

## Problem Set 8

This problem set is due on **Thursday November 10, by 5:00pm.**

Use the CS172 drop box.

Write **your name and your student ID number** on your solution. Write legibly. The description of your proofs should be as *clear* as possible (which does not mean *long* – in fact, typically, good clear explanations are also short.) Be sure to be familiar with the collaboration policy, and read the overview in the class homepage [www.cs.berkeley.edu/~luca/cs172](http://www.cs.berkeley.edu/~luca/cs172).

---

1. Formulate factorization as a language. That is, describe a language  $L$  such that  $L \in \mathbf{P}$  if and only if there is a polynomial time algorithm to (completely) factor positive integers (where the input is the binary representation of the integer). In addition, prove that your language has the required property.

2. Define  $\text{coNP}$  to be the class of languages  $L$  such that  $\bar{L} \in \mathbf{NP}$ , where  $\bar{L}$  is the complement of  $L$ .

Prove that  $\mathbf{NP} = \text{coNP}$  if and only if there is an  $\mathbf{NP}$ -complete problem in  $\text{coNP}$ .

3. (Sipser problem 7.17.) Prove that if  $\mathbf{P} = \mathbf{NP}$  then every language in  $\mathbf{P}$ , except  $\emptyset$  and  $\Sigma^*$ , is  $\mathbf{NP}$ -complete.

Why can't  $\emptyset$  and  $\Sigma^*$  be  $\mathbf{NP}$ -complete?