2018 USAMO #3

Tristan Shin

18 Sep 2018

For a given integer $n \geq 2$, let $\{a_1, a_2, \ldots, a_m\}$ be the set of positive integers less than n that are relatively prime to n. Prove that if every prime that divides m also divides n, then $a_1^k + a_2^k + \cdots + a_m^k$ is divisible by m for every positive integer k.

Let $A(n)$ be the set of positive integers less than n that are relatively prime to n so that $|A(n)| = \varphi(n)$. Also define $d_k(n)$ such that $\sum\limits_{a \in A(n)} a^k = d_k(n)\varphi(n)$. Then the problem statement is equivalent to proving that $d_k(n)$ is an integer for every non-negative integer k if every prime that divides $\varphi(n)$ also divides n (we can tack on $k = 0$ because clearly $d_0(n) = 1$).

Suppose that there is an integer $n \geq 2$ such that $\varphi(n)$ is only divisible by primes that also divide n but $d_k(n)$ is not an integer for some non-negative integer k, and pick n to be the smallest such integer. Clearly, $n \neq 2$ because $d_k(2) = 1$ as $A(2) = \{1\}$. Now, take the smallest non-negative integer k such that $d_k(n)$ is not an integer. We casework on whether or not n is squarefree.

Suppose n is squarefree. Take the largest prime p dividing n. Then $\frac{n}{p} \neq 1$, otherwise either $n = 2$ or $\varphi(n) = p - 1$ which is divisible by 2 but n is not even. Consider the numbers $a + i \cdot \frac{n}{p}$, where $a \in A\left(\frac{n}{p}\right)$ and $i \in \{0, 1, \ldots, p-1\}$. By definition, these are the positive integers less than n that are relatively prime to $\frac{n}{p}$, so $A(n)$ is a subset of these numbers. Now, observe that the numbers pa, where $a \in A\left(\frac{n}{p}\right)$, are relatively prime to $\frac{n}{p}$ and less than n but are not relatively prime to n. Thus, $A(n)$ is a subset of the first type we considered excluding the second type. But there are $p\varphi\left(\frac{n}{p}\right) - \varphi\left(\frac{n}{p}\right) = \varphi(n)$ such numbers, so $A(n)$ is precisely this set. That is,

$$A(n) = \left\{a + i \cdot \frac{n}{p} \mid a \in A\left(\frac{n}{p}\right), i \in \{0, 1, \ldots, p-1\}\right\} \setminus \left\{pa \mid a \in A\left(\frac{n}{p}\right)\right\}.$$

Then

$$\begin{aligned}
\sum_{a\in A(n)} a^k &= \sum_{i=0}^{p-1} \sum_{a\in A\left(\frac{n}{p}\right)} \left(a+i\cdot\frac{n}{p}\right)^k - \sum_{a\in A\left(\frac{n}{p}\right)} (pa)^k \\
&= \sum_{i=0}^{p-1} \sum_{a\in A\left(\frac{n}{p}\right)} \sum_{j=0}^{k} \binom{k}{j} a^j \left(i\cdot\frac{n}{p}\right)^{k-j} - p^k \sum_{a\in A\left(\frac{n}{p}\right)} a^k \\
&= \sum_{i=0}^{p-1} \sum_{j=0}^{k} \binom{k}{j} \left(i\cdot\frac{n}{p}\right)^{k-j} \sum_{a\in A\left(\frac{n}{p}\right)} a^j - p^k \sum_{a\in A\left(\frac{n}{p}\right)} a^k \\
&= \sum_{i=0}^{p-1} \sum_{j=0}^{k} \binom{k}{j} \left(i\cdot\frac{n}{p}\right)^{k-j} d_j\left(\frac{n}{p}\right)\varphi\left(\frac{n}{p}\right) - p^k d_k\left(\frac{n}{p}\right)\varphi\left(\frac{n}{p}\right) \\
&= \frac{\varphi(n)}{p-1}\left[\sum_{j=0}^{k}\binom{k}{j}\left(\frac{n}{p}\right)^{k-j} d_j\left(\frac{n}{p}\right)\sum_{i=0}^{p-1} i^{k-j} - p^k d_k\left(\frac{n}{p}\right)\right]
\end{aligned}$$

