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

External Link

https://aops.com/community/p15952782

Solution

The answer is that $\prod_{a \in A} a \equiv 2 \pmod{p}$ regardless of the value of p. In the following solution, we work in $\mathbb{F}_p$ always and abbreviate "quadratic residue" and "non-quadratic residue" to "QR" and "non-QR", respectively.

We define

$$\begin{aligned} A &= \{a \in \mathbb{F}_p \mid a, 4-a \text{ non-QR}\} \\ B &= \{b \in \mathbb{F}_p \mid b, 4-b \text{ QR}, b \neq 0, b \neq 4\}. \end{aligned}$$

Notice that

$$A \cup B = \{n \in \mathbb{F}_p \mid n(4-n) \text{ is QR } n \neq 0, 4\}.$$

We now present two approaches both based on the set B.

First approach (based on Holden Mui's presentation in Mathematics Magazine). The idea behind this approach is that $n(4-n)$ is itself an element of B for $n \in A \cup B$, because $4 - n(4-n) = (n-2)^2$. This motivates the following claim.

Claim. The map

$$A \cup B \setminus \{2\} \to B \qquad \text{by} \quad n \mapsto n(4-n)$$

is a well-defined two-to-one map, i.e. every $b \in B$ has exactly two pre-images.

Proof. Since $n \notin \{0, 2, 4\}$, we have $n(4-n) \notin \{0, 4\}$, so as discussed previously, $n(4-n) \in B$. Thus this map is well-defined.

Choose $b \in B$. The quadratic equation $n(4-n) = b$ in n rewrites as $n^2 - 4n + b = 0$, and has discriminant $4(4-b)$, which is a nonzero QR. Hence there are exactly two values of n, as desired. $\square$

Therefore, it follows that

$$\prod_{n \in A \cup B \setminus \{2\}} n = \prod_{b \in B} b$$

by pairing n with $4-n$ on the left-hand side. So, $\prod_{a \in A} a = 2$.

Second calculation approach (along the lines of official solution). We now do the following magical calculation in $\mathbb{F}_p$:

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

$$= \prod_{\substack{3 \le z \le p+1 \\ z \neq 4, p \\ z(4-z) \text{ is QR}}} z$$
$$= \prod_{\substack{0 \le z \le p-1 \\ z \neq 0, 4, 2 \\ z(4-z) \text{ is QR}}} z.$$

Note $z(4-z)$ is a nonzero QR 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.