Megmutatjuk, hogy az egyenletrendszer megoldhatatlan a pozitív egészek körében. Bizonyításunk módszere a következő lesz: feltételezzük, hogy létezik pozitív egészekből álló megoldás, és az esetleg több megoldás közül kiválasztunk egy – valamilyen szempontból – minimálisat. Ennek a minimális megoldásnak a segítségével pedig belátjuk, hogy létezik nála (az előbbi értelemben) „kisebb" megoldás is, ami nyilván ellentmondás. (Diofantikus egyenleteknek ezt a megoldási módszerét a végtelen leszállás (descente infinie) elvének hívjuk.)

Tételezzük föl tehát, hogy léteznek olyan a, b, c, d pozitív egészek, amelyekre $a^2+b^2=c^2-d^2$, $ab=cd$, és az ilyen számnégyesek közül tekintsünk a továbbiakban egy olyat, amelyre $abcd$ a lehető legkisebb.

(1) Mivel $ab=cd$, ezért (felhasználva a pozitív egészek egyértelmű felbonthatóságát prímszámok szorzatára) alkalmas p, q, r, s pozitív egészekkel $a=pq$, $b=rs$, $c=pr$, $d=qs$.

(2) Megmutatjuk, hogy az a, b, c, d számok relatív prímek. Tegyük fel ugyanis, hogy létezik 1-nél nagyobb k közös osztójuk; ekkor

$$a_1=\frac{a}{k},\quad b_1=\frac{b}{k},\quad c_1=\frac{c}{k},\quad d_1=\frac{d}{k}$$

pozitív egészek, és $a_1^2+b_1^2=c_1^2-d_1^2,\ a_1b_1=c_1d_1$. Ez azonban $a_1b_1c_1d_1=\dfrac{abcd}{k^4}<abcd$ miatt lehetetlen.

(3) Egymáshoz relatív prímek az a, b számok, és ugyanúgy a c, d számok is. Tételezzük fel ugyanis például, hogy a-nak és b-nek létezik közös, l prímosztója. Ekkor $cd=ab$ is osztható l-lel, ami csak úgy lehetséges, hogy c vagy d is osztható l-lel. Azonban $c^2-d^2=a^2+b^2$ is l-lel osztható lévén, c és d mindegyike l-lel osztható, ez pedig ellentmond (2)-nek. Ugyanígy látható be az is, hogy c és d relatív prímek.

(4) Négyzetszám 4-gyel osztva 1-et vagy 0-t adhat csak maradékul. Az $a^2+b^2=c^2-d^2$ egyenlőség ezért (relatív prím a, b-vel) csak akkor teljesülhet, ha a és b közül az egyik páros, a másik páratlan, c páratlan, d pedig páros. Az a és b szerepe felcserélhető, így feltehetjük, hogy például a páros és b páratlan. Az (1)-beli felbontások szereplőiről ezért tudhatjuk, hogy r és s páratlan, és ha p páratlan, akkor q páros. A (3)-ból pedig az következik, hogy a p, q, r, s számok egymáshoz páronként relatív prímek.

(5) Feltételezésünk és (1) szerint $p^2q^2+r^2s^2=p^2r^2-q^2s^2$, ezért

$$\left(r^2+q^2\right)s^2=p^2\left(r^2-q^2\right).$$

Mivel p^2 osztója $\left(r^2+q^2\right)s^2$-nek és relatív prím s^2-hez, ezért p^2 osztója kell legyen $\left(r^2+q^2\right)$-nek. Viszont r^2+q^2 és r^2-q^2 is relatív prímek: ha ugyanis t közös osztójuk, akkor t osztója $\left(r^2+q^2\right)+\left(r^2-q^2\right)=2r^2$-nek és $\left(r^2+q^2\right)-\left(r^2-q^2\right)=2q^2$-nek, így $t\mid\left(2r^2,2q^2\right)=2\left(r^2,q^2\right)=2(r,q)^2$. A (4) szerint $(r,q)=1$, és r^2+q^2 páratlan, ezért t csak 1 lehet. Tehát, mivel r^2+q^2 osztója $p^2\left(r^2-q^2\right)$-nek és relatív prím $\left(r^2-q^2\right)$-hez, r^2+q^2 osztója p^2-nek is, ezért az előbb belátott $p^2\mid r^2+q^2$ miatt

$$r^2+q^2=p^2,\qquad \text{és akkor szükségképpen}\qquad s^2+q^2=r^2.$$

Ez azt jelenti, hogy az r, q, p és az s, q, r egy-egy pitagoraszi számhármas, amelynek elemei egymáshoz relatív prímek, és q páros. Ismeretes, hogy ekkor (alkalmas x_1, y_1, ill. x_2, y_2 pozitív egészekkel)

$$r=x_1^2-y_1^2,\qquad q=2x_1y_1,\qquad p=x_1^2+y_1^2,\qquad \text{illetve} s=x_2^2-y_2^2,\qquad q=2x_2y_2,\qquad r=x_2^2+y_2^2.$$

Így $x_1^2-y_1^2=x_2^2+y_2^2$ és $x_1y_1=x_2y_2$. Azonban

$$x_1y_1x_2y_2=\frac{q^2}{4}\le(pqrs)^2=abcd,$$

ellentmondás.

Ujváry-Menyhárt Mónika (Fazekas M. Főv. Gyak. Gimn., IV. o.t.)