CSE 6321 - Problem Set 2
Due lecture on April 2nd

Collaboration is permitted; looking for solutions from external sources (books, the web, material from previous years, etc.) is prohibited.

1. Let

$$M = \{\langle a, b, c, d\rangle : a, b, c \text{ and } p \text{ are binary integers}$$
$$\text{such that } a^b \equiv c \mod p\}.$$

   Show that $M \in P$. (Note that the most obvious algorithm does not run in polynomial time. Hint: Try first where b is a power of 2.)

2. Prove that the following language is undecidable:

$$A = \{\langle M\rangle : M \text{ is a TM with running time } O(n)\}.$$

3. Show that the following language is NP-complete:

$$\{\langle G_1, G_2\rangle : G_1,\ G_2 \text{ are undirected graphs}$$
$$\text{and } G_1 \text{ contains a subgraph isomorphic to } G_2\},$$

   "G_1 contains a subgraph isomorphic to G_2" means: there exist a set of vertices $V' \subseteq V(G_1)$ and a set of edges $E' \subseteq E(G_1)$ such that $|V'| = |V(G_2)|$, $|E'| = |E(G_2)|$, and there exists a one-to-one function $f : V(G_2) \to V'$ satisfying $\{u, v\} \in E(G_2)$ iff $\{f(u), f(v)\} \in E'$.

4. Show that the following problem is NP-complete: "Given $\langle S, C\rangle$, where C is a collection of subsets of a finite set S, determine whether there is a partition of S into two subsets S_1, S_2 so that no set in C is entirely contained in either S_1 or S_2."

   Hint: 3-SAT.

5. Say that two Boolean formulas are equivalent if they have the same set of variables and are true on the same set of assignments to those variables (i.e., they describe the same Boolean function). A Boolean formula is *minimal* if no shorter Boolean formula is equivalent to it. Let MIN-FORMULA be the collection of minimal Boolean formulas. Show that, if $P = NP$, then MIN-FORMULA $\in P$.