

Assignment 12

We keep talking about all these NP-Complete problems but I'm not sure if it's really sunk in why these problems are even vaguely interesting. Most of the questions below (aside from 4) are directly from lecture.

Let $\mathbf{P}$ denote the class of all problems that have a polynomial time algorithm that gives the correct output on all possible inputs.

Let $\mathbf{NP}$ denote the class of all problems that for which we can verify a "solution" to the problem in a polynomial amount of time.

1. Convince me that all problems in $\mathbf{P}$ are also in $\mathbf{NP}$.
2. What would it mean about the "difficulty" of problems in $\mathbf{NP}$ if $\mathbf{P} = \mathbf{NP}$?
3. Check out https://simple.wikipedia.org/wiki/RSA_algorithm and https://en.wikipedia.org/wiki/Integer_factorization#Difficulty_and_complexity. RSA algorithms are involved in a wide variety things, including many password protection models. These encryption schemes only 'work' so long as nobody knows how to factor integers 'quickly', say in a polynomial amount of time. Currently, the state of the art algorithms to factor integers are relatively slow.
4. Convince me that the problem of determining the prime factors of an integer is in $\mathbf{NP}$. And hence, if $\mathbf{P} = \mathbf{NP}$, then you could crack RSA encryption.
5. Let A be any $\mathbf{NP}$ -COMPLETE problem. Convince me that if A is in $\mathbf{P}$, then $\mathbf{P} = \mathbf{NP}$.
6. Let A be $\mathbf{NP}$ -COMPLETE problem. Convince me that if A is not in $\mathbf{P}$, then $\mathbf{P} \neq \mathbf{NP}$.

Make sure you understand those last two - I am certain that they will appear on the exam in some way.