Problem 3.1. (6 pt) Prove that there exists a deterministic Turing machine with oracle for SAT that works in polynomial time, and that given a positive integer n finds its decomposition into prime numbers:

$$n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k},$$

where $p_1 < \cdots < p_k$ are prime numbers, and $\alpha_1, \ldots, \alpha_k$ are positive integers.
Remark. It is known that there is a primality test working in polynomial time (AKS).
Remark. A Turing machine with oracle for $X \subseteq \{0,1\}^*$ is a Turing machine equipped with an additional query tape. After writing some word to the query tape, it can enter a special query state, and then it instantly receives a (binary) answer whether the word belongs to X. The machine continues its computation, maybe asking further questions to the oracle.

Problem 3.2. (6 pt) For a language $L \subseteq \{0,1\}^*$, let

$$B(L,r) = \{u \mid \exists v \in L.\ d(u,v) \leq r\}$$

where $d(u,v)$ is the Hamming distance,

$$d(u,v) = \begin{cases} |\{i : u_i \neq v_i\}| & \text{if } |u| = |v|, \\ \infty & \text{if } |u| \neq |v|. \end{cases}$$

Show that for each $L \subseteq \{0,1\}^*$ and each $r \in \mathbb{N}$
(a) if $L \in \mathsf{RP}$ then $B(L,r) \in \mathsf{RP}$;
(b) if $L \in \mathsf{coRP}$ then $B(L,r) \in \mathsf{coRP}$.