2020 USOMO #3

Tristan Shin

19 June 2020

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.

The key claim is the following characterization of A:

$$A = \{\omega + \omega^{-1} + 2 \mid \omega^{2n} = -1 \text{ for } \omega \in \mathbb{F}_{p^2}\}$$

where n is the integer nearest $\frac{p}{4}$. Let A' be the set on the RHS. First, note that $|A| = |A'|$. Indeed, by pairing ω with ω^{-1}, we have that $|A'| = n$. And

$$\begin{aligned}
|A| &= \sum_{a \in \mathbb{F}_p} \frac{1}{4}\left(1 - \left(\frac{a}{p}\right)\right)\left(1 - \left(\frac{4-a}{p}\right)\right) = \frac{1}{4}\sum_{a \in \mathbb{F}_p} 1 - \left(\frac{a}{p}\right) - \left(\frac{4-a}{p}\right) + \left(\frac{4a - a^2}{p}\right) \\
&= \frac{1}{4}\left(p + \sum_{a \neq 0}\left(\frac{4/a - 1}{p}\right)\right) = \frac{1}{4}\left(p + \sum_{b \not\equiv -1}\left(\frac{b}{p}\right)\right) \\
&= \frac{p + (-1)^{\frac{p-1}{2}}}{4} = n
\end{aligned}$$

as desired.

Now, we show that every element of A' is a QNR.

First, suppose that $p \equiv 1 \pmod 4$ so $n = \frac{p-1}{4}$. Then $\omega^{\frac{p-1}{2}} = -1$, so ω is a QNR in $\mathbb{F}_p$. Then $\omega + \omega^{-1} + 2 = \frac{(\omega+1)^2}{\omega}$ is also a QNR in $\mathbb{F}_p$ as desired.

Next, suppose that $p \equiv 3 \pmod 4$ so $n = \frac{p+1}{4}$. Then $\omega^{\frac{p+1}{2}} = -1$. Then

$$(\omega + \omega^{-1} + 2)^{\frac{p-1}{2}} = \frac{(\omega+1)^{p-1}}{\omega^{\frac{p-1}{2}}} = \frac{(\omega+1)^p}{\omega^{\frac{p-1}{2}}(\omega+1)} = \frac{\omega^p + 1}{\omega^{\frac{p+1}{2}} + \omega^{\frac{p-1}{2}}} = \frac{\omega^p + 1}{-1 - \omega^p} = -1$$

so $\omega + \omega^{-1} + 2$ is a QNR in $\mathbb{F}_p$ as desired.

Finally, observe that $A' = 4 - A'$ by pairing ω with $-\omega$. This implies that $A = A'$ as claimed.

To finish, this implies that the elements of A are the roots of $T_n\left(\frac{X-2}{2}\right)$, where T_n is the nth Chebyshev polynomial. The leading coefficient of this is $\frac{1}{2}$ while the constant term is $T_n(-1) = (-1)^n$, so the product of the elements of A is 2. ■