18.404/6.840 Michael Sipser
Theory of Computation
Due via Gradescope 2:30pm sharp, Thursday, October 29, 2020 **Problem Set 4**

Read all of Chapter 7.

1. Let $MODEXP = \{\langle a, b, c, p\rangle \mid a, b, c, p$ are positive binary integers such that $a^b \equiv c \pmod{p}\}$. Show that $MODEXP \in$ P. (You can assume that basic arithmetical operations, such as $+$, $\times$, and mod, are computable in polynomial time.)

2. Let *UNARY-SSUM* be the subset sum problem in which all numbers are represented in unary, i.e., $\mathtt{1}^k$ 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. 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.)

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

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

7.* (optional) The ***difference hierarchy*** $\mathrm{D}_i\mathrm{P}$ is defined recursively as

   i. $\mathrm{D}_1\mathrm{P} = \mathrm{NP}$, and
   ii. $\mathrm{D}_i\mathrm{P} = \{A \mid A = B \setminus C$ for B in NP and C in $\mathrm{D}_{i-1}\mathrm{P}\}$. (Here $B \setminus C = B \cap \overline{C}$.)

   For example, a language in $\mathrm{D}_2\mathrm{P}$ is the difference of two NP languages. Let $\mathrm{DP} = \mathrm{D}_2\mathrm{P}$. Let

$$Z = \{\langle G_1, k_1, G_2, k_2\rangle \mid G_1 \text{ has a } k_1\text{-clique and } G_2 \text{ doesn't have a } k_2\text{-clique}\}.$$

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 $MAX\text{-}CLIQUE = \{\langle G, k\rangle \mid$ a largest clique in G is of size exactly $k\}$.
Use part (a) to show that *MAX-CLIQUE* is DP-complete.