2019 Putnam A5

Tristan Shin

7 Dec 2019

(filler)

The answer is $\boxed{\dfrac{p-1}{2}}$.

The only number theoretic fact necessary is that the mth moment of $\mathbb{F}_p$ for $m \not\equiv 0 \pmod{p-1}$ is 0. There are a few different reasons this is true: (number theory) plug in a primitive root and use geometric series, (group theory) the sum is a multiple of the sum of a subgroup with zero sum, (algebra) use Newton sums on the polynomial $x^{p-1} - 1$.

An immediate corollary is that for any polynomial that has 0 as a root has degree $\leq p - 2$, the sum of the polynomial over $\mathbb{F}_p$ is 0.

Take the jth derivative; we get

$$q^{(j)}(1) = \sum_{a \in \mathbb{F}_p} a^{\frac{p-1}{2}} a^{\underline{j}}$$

where $x^{\underline{j}} = x(x-1)\cdots(x-j+1)$ is the falling factorial. When $j = 0, \ldots, \frac{p-3}{2}$, this is 0 by the corollary. When $j = \frac{p-1}{2}$, the corollary implies that

$$q^{(j)}(1) = \sum_{a \in \mathbb{F}_p} a^{p-1} = -1.$$

So the first $\frac{p-1}{2} - 1$ derivatives of q at 1 (a root of q) are 0, so 1 has multiplicity $\frac{p-1}{2}$ in q. ■