Twitch 067.1

Evan Chen

Twitch Solves ISL

Episode 67

Problem

Let m be an odd positive integer. Show that there exist infinitely many positive integers n where $mn+1$ divides 2^n-1.

Video

https://youtu.be/9tL7vedNX_M

Solution

We will restrict our attention to n such that $mn+1=p$ is prime. In other words, we are hoping for

$$p \mid 2^{\frac{p-1}{m}} - 1.$$

In fact, we are going to prove there are infinitely many primes p such that

$$X^m - 2 \in \mathbb{F}_p[X]$$

splits completely. For this, it's sufficient to let $E = \mathbb{Q}(\sqrt[m]{2})$, let K be its Galois closure, and use the following theorem.

Theorem 1 (Chebotarev density)**.** Each conjugacy class C of $G = \operatorname{Gal}(K/\mathbb{Q})$, is obtained as the Frobenius above p for a density $|C|/|G|$ of rational primes p.

In particular, there are infinitely many primes p such that the Frobenius above p is the identity element, which solves the problem.