Problem 12200
(American Mathematical Monthly, Vol.127, August-September 2020)

Proposed by I. S. Evren (Turkey).

Prove that for every positive integer m, there is a positive integer k such that k does not divide $m + x^2 + y^2$ for any positive integers x and y.

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

Solution. For any prime p and for any positive integer n, let $\nu_p(n)$ be the exponent of the largest power of p that divides n. Given a positive integer m, we distinguish two cases.

1) If $m = a \cdot 2^s$ with $a \equiv 1 \pmod 4$ and $s = \nu_2(m) \geq 0$ then let $k = 2^{s+2}$.
Assume that $m + x^2 + y^2$ is divisible by k:

$$a \cdot 2^s + x^2 + y^2 \equiv 0 \pmod{2^{s+2}}.$$

If $s \geq 2$ then $x^2 + y^2 \equiv 0 \pmod 4$ which implies that $x \equiv y \equiv 0 \pmod 2$ and, after dividing by 4, we find

$$a \cdot 2^{s-2} + x_1^2 + y_1^2 \equiv 0 \pmod{2^s}$$

where $x_1 = x/2$ and $y_1 = y/2$. By applying the same argument $n = \lfloor s/2 \rfloor$ times we obtain one of two possible congruences. If s is even then

$$a + x_n^2 + y_n^2 \equiv 0 \pmod 4$$

which is a contradiction because the LHS modulo 4 can be 1, 2, or 3. If s is odd then

$$2a + x_n^2 + y_n^2 \equiv 0 \pmod 8$$

which is a contradiction because the LHS modulo 8 can be 2, 3, 4, 6 or 7.

2) Otherwise, there is a prime $p \equiv 3 \pmod 4$ such that $m = a \cdot p^{2s+1}$ where $\gcd(a, p) = 1$ and $\nu_p(m) = 2s + 1$ is odd. Then let $k = p^{2s+2}$.
Assume that $m + x^2 + y^2$ is divisible by k:

$$a \cdot p^{2s+1} + x^2 + y^2 \equiv 0 \pmod{p^{2s+2}}.$$

Then $x^2 + y^2 \equiv 0 \pmod p$ which implies that $x \equiv y \equiv 0 \pmod p$, otherwise $-1 \equiv (x/y)^2 \pmod p$ is a quadratic residue modulo p, which is not possible because $p \equiv 3 \pmod 4$. If $s \geq 1$ then we divide both sides by p^2. By applying this argument $n = s$ times we obtain

$$a \cdot p + x_n^2 + y_n^2 \equiv 0 \pmod{p^2}.$$

Again $x_n \equiv y_n \equiv 0 \pmod p$ and therefore

$$a \cdot p \equiv 0 \pmod{p^2},$$

that is a is divisible by p which contradicts the fact that $\gcd(a, p) = 1$. □