Thailand 2025/9

Evan Chen

Twitch Solves ISL

Episode 167

Problem

Let p be an odd prime and $S = \{1, 2, 3, \ldots, p\}$. Let $U \colon S \to S$ be a bijection. Let B be an integer such that $p \mid B \cdot U(U(a)) - a$ for all $a \in S$. Prove that $B^{\frac{p-1}{2}} - 1$ is a multiple of p.

External Link

https://aops.com/community/p34826465

Solution

Let $f = U^2$ be a bijection with the property that even cycle lengths in pairs (this is true for any bijection that factors as a square).

Claim. $f(p) = p$

Proof. Note we have p, we have $p \mid B \cdot f(p)$. If $p \mid B$ we die instantly, so $f(p) = p$. □

Hence, f is a bijection on the remaining numbers $\{1, \dots, p-1\}$. We only consider those numbers henceforth. Then, the problem statement means that f is

$$f(a) \equiv \frac{a}{B} \pmod{p}.$$

Since f is exactly division by B,

- all cycle lengths of f have length $\operatorname{ord} B \pmod{p}$,
- the number of cycles is $\frac{p-1}{\operatorname{ord} B}$.

Because of our observation from $f = U^2$, if $\operatorname{ord} B$ is even then so is the quotient. Meanwhile if $\operatorname{ord} B$ is odd the quotient is trivially odd since $p-1$ is even. Either way, $\operatorname{ord} B$ divides $\frac{p-1}{2}$ as needed.