from CLIQUE to HALTING. (c) Prove that there is no Karp-reduction from HALTING to CLIQUE.

4. (5+10 points) When asked to give a formal definition of NP, Dick gave this answer: "A language $L \subseteq \Sigma^*$ belongs to NP if and only if there exists a finite alphabet Σ_1 and a language $L_1 \subseteq \Sigma_1^*$ such that $L_1 \in P$ and $(\exists c)(\forall x \in \Sigma^*)(x \in L \Rightarrow (\exists y \in \Sigma_1^*)(|y| \leq |x|^c$ AND $(x, y) \in L_1)$." (a) Find the error in this definition; make the small change needed to correct it. (There is only one small error.) (b) Determine, exactly which languages L satisfy Dick's definition. Prove your answer.

5. (6 points) Describe the RSA (a) public key and (b) private key. Indicate the algorithms used in constructing them.

6. (Bonus problem, 6 bonus points) Let K be the set of those 3-colorable graphs which have fewer edges than vertices. Assuming 3-COL is NP-complete, prove that K is NP-complete,