2009 IMO #1

Tristan Shin

12 Apr 2018

Let n be a positive integer and let $a_1, a_2, a_3, \ldots, a_k$ $(k \geq 2)$ be distinct integers in the set $\{1, 2, \ldots, n\}$ such that n divides $a_i(a_{i+1} - 1)$ for $i = 1, 2, \ldots, k-1$. Prove that n does not divide $a_k(a_1 - 1)$.

Suppose the opposite. Take any prime p dividing n. Then

$$\nu_p(n) \leq \nu_p(a_i(a_{i+1} - 1)) = \nu_p(a_i) + \nu_p(a_{i+1} - 1)$$

for $i = 1, 2, \ldots, k$. Summing this up, we get that

$$k\nu_p(n) \leq \sum_{i=1}^{k} \nu_p(a_i) + \nu_p(a_{i+1} - 1) = \sum_{i=1}^{k} \nu_p(a_i) + \nu_p(a_i - 1),$$

so there is some j such that $\nu_p(n) \leq \nu_p(a_j) + \nu_p(a_j - 1)$. Observe that $\min(\nu_p(a_j), \nu_p(a_j - 1)) = 0$, so $\max(\nu_p(a_j), \nu_p(a_j - 1)) \geq \nu_p(n)$.

- Suppose $\nu_p(a_j) \geq \nu_p(n)$. I claim that $\nu_p(a_i) \geq \nu_p(n)$ for all i. We start at $i = j$; this is true. If the inequality is true for i, then $\nu_p(a_i - 1) = 0$, so

  $$\nu_p(a_{i-1}) = \nu_p(a_{i-1}) + \nu_p(a_i - 1) \geq \nu_p(n),$$

  so the inequality is true for $i - 1$. So by induction, the inequality is true. Then $a_i \equiv 0 \pmod{p}^{\nu_p(n)}$ for all i.

- Otherwise, $\nu_p(a_j - 1) \geq \nu_p(n)$. I claim that $\nu_p(a_i - 1) \geq \nu_p(n)$ for all i. We start at $i = j$; this is true. If the inequality is true for i, then $\nu_p(a_i) = 0$, so

  $$\nu_p(a_{i+1} - 1) = \nu_p(a_i) + \nu_p(a_{i+1} - 1) \geq \nu_p(n),$$

  so the inequality is true for $i + 1$. So by induction, the inequality is true. Then $a_i \equiv 1 \pmod{p}^{\nu_p(n)}$ for all i.

In all cases, the a_i are all the same mod $p^{\nu_p(n)}$. By CRT, the a_i are all the same mod n, contradiction.

So n does not divide $a_k(a_1 - 1)$. ∎