**Problem 12300**
(American Mathematical Monthly, Vol.129, February 2022)

Proposed by H. A. ShahAli (Iran).

*Let $n$ be an integer such that $n \geq 3$. Prove that there is no permutation $\pi$ of $\{1, 2, \ldots, n\}$ such that $\pi(1), 2\pi(2), \ldots, n\pi(n)$ are distinct modulo $n$.*

Solution proposed by Roberto Tauraso, University of Rome Tor Vergata, Rome, Italy.

*Solution.* We break our proof by contradiction into three steps. Let $\pi$ be a permutation such that $\pi(1), 2\pi(2), \ldots, n\pi(n)$ are distinct modulo $n$ with $n \geq 3$, that is $S := \{k\pi(k) : k = 1, \ldots, n\}$ is complete residue system modulo $n$.

1) For any divisor $d$ of $n$, $d$ divides $k$ if and only if $d$ divides $\pi(k)$.

Since $S$ is complete residue system modulo $n$ and $d$ divides $n$, then $S$ has the same number of multiples of $d$ as $\{1, \ldots, n\} = \{\pi(k) : k = 1, \ldots, n\}$. On the other hand, $k\pi(k)$ is a multiple of $d$ if and only if $d$ divides $k$ or $\pi(k)$. Hence, the asserted property holds if and only if the claim is true, otherwise the number of multiples of $d$ in $S$ would be larger.

2) $n$ is square-free.

If $n$ is not square-free then there is a prime $p$ such that $p^2$ divides $n$. Since $S$ is complete residue system modulo $n$, there is an integer $k$ such that $k\pi(k) \equiv p \pmod{n}$, that is $k\pi(k) = ap^2 + p$ for some integer $a$, which implies that $p$ divides $k$ or $\pi(k)$. Hence, by 1), $p$ divides both $k$ and $\pi(k)$, and therefore $p^2$ divides $k\pi(k) = ap^2 + p \equiv p \pmod{p^2}$ which is impossible.

3) Conclusion.

Since $n \geq 3$ is square-free by 2), there is a prime $p \geq 3$ such that $n = pa$ and $\gcd(p, a) = 1$. By 1), $\pi(n) = n$, and there are two permutations $\sigma_1$ and $\sigma_2$ of $\{1, 2, \ldots, p-1\}$ such that for $j = 1, \ldots, p-1$

$$\pi(ja) \equiv \sigma_1(j)a \quad \text{and} \quad ja \cdot \pi(ja) \equiv \sigma_2(j)a \pmod{n}.$$

Therefore, since the above congruences hold also modulo $p$, it follows that

$$\prod_{j=1}^{p-1} ja \cdot \pi(ja) \equiv \prod_{j=1}^{p-1} \sigma_2(j)a \pmod{p}.$$

By Wilson's theorem and Fermat's little theorem, we find that the two sides are different modulo $p$ which is a contradiction:

$$\prod_{j=1}^{p-1} ja \cdot \pi(ja) \equiv \prod_{j=1}^{p-1} ja \cdot \sigma_1(j)a = ((p-1)!a^{p-1})^2 \equiv (-1)^2 = 1 \pmod{p}$$

$$\prod_{j=1}^{p-1} \sigma_2(j)a \equiv= (p-1)!a^{p-1} \equiv -1 \pmod{p}.$$

□