**Problem 1: Factoring, NP, and coNP**

Consider the factoring decision problem:

$$\text{FACTORING} := \{(N, L, U) : \exists \text{ prime } p \text{ s.t. } p \mid N, L \leq p \leq U\}.$$ 

That is, the factoring decision problem is to decide whether $N$ has a prime factor between $L$ and $U$.

The factoring search problem is: Given $N \geq 2$, find primes $p_1, \ldots, p_n$ (not necessarily distinct) such that $p_1 \cdot \ldots \cdot p_n = N$.

(a) Assume you have a polynomial-time Turing machine $M$ that solves the factoring search problem.\(^1\)

Construct a polynomial-time Turing machine $M'$ that solves FACTORING\(^2\).

**Note:** You do not need to describe the Turing machine in detail (giving the list of states, symbols, transition function). It is sufficient to describe the algorithm in pseudocode. You do not need to prove that the resulting Turing machine is polynomial-time (but it should be polynomial-time). You may assume without proof that there is a polynomial-time algorithm that decides whether a number is a prime.

(b) Construct an polynomial-time oracle Turing machine $M$ such that $M^{\text{FACTORING}}$ solves the factoring search problem.\(^3\)

**Note:** Same as the note in (a).

**Hint:** Do a binary search for the smallest prime factor first. And then use recursion.

(c) Show that FACTORING $\in$ NP.

**Note:** It is sufficient to say what the certificate $u$ is and what the Turing machine $M((N, L, U), u)$ computes. You may assume without proof that there is a polynomial-time algorithm that decides whether a number is a prime.

---

\(^1\)That is, for any positive $N$, we have $M(N) = (p_1, \ldots, p_n)$ such that all $p_i$ are prime and $p_1 \cdot \ldots \cdot p_n = N$.

\(^2\)That is, $M'(N, L, U) = 1$ iff $(N, L, U) \in \text{FACTORING}$.

\(^3\)If you were not in the practice session: the definition of an oracle Turing machine is given in Arora-Barak, Sec. 3.4.
(d) Show that FACTORING $\in$ coNP.

**Note:** Same as the note in (c).

**Hint:** Prime factors.

(e) **(Bonus points)** Show that if FACTORING is NP-complete, then NP = coNP.

**Note:** For this reason, it is commonly assumed that factoring is not NP-complete. (Since it is believed that NP $\neq$ coNP.)

**Hint:** For an $L \in$ NP, show that $L \leq_p$ FACTORING. Then show $L \in$ NP and $L \in$ coNP. Then you will have shown NP $\subseteq$ coNP. For the other direction, proceed similarly. Recall that $\overline{L}$ denotes the complement of $L$. 