06IMO5

Himadri Mandal

December 23, 2021

§1 Solution

Solution. Huh. Very nice.

Lemma

For any $P \in \mathbb{Z}[X]$, and $m \in \mathbb{Z}$ with $P^k(m) = m \implies k \in \{1, 2\}$

Proof.

$$m - P(m)|P(m) - P(P(m))| \cdots |P^{k-1}(m) - m|m - P(m)$$

So, $\dfrac{P^{i+1}(m) - P^i(m)}{P^i(m) - P^{i-1}(m)} = \{-1, 1\} \forall i$, if this equals -1 atleast once then,

$$P^c(m) = P^{c-2}(m) \implies P(P(m)) = P^{gk+2}(m) = P^{gk}(m) = m$$

So $P^k(m) - P^{k-1}(m) = P^{k-1}(m) - P^{k-2}(m) = \cdots = P(m) - m$, which means $m = P^k(m) = m + k(P(m) - m)$, so we are done. □

Using this lemma we reduce the problem to $k = 2$. Define $\#_{\mathbb{Z}}(P(x))$ to be the number of distinct integer roots of $P(x)$. Let $S_1 = \{a_i\}_{i \le k_1}$ be the set of integers with cyclicity 1 and $S_2 = \{b_i\}_{i \le k_2}$ be the set of integers with cyclicity 2. If S_2 is empty we are done, so assume not.

Claim — $\#_{\mathbb{Z}}(P(P(x)) - x) \le n$

Proof. If $|S_1| \neq 0$ then

$$b_i - a_1 | P(b_i) - a_1 | b_i - a_1$$

$\implies P(b_i) - a_1 = a_1 - b_i \implies P(b_i) = 2a_1 - b_i = 2a_j - b_i$ thus $S_1 = \{a_1\}$. But then clearly $P(x) - 2a_1 + x$ has all of $S_1 \cup S_2$.

If $|S_1| = 0$ then

$$b_1 < \cdots < b_{k_2}$$

$$b_i - b_1 | P(b_i) - P(b_1) | b_i - b_1$$

Assume there exist $p > q > 1$ then $P(b_p) - P(b_1) = b_p - b_1$ and $P(b_q) - P(b_1) = b_1 - b_q$ $P(b_p) - P(b_q) = |b_p + b_q - 2b_1| = b_p - b_q$ which is absurd. Therefore, $\{b_i\}$ are all either the roots of $P(x) + x - (P(b_1) + b_1)$ or $P(x) - x - (P(b_1) - b_1)$. So we are done by fundamental theorem. ■
