Problem 3.1. (0.25 pt) An oracle machine M is called *Zosia Samosia* if $L(M^K) = L(M^\emptyset)$ for every language K, i.e., if for every oracle the language recognized by M remains the same (but the running time may differ). Let **ZSP** be the class of languages that can be recognized in polynomial time by some Zosia Samosia with some oracle. Prove that **ZSP** = **NP** ∩ **coNP**.

Problem 3.2. (0.25 pt) There are two persons: Alice and Bob. They both know an undirected graph $G = (V, E)$. Moreover, Alice knows a set $A \subseteq V$, and Bob knows a set $B \subseteq V$. Alice and Bob want to check whether there is a triangle (i.e., a 3-node clique) in the set $A \cup B$, but they want to limit the length of messages they send to each other. They may benefit from a help of a wizard Merlin, who knows both A and B (as well as G), but who is biased: he wants to convince Alice and Bob that there is no such triangle.

Design a probabilistic protocol of the following shape (where $n = |V|$):

1. Merlin sends $O(\sqrt{n} \cdot \log n)$ bits of information to Alice;
2. Bob tosses $O(\log n)$ coins;
3. Bob sends $O(\sqrt{n} \cdot \log n)$ bits of information to Alice;
4. Alice accepts or rejects.

Alice and Bob should work in polynomial time. If there is no triangle in $A \cup B$, there should exist a message from Merlin such that Alice always rejects, otherwise (for every message from Merlin) Alice should accept with probability $\geq \frac{1}{2}$. We assume that Alice and Bob are honest, and that Merlin does not know the future (in particular, Bob's random bits).

Hint As a starting point consider the following protocol for checking whether the sets A and B are disjoint. For simplicity, we present it only for the case when $\sqrt{n} \in \mathbb{Z}$. Suppose that $V = \{1, \ldots, n\}$ and denote $k = \sqrt{n}$. Let p be the smallest prime number such that $p \geq 4n$. Let $Q_1, \ldots, Q_k, R_1, \ldots, R_k$ be polynomials in $\mathbb{Z}_p[x]$ of degree at most $k-1$ such that for all $i, j \in \{1, \ldots, k\}$ it holds that

- $Q_i(j) = 1$ iff $(i-1)k + j \in A$,
- $Q_i(j) = 0$ iff $(i-1)k + j \notin A$,
- $R_i(j) = 1$ iff $(i-1)k + j \in B$,
- $R_i(j) = 0$ iff $(i-1)k + j \notin B$,

The protocol is as follows:

1. Merlin sends to Alice coefficients of a polynomial $P \in \mathbb{Z}_p[x]$ of degree at most $2(k-1)$.
2. Bob draws $l \in \mathbb{Z}_p$ uniformly at random.
3. Bob sends to Alice l and $R_i(l)$ for all $i \in \{1, \ldots, k\}$.
4. Alice accepts if $P(j) = 0$ for all $j \in \{1, \ldots, k\}$ and $P(l) = \sum_{i=1}^{k} Q_i(l) \cdot R_i(l)$; otherwise she rejects.

If $A \cap B = \emptyset$, there exists a message from Merlin such that Alice always accepts, otherwise Alice rejects with probability $\geq \frac{1}{2}$. (This hint is given without any proof, but in your solution you should prove all required properties.)