Zadanie domowe nr 3

Rozwiązania należy wysyłać na adres `niwinski@mimuw.edu.pl`
do **poniedziałku, 1 czerwca, godz. 23:59**.

Problem faktoryzacji określamy następująco.
Dla danej liczby naturalnej $n \geq 1$, znaleźć jej rozkład na czynniki pierwsze, dany w postaci ciągu liczb naturalnych $p_1, \alpha_1, \ldots, p_k, \alpha_k$, gdzie $p_1, \ldots, p_k$ są pierwsze i

$$n \quad = \quad p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}. \tag{1}$$

Wszystkie liczby są reprezentowane binarnie.

Uwaga. Dla wykazania, że rozwiązanie jest poprawne, należy sprawdzić nie tylko równość (1), ale także, że p_i są pierwsze. Wiadomo, że istnieje deterministyczny wielomianowy test pierwszości (AKS).

Maszyna z wyrocznią $X \subseteq \{0,1\}^*$ jest deterministyczną maszyną Turinga wyposażoną dodatkowo w taśmę pytań. Po napisaniu na tej taśmie jakiegoś słowa maszyna może wejść w stan pytający i wtedy w jednej chwili otrzymuje (binarną) odpowiedź, czy to słowo należy do X. Maszyna kontynuuje obliczenie, być może zadając kolejne pytania.

Polecenie: Dowieść, że istnieje maszyna z wyrocznią SAT, która w czasie wielomianowym rozwiązuje problem faktoryzacji.