where we use the fact that $\varphi(n) = (p-1)\varphi\left(\frac{n}{p}\right)$. Now, it is clear that

$$(p-1)\,d_k(n) = \sum_{j=0}^{k}\binom{k}{j}\left(\frac{n}{p}\right)^{k-j} d_j\left(\frac{n}{p}\right)\sum_{i=0}^{p-1} i^{k-j} - p^k d_k\left(\frac{n}{p}\right)$$

is an integer as each of the terms is an integer. Take a prime q dividing $p-1$. Observe that $q \mid n$ because $q \mid \varphi(n)$. By Faulhaber's formula, $\sum_{i=0}^{p-1} i^{k-j}$ is $\frac{p-1}{(k-j+1)!}$ times an integer when $j<k$. Then

$$\begin{aligned}
\nu_q\left(n^{k-j}\sum_{i=0}^{p-1} i^{k-j}\right) &\geq (k-j)\,\nu_q(n) + \nu_q(p-1) - \nu_q((k-j+1)!) \\
&= (k-j)\,\nu_q(p-1) + \nu_q(p-1) - \frac{k-j+1-s_q(k-j+1)}{q-1} \\
&\leq (k-j) + \nu_q(p-1) - (k-j) \\
&= \nu_q(P-1)
\end{aligned}$$

for all primes q which divide $p-1$, so $p-1$ divides $n^{k-j}\sum_{i=0}^{p-1} i^{k-j}$. Then

$$(p-1)\,d_k(n) \equiv p d_k\left(\frac{n}{p}\right) - p^k d_k\left(\frac{n}{p}\right) \equiv 0 \pmod{p-1},$$

contradiction.

Suppose n is not squarefree. Take a prime p dividing n such that $p^2 \mid n$. Consider the numbers $a + i\cdot\frac{n}{p}$, where $a \in A\left(\frac{n}{p}\right)$ and $i \in \{0,1,\ldots,p-1\}$. By definition, these are the positive integers less than n that are relatively prime to $\frac{n}{p}$, so $A(n)$ is a subset of these numbers. But there are $p\varphi\left(\frac{n}{p}\right) = \varphi(n)$ such numbers, so $A(n)$ is precisely this set. That is,

$$A(n) = \left\{a + i \cdot \frac{n}{p} \mid a \in A\left(\frac{n}{p}\right), i \in \{0, 1, \ldots, p-1\}\right\}.$$

Then

$$\begin{aligned}
\sum_{a \in A(n)} a^k &= \sum_{i=0}^{p-1} \sum_{a \in A\left(\frac{n}{p}\right)} \left(a + i \cdot \frac{n}{p}\right)^k \\
&= \sum_{i=0}^{p-1} \sum_{a \in A\left(\frac{n}{p}\right)} \sum_{j=0}^{k} \binom{k}{j} a^j \left(i \cdot \frac{n}{p}\right)^{k-j} \\
&= \sum_{i=0}^{p-1} \sum_{j=0}^{k} \binom{k}{j} \left(i \cdot \frac{n}{p}\right)^{k-j} \sum_{a \in A\left(\frac{n}{p}\right)} a^j \\
&= \sum_{i=0}^{p-1} \sum_{j=0}^{k} \binom{k}{j} \left(i \cdot \frac{n}{p}\right)^{k-j} d_j\left(\frac{n}{p}\right) \varphi\left(\frac{n}{p}\right) \\
&= \frac{\varphi(n)}{p} \sum_{i=0}^{p-1} \sum_{j=0}^{k} \binom{k}{j} \left(i \cdot \frac{n}{p}\right)^{k-j} d_j\left(\frac{n}{p}\right)
\end{aligned}$$

where we use the fact that $\varphi(n) = p\varphi\left(\frac{n}{p}\right)$. But n^{k-j} is divisible by p when $j < k$, so

$$pd_k(n) = \sum_{i=0}^{p-1} \sum_{j=0}^{k} \binom{k}{j} \left(i \cdot \frac{n}{p}\right)^{k-j} d_j\left(\frac{n}{p}\right) \equiv 0 \pmod{p}$$

and hence $d_k(n)$ is an integer, contradiction.

Thus, there is always a contradiction so our assumption is wrong and hence the problem statement must be true. ■