Problem 11591
(American Mathematical Monthly, Vol.118, August-September 2011)

Proposed by Dan White and Lenny Jones (USA).

Let I_n be the set of all idempotent elements of $\mathbb{Z}_n$. That is, $e \in I_n$ if and only if $e^2 = e \pmod{n}$. Let $I_n^1 = I_n$, and for $k \geq 2$, let I_n^k be the set of all sums of the form $u + v$ where $u \in I_n$, $v \in I_n^{k-1}$, and the addition is done modulo n. Determine, in terms of n, the least k such that $I_n^k = \mathbb{Z}_n$.

Solution proposed by Roberto Tauraso, Dipartimento di Matematica, Università di Roma "Tor Vergata", via della Ricerca Scientifica, 00133 Roma, Italy.

We first show that if n is a power of a prime p then the only idempotents in $\mathbb{Z}_n$ are 0 and 1. Suppose that $x \neq 0$ is a solution of $x^2 \equiv x \pmod{p^e}$. Let $x = p^a b$, where $0 \leq a < e$ and $\gcd(b, p) = 1$. Then $b(p^a b - 1) \equiv 0 \pmod{p^{e-a}}$ which yields that $p^a b \equiv 1 \pmod{p^{e-a}}$. Thus $a = 0$ and $x = b \equiv 1 \pmod{p^e}$. It follows at once that for such n, $I_n^k = \{0, 1, \ldots, k\}$ for $k = 1, \ldots, n-1$ and $I_n^k = \mathbb{Z}_n$ as soon as $k \geq n - 1$.
In the general case, where the factorization of n is $p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, by the Chinese Remainder Theorem

$$I_n^k = I_{p_1^{e_1}}^k \times I_{p_2^{e_2}}^k \times \cdots \times I_{p_r^{e_r}}^k.$$

So, $I_n^k = \mathbb{Z}_n$ when $I_{p_i^{e_i}}^k = \mathbb{Z}_{p_i^{e_i}}$ for all $i = 1, \ldots, r$, which implies that the least k such that the desired condition is fulfilled is

$$\min\{p_i^{e_i} \, : \, i = 1, \ldots, r\} - 1.$$

□