Iran 2010/2/6

Evan Chen

Twitch Solves ISL

Episode 23

Problem

Let g and n be positive integers such that $\gcd(g^2 - g, n) = 1$. Define B as the set of possible remainders when g^k is divided by n, across all integers $k \geq 0$. For each $i = 0, \dots, g-1$ define a_i as the number of elements of B which lie in the interval

$$\left[\frac{ni}{g}, \frac{n(i+1)}{g}\right).$$

Show that $g - 1$ divides $\sum_{i=0}^{g-1} ia_i$.

Video

https://youtu.be/CC5w3OLl18A

Solution

Let $e > 0$ denote the order of g modulo n. Also, by $a\%n$ we mean the remainder when a is divided by n.

The main observation is that an element $b \in B$ will fall in the $\left\lfloor \frac{g \cdot b}{n} \right\rfloor$'th interval, and contribute that amount to the sum given in the problem. This gives the first equality in the following calculation:

$$\begin{aligned}
\sum i a_i &= \sum_{b \in B} \left\lfloor \frac{g \cdot b}{n} \right\rfloor \\
&= \sum_{k=0}^{e-1} \left\lfloor \frac{g \cdot (g^k \% n)}{n} \right\rfloor \\
&= \sum_{k=0}^{e-1} \frac{g \cdot (g^k \% n) - \left(g \cdot (g^k \% n)\right) \% n}{n}
\end{aligned}$$

We may now take modulo $g-1$, noting that $g \equiv 1 \pmod{g-1}$ and n is relatively prime to $g-1$, hence

$$\begin{aligned}
\sum i a_i &= \sum_{k=0}^{e-1} \frac{(g^k \% n) - \left(g^{k+1} \% n\right)}{n} \pmod{g-1} \\
&= 0
\end{aligned}$$

as desired, with the sum telescoping.