CS401 - Problem Set 3

1. **[Moved to Pset 4]** In class, we discussed how the definition of $\mathbf{NP}$ involving a witness (perhaps) captures the creativity involved in problem solving. Now that we've seen the NTM definition of $\mathbf{NP}$, can you make a connection between creativity and our new definition?

2. Prove that the language HALT is $\mathbf{NP}$-HARD but not $\mathbf{NP}$-Complete, where

$$\mathsf{HALT} = \{\langle \alpha, x\rangle : \alpha \text{ describes the TM } M_\alpha, \text{ and } M_\alpha \text{ halts on input } x\}. \tag{1}$$

   See Theorem 1.11 (book), §1.4.1 (online) for more on HALT, and last page for a hint.

3. * (It took me two nights of sleeping on it to figure this one out. Make sure you give yourself time to play around with different ideas. You may find it is a bit of an addictive puzzle. Or maybe it will come to you immediately - the creative insight!)

   A quadratic equation is defined by a parameter n, a binary string of length n^2 : $a = a_{11}a_{12}\ldots a_{1n}a_{21}a_{22}\ldots a_{nn}$ and a bit b. A binary string $u = u_1u_2\ldots u_n$ is a satisfying assignment if

$$\sum_{i\in n}\sum_{j\in n} a_{ij}u_iu_j = b \mod 2. \tag{2}$$

   Let x describe a set of m quadratic equations each with the same parameter n. Then $x \in \mathsf{QUADEQ}$ if there is a string u that is a satisfying assignment for all m quadratic equations in the set x.

   Prove that $\mathsf{QUADEQ} \in \mathbf{NP}$-COMPLETE.

Hint on 2: You don't need to reduce 3SAT to Halt, but can go do a reduction directly from the definition of **NP**. The reduction should create a description of a TM, since that is the form of the input to **HALT**. While it must take polynomial time to create the description, the TM that you describe does not have to take polynomial time to run, and probably should not halt on certain inputs.