Problem 12321
(American Mathematical Monthly, Vol.129, May 2022)

Proposed by M. Sharifi (Iran).

Let p be a prime number, and let N be the number of perfect squares m such that the least non-negative remainder of $p \pmod m$ is a perfect square. Prove that N is less than $2p^{1/3}$.

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

Solution. The number N is equal to the cardinality of the set

$$S_p := \Big\{(q,x,y) \in \mathbb{N}^3 : p = qx^2 + y^2, q = \lfloor p/x^2 \rfloor, 0 \le y < x < p^{1/2}\Big\}.$$

We first show that

$$(q,x,y),(q,u,v) \in S_p \implies x = u \text{ and } y = v. \tag{1}$$

If $q = p$ then it easy to see that $x = u = 1$ and $y = v = 0$. Assume now that $0 < q < p$. If $x \neq u$ then we may assume that $x > u$ and therefore $x > u > v > y > 0$.
From $p = qx^2 + y^2 = qu^2 + v^2$ we get

$$(qx^2)(v^2) = (p - y^2)(p - qu^2) \equiv (y^2)(qu^2) \pmod p$$

which implies that p divides $q(x^2v^2 - y^2u^2) = q(xv - yu)(xv + yu)$. Moreover

$$0 < q < p \quad \text{and} \quad 0 < xv - yu < x^2 < p,$$

and therefore p divides $xv + yu$. Hence, by Brahmagupta's identity,

$$p^2 = (qx^2 + y^2)(qu^2 + v^2) = q(xv + yu)^2 + (qxu - yv)^2 \equiv (qxu - yv)^2 \pmod{p^2}$$

and we find that p divides $qxu - yv$ which is a contradiction because

$$0 < qxu - yv \le qx^2 < p.$$

Finally, by property (1), we may conclude that

$$\begin{aligned} N &\le \Big|\Big\{\lfloor p/x^2 \rfloor \,:\, x \in \mathbb{N} \cap [1, p^{1/2})\Big\}\Big| \\ &\le \Big|\Big\{\lfloor p/x^2 \rfloor : x \in \mathbb{N} \cap [1, p^{1/3})\Big\}\Big| + \Big|\Big\{\lfloor p/x^2 \rfloor : x \in \mathbb{N} \cap (p^{1/3}, p^{1/2})\Big\}\Big| \\ &< p^{1/3} + p^{1/3} = 2p^{1/3} \end{aligned}$$

where at the last step we applied

$$\begin{aligned} \Big\{\lfloor p/x^2 \rfloor : x \in \mathbb{N} \cap (p^{1/3}, p^{1/2})\Big\} &= \Big\{\lfloor p/x^2 \rfloor : x \in \mathbb{N}, p^{2/3} < x^2 < p\Big\} \\ &= \Big\{\lfloor p/x^2 \rfloor : x \in \mathbb{N}, 1 < p/x^2 < p^{1/3}\Big\} \subseteq \mathbb{N} \cap [1, p^{1/3}). \end{aligned}$$

□