Theoretical Cryptography	Manuel Blum and Steven Rudich
HW2	Due: 2/22/06

Rules: As usual, please cite all sources that you may use.

1. (a) Prove that $\mathsf{NP} \subseteq \mathsf{IP}$.
   (b) Recall the definition of PSPACE: a language L is in PSPACE if and only if there exists a Turing machine M and constant $k \geq 1$ such that M recognizes L, and on every input x, M uses at most $|x|^k$ tape cells.
   Prove that $\mathsf{IP} \subseteq \mathsf{PSPACE}$.

2. This question concerns the existence of "strong" interactive proof systems for a language, assuming that a "weak" one exists.

   (a) Suppose for a language L that there is an interactive proof system (P, V), where
   $$x \in L \implies \Pr[(P \leftrightarrow V)(x) \text{ accepts}] = 1$$
   $$x \notin L \implies (\forall \tilde{P}) \Pr[(\tilde{P} \leftrightarrow V)(x) \text{ accepts}] \leq 1/2.$$
   Prove that, for all $k > 1$, there is an interactive proof system (P_k, V_k) such that
   $$x \in L \implies \Pr[(P_k \leftrightarrow V_k)(x) \text{ accepts}] = 1$$
   $$x \notin L \implies (\forall \tilde{P}) \Pr[(\tilde{P} \leftrightarrow V_k)(x) \text{ accepts}] \leq \frac{1}{2^{|x|^k}}.$$

   (b) Suppose for a language L that there is an interactive proof system (P, V), where
   $$x \in L \implies \Pr[(P \leftrightarrow V)(x) \text{ accepts}] > 2/3$$
   $$x \notin L \implies (\forall \tilde{P}) \Pr[(\tilde{P} \leftrightarrow V)(x) \text{ accepts}] < 1/3.$$
   Prove that, for all $k > 1$, there is an interactive proof system (P_k, V_k), such that
   $$x \in L \implies \Pr[(P_k \leftrightarrow V_k)(x) \text{ accepts}] > 1 - \frac{1}{2^{|x|^k}}$$
   $$x \notin L \implies (\forall \tilde{P}) \Pr[(\tilde{P} \leftrightarrow V_k)(x) \text{ accepts}] < \frac{1}{2^{|x|^k}}.$$

3. What is the continued fraction expansion of...

   (a) $e = 2.71828\cdots$, the base of the natural logarithm?
   (b) $\phi = (\sqrt{5}+1)/2$, the golden ratio?
   (c) $\tan(1) = 1.5574\cdots$?

   For each of the three, show your work, and generate a few partial quotients. Guess a general rule for the partial quotients, *i.e.* a closed-form expression that gives the kth partial quotient for all k.

   Extra Credit: Prove that the general rules you guessed are correct.

   More Extra Credit: What is $1/(1+1/(2+1/(3+(1/4+\cdots))))$? Express your answer in some nice closed form.

4. Suppose a three-digit prime P has inverse $1/P = 0.00 \cdots 141592 \cdots$.

   (a) Exhibit a possible value for P.

   (b) Assuming your P is correct, what digit should come after the 2 in "141592"? What digit should come before the first 1 in "141592"?

   Show all of your work.

5. Show us something that you find interesting about continued fractions. Feel free to use Google; just say where you got what you did. If you come up with your own self-discovered something, be sure to tell us that you came up with it yourself.

6. **(Taken from *Knuth Vol.2, 4.5.3*)**
   A *quadratic irrationality* is a number of the form

$$X = (\sqrt{D} - U)/V,$$

   where D, U, V are integers, $D > 0$, $V \neq 0$, and D is not a perfect square. We may assume that V is a divisor of $D - U^2$, for otherwise the number may be rewritten as $(\sqrt{DV^2} - U|V|)/V|V|$.

   (a) Prove that the continued fraction expansion $X = q_0 + 1/(q_1 + 1/(q_2 + \cdots))$ of a quadratic irrationality $X = (\sqrt{D} - U)/V$ is obtained by the following formulas:

$$V_0 = V, \quad q_0 = \lfloor X \rfloor, \quad U_0 = U + q_0 V$$

$$V_{n+1} = \frac{D - U_n^2}{V_n}, \quad q_{n+1} = \left\lfloor \frac{\sqrt{D} + U_n}{V_{n+1}} \right\rfloor, \quad U_{n+1} = q_{n+1} V_{n+1} - U_n.$$

   (b) Prove that the continued fraction representation of an irrational number X is eventually periodic *if and only if* X is a quadratic irrationality. (This is the continued fraction analog of the fact that the decimal expansion of a real number X is eventually periodic iff X is rational.)