Math 387

Homework 6

Due Wednesday, October 14

Practice exercises from the book

7.1, 7.2, 7.7, 7.11, 7.13, 7.19

Problems

1. Take $MODEXP = \{< a, b, c, p > \mid a, b, c$ and p are binary integers and $a^b \equiv c \pmod{p}\}$. Show that $MODEXP \in P$. (Hint: The obvious algorithm doesn't run in polynomial time. Try it first where b is a power of 2.)

2. Show that P is closed under union, concatenation, and complement.

3. Let $3COLOR$ be the set of 3-colorable graphs. That is, $3COLOR = \{< G > \mid G$ is a graph, and we can assign each node of G one of three colors such that no two nodes of G that are connected by an edge have the same color)$\}$. Show that $3COLOR \in NP$.

Bonus problems

1. Show that if $P = NP$ we can construct a polynomial-time algorithm to find a satisfying assignment for a given satisfiable boolean formula. (Note: If $P = NP$ that means that SAT is in P, but P as we have defined it contains languages, and machines give yes/no answers. What you are being asked to do here is create a machine that computes a function. You can think of this as a Turing machine that starts with the input on its tape, and then eventually halts with the ouptut of the function on its tape instead.)