Problem Set 4

Please turn in each problem on a separate page with your name.

Read all of Chapter 7.

1. Let $MODEXP = \{\langle a, b, c, p \rangle | a, b, c, p$ are positive binary integers such that $a^b \equiv c \pmod{p}\}$. Show that $MODEXP \in P$.

2. Let $UNARY-SSUM$ be the subset sum problem in which all numbers are represented in unary, i.e., $1^k$ represents the number $k$. Why does the NP-completeness proof for $SUBSET-SUM$ (see textbook) fail to show $UNARY-SSUM$ is NP-complete? Show that $UNARY-SSUM \in P$.

3. Show that if $P = NP$, then every language $A \in P$, except $A = \emptyset$ and $A = \Sigma^*$, is NP-complete.

4. Let $CNF_k = \{ \langle \phi \rangle | \phi$ is a satisfiable cnf-formula where each variable appears at most $k$ times$\}$. Show that $CNF_2 \in P$.

5. Define $CNF_k$ as above. Show that $CNF_3$ is NP-complete.

6. Show that if $P = NP$, we can factor integers in polynomial time.
   (Note: The algorithm you are asked to provide computes a function, and NP contains languages, not functions. Therefore, you cannot solve this problem simply by saying “factoring is in NP and $P = NP$ so factoring is in P”. The assumption $P = NP$ implies that all languages in NP are in P, so you need to find an NP language that relates to the factoring function.)

7* (optional) The difference hierarchy $D_i P$ is defined recursively as
   i. $D_1 P = NP$, and
   ii. $D_i P = \{ A | A = B \setminus C \text{ for } B \in NP \text{ and } C \in D_{i-1} P \}$. (Here $B \setminus C = B \cap \overline{C}$.)
   For example, a language in $D_2 P$ is the difference of two NP languages. Let $DP = D_2 P$. Let $Z = \{ \langle G_1, k_1, G_2, k_2 \rangle | G_1$ has a $k_1$-clique and $G_2$ doesn’t have a $k_2$-clique$\}$.
   a. Show that $Z$ is complete for $DP$. In other words, show that $Z$ is in $DP$ and every language in $DP$ is polynomial time reducible to $Z$.
   b. Let $MAX-CLIQUE = \{ \langle G, k \rangle | \text{ a largest clique in } G \text{ is of size exactly } k \}$. Use part (a) to show that $MAX-CLIQUE$ is DP-complete.