CS401 - Problem Set 3

Note: Most of you will probably find these problems challenging. I hope you will also find them interesting, or in the best case, fun to puzzle over. Make sure you give yourself time. It will likely take several nights of sleep before your brain is ready for that creative insight!

1. (a) Prove if $L' \in \mathbf{NP}$ and $L \leq_p L'$, then $L \in \mathbf{NP}$.
   (b) Please explain in English what this statement is saying (roughly - go for big-picture meaning instead of precision).

2. (a) *A unary language L is a subset of $\{1\}^*$. Let $\mathbf{NP}_U$ be the set of unary languages that are also in **NP**. Prove that if $\mathbf{NP}_U \subseteq \mathbf{P}$, then $\mathbf{EXP} = \mathbf{NEXP}$, where **NEXP** is defined similarly to **NP** except now the TM can run for exponential time in the size of the input, and the witness u can be of exponential size in the size of the input.
   (b) The above result seems to imply that it is easier to prove $\mathbf{EXP} = \mathbf{NEXP}$ than $\mathbf{P} = \mathbf{NP}$. Please explain why on the surface it seems this way. Can you explain why this might not actually be the case? Would it make sense that it is easier to say something about the **EXP** vs **NEXP** problem instead of the **P** vs **NP** problem? What might this tell us about the difficulty of solving unary problems?

3. **Please start thinking about this problem this week - but it won't be due until next week.**
   Let

   $\mathsf{QUADEQ} = \{\langle x \rangle : x \text{ is a set of binary quadratic equations modulo 2 with a satisfying assignment}\}$.

   Examples of binary quadratic equations modulo 2 are:

   $$u_1u_1 + u_2u_3 = 0 \pmod 2 \tag{1}$$
   $$u_1u_4 + u_2u_5 + u_2u_4 = 1 \pmod 2 \tag{2}$$

   where each u_i must equal 0 or 1.

   Prove that $\mathsf{QUADEQ} \in$ **NP**-Hard.