USAMO 2020/3

Evan Chen

Twitch Solves ISL

Episode 16

Problem

Let p be an odd prime. An integer x is called a *quadratic non-residue* if p does not divide $x - t^2$ for any integer t.

Denote by A the set of all integers a such that $1 \le a < p$, and both a and $4 - a$ are quadratic non-residues. Calculate the remainder when the product of the elements of A is divided by p.

Video

https://youtu.be/r7j0oRtpErA

Solution

The answer is that $\prod_{a\in A} a \equiv 2 \pmod p$ regardless of the value of p. Here is the official solution, where we always work in $\mathbb{F}_p$.

We define

$$A = \{a \in \mathbb{F}_p \mid a, 4-a \text{ not qr}\}$$
$$B = \{b \in \mathbb{F}_p \mid b, 4-b \text{ qr}, b \neq 0, b \neq 4\}.$$

Note that $a \in A \iff 4-a \in A$ and $b \in B \iff 4-b \in B$.

We now do the following magical calculation in $\mathbb{F}_p$:

$$\begin{aligned}
\prod_{b\in B} b = \prod_{b\in B}(4-b) &= \prod_{\substack{1\le y\le (p-1)/2 \\ y\neq 2 \\ 4-y^2 \text{ is qr}}} (4-y^2) \\
&= \prod_{\substack{1\le y\le (p-1)/2 \\ y\neq 2 \\ 4-y^2 \text{ is qr}}} (2+y) \prod_{\substack{1\le y\le (p-1)/2 \\ y\neq 2 \\ 4-y^2 \text{ is qr}}} (2-y) \\
&= \prod_{\substack{1\le y\le (p-1)/2 \\ y\neq 2 \\ 4-y^2 \text{ is qr}}} (2+y) \prod_{\substack{(p+1)/2\le y\le p-1 \\ y\neq p-2 \\ 4-y^2 \text{ is qr}}} (2+y) \\
&= \prod_{\substack{1\le y\le p-1 \\ y\neq 2,p-2 \\ 4-y^2 \text{ is qr}}} (2+y) \\
&= \prod_{\substack{3\le z\le p+1 \\ z\neq 4,p \\ z(4-z) \text{ is qr}}} z \\
&= \prod_{\substack{0\le z\le p-1 \\ z\neq 0,4,2 \\ z(4-z) \text{ is qr}}} z.
\end{aligned}$$

Note $z(4-z)$ is a nonzero quadratic residue if and only if $z \in A \cup B$. So the right-hand side is almost the product over $z \in A \cup B$, except it is missing the $z = 2$ term. Adding it in gives

$$\prod_{b\in B} b = \frac{1}{2} \prod_{\substack{0\le z\le p-1 \\ z\neq 0,4 \\ z(4-z) \text{ is qr}}} z = \frac{1}{2} \prod_{a\in A} a \prod_{b\in B} b.$$

This gives $\prod_{a\in A} a = 2$ as desired.