Brazil 2017/6

Evan Chen

Twitch Solves ISL

Episode 26

Problem

Let a be a positive integer and p a prime divisor of $a^3 - 3a + 1$, with $p \neq 3$. Prove that p is of the form $9k + 1$ or $9k - 1$, where k is integer.

Video

https://youtu.be/A3AQVRvVk3g

Solution

Write $a = x + \frac{1}{x}$ for some $x \in \mathbb{F}_{p^2}$.

Claim. The element x has order 9.

Proof. Because

$$\begin{aligned} 0 &= \left(x + \frac{1}{x}\right)^3 - 3\left(x + \frac{1}{x}\right) + 1 \\ &= x^3 + x^{-3} + 1 = \frac{x^6 + x^3 + 1}{x^3}. \end{aligned}$$

This implies $x^9 = 1$, so x has order dividing 9. However, $x^3 \neq 1$ since $p > 3$. Therefore, x has order exactly 9. $\square$

Thus $9 \mid p^2 - 1$ so we're done.