Problem 12021
(American Mathematical Monthly, Vol.125, February 2018)

Proposed by O. Sonebi (Morocco).

Let φ be the Euler totient function. Given $a \in \mathbb{Z}^+$ and $b \in \mathbb{Z}^+$, show that there exists $n \in \mathbb{Z}^+$ such that $an + b$ is not in the range of φ.

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

Solution. Let $m := \gcd(a, b)$, $A := a/m$ and $B := b/m$. Let $d_1, d_2, \dots, d_r$ be all the positive divisors of m and the primes p_i for $i = 1, \dots, r$ such that $\max(a, b) < p_1 < p_2 < \cdots < p_r$. Consider the system of congruences

$$\begin{cases} x \equiv B & \pmod{A}, \\ xd_i \equiv -1 & \pmod{p_i} \quad \text{for } i = 1, \dots, r. \end{cases}$$

Since $\gcd(d_i, p_i) = 1$ (because $p_i > d_i$), and $A, p_1, p_2, \dots, p_r$ are pairwise coprime, by the Chinese remainder theorem, there exists a positive integer $x_0 = Ak_0 + B$ such that for all $k \in \mathbb{Z}$,

$$x_k = Ap_1 \cdots p_r k + x_0$$

is a solution of the system of congruences.
Notice that $\gcd(Ap_1 \cdots p_r, x_0) = 1$ and by Dirichlet's theorem the arithmetic progression $(x_k)_{k \geq 0}$ contains infinitely many primes. Hence there is a positive integer k such that $p := x_k > p_r$ is a prime.
It remains to verify that

$$mp = m(Ap_1 \cdots p_r k + x_0) = m(Ap_1 \cdots p_r k + Ak_0 + B) = an + b$$

where $n := p_1 \cdots p_r k + k_0$ is not in the range of φ.
Assume that $\varphi(y) = \prod_{j=1}^{s} q_j^{\alpha_j - 1}(q_j - 1) = mp$ for some positive integer $y = \prod_{j=1}^{s} q_j^{\alpha_j}$ then we have two cases.

i) $p = q_j$ for some j with $\alpha_j > 1$. Then $p(p-1)$ divides $\varphi(y) = mp$ and therefore $p - 1$ divides m. Hence $p \leq m + 1$ which contradicts $p > p_1 > m$.

ii) p divides $q_j - 1$ for some j. Then $p < q_j$. Moreover $pd = q_j - 1$ divides $\varphi(y) = mp$, which implies that d is a divisor of m, that is $d = d_i$ for some i. Since p is a solution of the above system of congruences, it follows that p_i divides $pd_i + 1 = q_j$ which means that $p_i = q_j$. This contradicts $q_j > p > p_i$.

□