Jelöljük az $a+b$ és az a^2+b^2 legnagyobb közös osztóját d-vel. Mivel $d \mid a+b$ és $d \mid a^2+b^2$, azért $d \mid \left((a+b)^2 - a^2 - b^2\right)$ is fennáll, azaz $d \mid 2ab$.

Ha d-nek és a-nak lenne 1-nél nagyobb közös osztója, mondjuk m, akkor $m \mid d$ és $d \mid a+b$ miatt $m \mid a+b$, ekkor viszont $m \mid a$, $m \mid a+b-a$ teljesülne, ami ellentmondana annak, hogy a és b relatív prímek. Ugyanígy látható be, hogy d és b legnagyobb közös osztója is 1.

A $d \mid 2ab$ oszthatóság azt jelenti, hogy d minden prímtényezője legalább akkora kitevővel szerepel $2ab$-ben, mint d-ben. Azonban sem d-nek és a-nak, sem d-nek és b-nek nincs közös prímtényezője, így csak az lehetséges, hogy $d \mid 2$, azaz $d = 1$ vagy 2, s éppen ezt kellett bizonyítani. A $d = 2$ eset akkor áll fönn, ha a és b is páratlan.

Megjegyzés. Viszonylag egyszerűen igazolható az az általánosabb állítás is, hogy ugyanezen feltételek mellett az $a+b$ és $a^{2k}+b^{2k}$ legnagyobb közös osztója is 1 vagy 2. Itt a

$$d \mid (a+b)\left(a^{2k-1}+b^{2k-1}\right) - \left(a^{2k}+b^{2k}\right)$$

összefüggést használjuk, amiből

$$d \mid ab\left(a^{2k-2}+b^{2k-2}\right).$$

Az előzőekben látottak alapján ez csak úgy lehet, hogy

$$d \mid a^{2k-2}+b^{2k-2}.$$

E gondolatmenettel eljutunk oda, hogy

$$d \mid a^2+b^2, \qquad d \mid a+b,$$

s ebből már tudjuk, hogy csak a $d = 1$ vagy 2 eset állhat fönn.

Tóth Gábor Zsolt (Budapest, Árpád Gimn., II. o. t.) dolgozata alapján