

1. Consider the *EWM* (exponentiation with modulo) problem:

Input: Integers a , b , c , and d .

Question: Is $a^b = c \pmod{d}$?

- (a) Consider the following algorithm:

- Let $p = 1$
- For $i = 1$ to b
- $p = p \cdot a$.
- If $p = c \pmod{d}$, return “Yes” otherwise return “No”.

(a) This algorithm provides you with the correct answer. However, describe why it does not show that $EWM \in P$.

(b) Show that $EWM \in P$.

2. We say that two graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ are isomorphic to each other if there is a one-to-one and onto mapping $\pi : V_1 \rightarrow V_2$ (in other words, π is a permutation mapping the nodes of G_1 to the nodes of G_2) such that $(u, v) \in E_1$ iff $(\pi(u), \pi(v)) \in E_2$.

Define the problem *SUB-ISO* as follows:

Input: Undirected graphs G and H .

Question: Is H isomorphic to some subgraph of G ?

Show that *SUB-ISO* is NP-Complete.

3. We define the problem SET-BREAKING as follows:

Input: Finite set S and $C = \{C_1, \dots, C_k\}$, where each C_i is a subset of S .

Question: Can the elements of S be colored *red* or *blue* in such a way that no C_i has all its elements colored with the same color.}

Show that SET-BREAKING is NP-Complete. Hint: one possible reduction uses *3SAT*.

4. A Hamiltonian cycle in a graph G is a cycle that goes through every node of the graph exactly once. Show that if $P = NP$, then we can find a Hamiltonian cycle in G (if one exists) in polynomial time. Keep in mind that both P and NP are classes of decision problems, but here we want to actually find the actual cycle.