SMO 2020/4

Evan Chen

Twitch Solves ISL

Episode 27

Problem

Let $p > 2$ be a fixed prime number. Find all functions $f\colon \mathbb{F}_p \to \mathbb{F}_p$, such that $f(f(n)) = f(n+1) - 1$ for all n.

Video

https://youtu.be/8IjDBRNMGI0

Solution

Only the identity function works.

Claim. f is bijective.

Proof. The function f is surjective since $f(f(n)) = f(n+1) - 1$ means that if y is in the range of f, then so is $y - 1$. Since the domain and codomain are finite with equal cardinality, this implies it is actually a bijection. □

Claim. For every integer $e \geq 1$ we have the statement

$$P_e(n): \qquad f^{2^e}(n) + e = f(n+e).$$

Proof. The statement P_1 is given. By applying f to both sides of $P_1(n)$ we have

$$f^2(f^2(n)) + 1 \overset{P_1(f^2(n))}{=} f(f^2(n) + 1) = f^2(n+1) \overset{P_1(n+1)}{=} f(n+2) - 1$$

and thus we arrive at the statement

$$P_2(n): \qquad f^4(n) + 2 = f(n+2)$$

which is the statement P_2.

Take f of both sides again and

$$f^8(n) + 2 \overset{P_2(f^4(n))}{=} f(f^4(n) + 2) = f(f(n+2)) \overset{P_1(n)}{=} f(n+3) - 1$$

which gives the statement P_3 and repeating this argument yields the general claim. □

Now we have in particular that $f^{2^p}(n) = f(n)$, and hence all elements of $\mathbb{F}_p$ have order dividing $2^p - 1$. However, all divisors of $2^p - 1$ are $1 \pmod p$, and in particular no divisor other than 1 is greater than p. So f has order 1 on all elements, ergo it must be the identity.