

A permutation on the set $\{1, 2, \dots, k\}$ is a one-to-one, onto function on this set. If p is a permutation then p^t says that the composition of p with itself t times.

The **PERM-POWER** is defined as follows:

PERM-POWER = $\{ \langle p, q, t \rangle \mid p = q^t \text{ where } p \text{ and } q \text{ are permutations on } \{1, \dots, k\} \text{ and } t \text{ is a binary integer} \}$

The binary integer t can be represented as $t = x_0 2^0 + x_1 2^1 + \dots + x_n 2^n$ where x_i acquires a value either 0 or 1.

Now, q^t can be written as,

$$\begin{aligned} q^t &= q^{x_0 2^0 + x_1 2^1 + \dots + x_n 2^n} \\ &= q^{x_0 2^0} \times q^{x_1 2^1} \times \dots \times q^{x_n 2^n} \end{aligned}$$

From this, compute q^{2^j} where $j = 1, 2, \dots, \lfloor \log t \rfloor$. By substituting j value, q^{2^j} can be $q^1, q^2, q^4, q^8, \dots$. It is easy to compute the permutation by applying q on q itself. It takes $O(k \log t)$ steps to compute q^{2^j} where each product requires $O(k)$ steps. Finally, the value of q^{2^j} is compared with p which takes additional k steps. Thus, it can be said that **PERM-POWER** $\in P$.