IMO 2025 P3 Solution

ByteDance Seed AI4Math

17 July 2025

This is a compilation of ByteDance Seed AI4Math team's solutions to the 2025 IMO competition. All of the solutions are generated by Artificial Intelligence (AI) methods. However, to help human graders, ByteDance Seed Prover team translates the machine proof into natural language (English) solutions by human, with the original machine proof attached. Some very minor proof details may be omitted and can be checked in the LEAN version. The proof of IMO 2025 P3 has been fully verified under LEAN v4.14.0.

§1 IMO 2025/3

Problem statement

Let $\mathbb{N}$ denote the set of positive integers. A function $f\colon \mathbb{N} \to \mathbb{N}$ is said to be *bonza* if $f(a)$ divides $b^a - f(b)^{f(a)}$ for all positive integers a and b. Determine the smallest real constant c such that $f(n) \leqslant cn$ for all bonza functions f and all positive integers n.

Claim — When $c = 4$, there exists a function f is *bonza*.

Proof.

$$f(k) = \begin{cases} 16 & \text{if } k = 4, \\ 1 & \text{if } 2 \nmid k, \\ 2 & \text{if } 2 \mid k \wedge k \neq 4. \end{cases}$$

To prove that f is bonza, we first consider $a = 4$. When $b = 4$, it is clear that $16 \mid 4^4 - 16^{16}$. When $2 \nmid b$, we have $16 \mid b^4 - 1$ by enumerating $b \equiv 1, 3, 5, 7, 9, 11, 13, 15 \mod 16$. When $2 \mid b \wedge b \neq 4$, it is trivial that $16 \mid b^4 - 2^{16}$. When $2 \nmid a$, we need to prove $1 \mid b^a - f(b)$ which is true. When $2 \mid a \wedge a \neq 4$, we need to prove $2 \mid b^a - f(b)^2$. This is true since b and $f(b)$ have the same parity. □

Claim — $f(1) = 1$

Proof. Let $a = b = 1$, we have $f(1) \mid 1 - f(1)^{f(1)}$. Since $f(1) \mid f(1)^{f(1)}$, we have $f(1) \mid 1$ and $f(1) = 1$. □

Claim — For any prime p, $f(p) = p^k$.

Proof. Set $a = b = p$, we have $f(p) \mid p^p - f(p)^{f(p)}$. And this means $f(p) \mid p^p$. So there exists $k \in \mathbb{N}$, $f(p) = p^k$. $\square$

Claim — For any $b \in \mathbb{N}+$ and any prime number p, if $f(p) \neq 1$ then $b \equiv f(b) \mod p$.

Proof. Since $p \mid f(p)$ and $f(p) \mid b^p - f(b)^{f(p)}$. By Fermat's little theorem, we have $p \mid b - f(b)$. $\square$

Claim — If f is not the identity function, for any $k \in \mathbb{N}+$, there exists a prime $p > k$ and $f(p) = 1$.

Proof. If not, for any prime $p > k, f(p) \neq 1$. Since f is not the identity function, we have i_0, s.t. $f(i_0) \neq i_0$. We take $M = \max(k, i_0, f(i_0))$, $q > M$ which is a prime. Since $i_0 \equiv f(i_0) \mod q$, $q > i_0$, and $q > f(i_0)$. This contradicts to $f(i_0) \neq i_0$. $\square$

Claim — If f is not the identity function, p_0 is a prime number and $f(p_0) = 1$. For any prime $p \geq p_0$, we have $f(p) = 1$.

Proof. We have $p \mid p_0 - f(p_0)$, which is the same as $p \mid p_0 - 1$. This contradicts to $p \geq p_0$. $\square$

Claim — If f is not the identity function, for any odd prime number p, $f(p) = 1$.

Proof. We obtain a prime number $p_0 > p, f(p_0) = 1$. We also have for any prime number $q \geq p_0, f(q) = 1$. From Dirichlet's theorem, we have a prime number q, s.t. $q > p_0, q \equiv 2 \mod p, f(q) = 1$. We also have $p \mid q - 1$. This contradicts $p \mid q - 2$. $\square$

Claim — If f is not the identity function, for any n, $f(n) = 2^k$.

Proof. We only need to prove that 2 is the only possible prime factor of $f(n)$. When n is an odd prime number, $f(n) = 1$. For other cases, we take q is a prime factor of $f(n)$. If $q > 2$, we have $f(q) = 1$. Then $q \mid q - f(q)$ which means $q \mid q - 1$. This is impossible. $\square$

Claim — If f is not the identity function, for any n, $f(n) \mid 3^n - 1$.

Proof. Set $a = n, b = 3$ with $f(b) = 1$. It is obvious $f(a) \mid 3^n - 1$. $\square$

Claim — $f(n) \leq 4n$

Proof. If f is the identity function, $f(n) \leq n \leq 4n$. If f is not the identity function, $f(n) = 2^k \leq 2^{v_2(3^n-1)}$. If n is odd, $v_2(3^n - 1) = 1$, $f(n) \leq 2$. If n is even, $v_2(3^n - 1) = 2 + v_2(n)$, $f(n) \leq 2^{2+v_2(n)} \leq 4n$. $\square$