Problema 4 (TW 2 / Murilo)

(Romênia) Seja S o conjunto de inteiros da forma a^2+2b^2, onde $a,b\in\mathbb{Z}$ e $b\neq 0$. Prove que se p é primo e $p^2\in S$, então $p\in S$.

$$p^2 = a^2+2b^2$$

$$p^2-a^2 = 2b^2$$

$$(p-a)(p+a) = 2b^2$$

- $2 \mid 2b^2 = (p-a)(p+a) \Rightarrow 2\mid p-a$ e $2\mid p-a \Rightarrow 4 \mid 2b^2 \Rightarrow 2\mid b$.
- $b=2d$.

$$\left(\frac{p-a}{2}\right)\left(\frac{p+a}{2}\right) = 2d^2.$$

$$\operatorname{mdc}\left(\frac{p-a}{2}, \frac{p+a}{2}\right) \mid p \quad \text{e} \quad \operatorname{mdc}\left(\frac{p-a}{2}, \frac{p+a}{2}\right) \mid a.$$

$\Rightarrow \operatorname{mdc}(m, n) = 1$ ou $\operatorname{mdc}(m, n) = p$

$\Downarrow$

$$\begin{cases} \dfrac{p\pm a}{2} = 2n^2 \\[2ex] \dfrac{p\mp a}{2} = m^2 \end{cases} \quad ①$$

$$p = 2n^2+m^2 \in S.$$

① note que $p\neq a \Rightarrow$
$\Rightarrow n, m \neq 0$.

$\Downarrow$

$p\mid a \Rightarrow a \geq p$ ou $a=0$

$a \geq p \Rightarrow a^2 \geq p^2 \Rightarrow a^2+2b^2 > p^2$ Abs!

$a = 0 \Rightarrow p^2 = 2b^2$ Abs! (olhando v_2)

$\square$