Putnam 2019 A5

Evan Chen

Twitch Solves ISL

Episode 24

Problem

Let p be an odd prime and define

$$q(x) = \sum_{k=1}^{p-1} k^{\frac{p-1}{2}} x^k$$

in $\mathbb{F}_p[x]$. Find the greatest nonnegative integer n such that $(x-1)^n$ divides $q(x)$ in $\mathbb{F}_p[x]$.

Video

https://youtu.be/K_YcIS8PW3g

Solution

The answer is $n = \frac{1}{2}(p-1)$.

We use derivatives in the following way.

Claim. Define $q_0 = q$, and $q_{i+1} = x \cdot q_i'$. Suppose n is such that $q_1, \dots, q_{n-1}$ has $x = 1$ as a root, but q_n does not have $x = 1$ as a root. Then n is the multiplicity of $x = 1$ in q.

Proof. This follows from the fact that q_{i+1} will have multiplicity of $x = 1$ one less than in q_i. $\square$

On the other hand, we may explicitly compute

$$q_n(1) = \sum_{k=1}^{p-1} k^n \left(\frac{k}{p}\right) = \sum_{k \text{ qr}} k^n - \underbrace{2\sum_{k=1}^{p-1} k^n}_{=0 \text{ for } n<p-1}$$

Let g be a primitive root modulo p. The first sum then equals

$$g^0 + g^{2n} + g^{4n} + \dots + g^{(p-3)n}$$

which equals $\frac{p-1}{2}$ if $n = (p-1)/2$ but $\frac{g^{(p-1)n}-1}{g^{2n}-1} = 0$ otherwise.

Consequently, the answer is $n = \frac{1}{2}(p-1)$ as claimed.