I. megoldás. Tegyük fel, hogy a p prímszámra

(1) $$p=a^2+b^2=x^2+y^2.$$

Ha $a=x$, akkor $b^2=y^2$, a két felbontás azonos, így föltehető, hogy $a>x$. Ekkor

$$0<p(a^2-x^2)=(x^2+y^2)a^2-(a^2+b^2)x^2=y^2a^2-x^2b^2.$$

A jobb oldalon négyzetek különbsége áll, ami szorzattá alakítható, és így

(2) $$0<p(a^2-x^2)=(ya+xb)(ya-xb).$$

A *Cauchy–Schwartz* egyenlőtlenség szerint a jobb oldal tényezőinek a négyzete legfeljebb

$$(a^2+b^2)(x^2+y^2)=p^2,$$

így (2) jobb oldala egyik tényezőjének abszolút értéke sem nagyobb p-nél. A p másfelől prímszám, így a két tényező közül legalább az egyiknek osztója. Mivel a tényezők egyike sem nulla, ez pontosan akkor lehetséges, ha

$$\begin{aligned}&\text{vagy}\quad ya+xb=p,\quad \text{és így}\quad ya-xb=a^2-x^2,\\ &\text{vagy}\quad ya-xb=p,\quad \text{és így}\quad ya+xb=a^2-x^2.\end{aligned}$$

Mindkét esetben a két egyenlőséget összeadva és felhasználva, hogy $p=x^2+y^2$, kapjuk, hogy

$$2ya=a^2+y^2,\quad \text{azaz}\quad (a-y)^2=0,$$

tehát $a=y$, és így $b^2=x^2$.

Ez azt jelenti, hogy a p prímszám valóban legfeljebb egyféleképpen írható fel két négyzetszám összegeként.

Matolcsi Máté (Bp., Fazekas M. Gyak. Gimn., II. o. t.)
dolgozata nyomán

II. megoldás. Az (1) feltételben p-vel osztva kapjuk:

$$1=\frac{a^2+b^2}{p}=\frac{(a^2+b^2)(x^2+y^2)}{p^2}.$$

A számláló az ismert Euler – Lagrange azonosság szerint kétféleképpen is felírható két négyzetszám összegeként:

$$(a^2+b^2)(x^2+y^2)=(ax+by)^2+(ay-bx)^2=(ax-by)^2+(ax+bx)^2.$$

Így kapjuk, hogy

(3) $$1=\left(\frac{ax+by}{p}\right)^2+\left(\frac{ax-bx}{p}\right)^2=\left(\frac{ax-by}{p}\right)^2+\left(\frac{ay+bx}{p}\right)^2.$$

Az első megoldás (2) felbontásához hasonlóan kapjuk, hogy $p(y^2-b^2)=a^2y^2-b^2x^2=(ay+bx)(ay-bx)$, azaz vagy $p|ay+bx$ vagy $p|ay-bx$. A (3)-beli két felbontásban tehát legalább az egyik esetben valamelyik tag egész, így viszont, mivel az összeg 1, a másik tagnak is egésznek kell lennie. Föltehető, hogy erre a megadott két felbontás közül az elsőben kerül sor. Így

$$1=\left(\frac{ax+by}{p}\right)^2+\left(\frac{ay-bx}{p}\right)^2,$$

és a jobb oldalon egész számok állnak. Ez csak úgy lehetséges, ha egyikük 0, másikuk pedig 1. Nyilván föltehető, hogy a, b, x és y nemnegatív egészek, így viszont csak

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

és

$$ay-bx=0$$

lehetséges. A talált feltételek elsőfokú kétismeretlenes egyenletrendszert alkotnak x-re és y-ra, mint ismeretlenekre. Ennek egyetlen megoldása $x=a$ és $y=b$, ami azt jelenti, hogy egy prímszámnak két négyzetszám összegeként való előállítása valóban egyértelmű.

III. megoldás. Tegyük föl, hogy egy adott $p>1$ egész két különböző módon is előáll két négyzet összegeként, azaz léteznek olyan a, b, c, d egészek, hogy

(4) $$p=a^2+b^2=c^2+d^2.$$

Megmutatjuk, hogy ekkor a p összetett. Ez nyilván teljesül, ha a négy szám valamelyike 0, hiszen ekkor a p négyzetszám. Föltehető tehát, hogy a, b, c és d pozitív egészek.

A (4)-ből rendezés után négyzetek különbségének egyenlőségét kapjuk; ezt szorzattá alakítva

$$(a-c)(a+c)=(d-b)(d+b) \tag{5}$$

adódik. Vegyük észre, hogy az a, b, c, d számokat az (5) egyenlőség tényezői egyértelműen meghatározzák: bevezetve az

$$x=a-c,\quad y=a+c,\quad z=d-b,\quad v=d+b$$

változókat,

$$a=\frac{x+y}{2},\quad b=\frac{v-z}{2},\quad c=\frac{y-x}{2},\quad d=\frac{v+z}{2},$$

így (4) az alábbi alakot ölti:

$$4p=4(a^2+b^2)=(x+y)^2+(v-z)^2. \tag{6}$$

Írjuk fel a II. megoldásban is jó szolgálatot tett Euler – Lagrange azonosságot:

$$(A^2+B^2)(C^2+D^2)=(AC+BD)^2+(AD-BC)^2. \tag{7}$$

Ha most a (6) és (7) jobb oldalán álló két négyzetösszeget sikerülne azonosítani, azaz találnánk olyan A, B, C, D egészeket, melyekre

$$x=AC,\quad y=BD,\quad z=BC,\quad v=AD, \tag{8}$$

akkor a (7) azonosság nyomán éppen (6) jobb oldalának egy szorzat alakját kapnánk, azt, hogy

$$4p=(A^2+B^2)(C^2+D^2). \tag{9}$$

A (8) egyenlőség az x, y, z, v egészekre azt mondja, hogy

$$xy=zv.$$

Ekkor viszont a *Kalmár László*tól származó ún. *négyszám-tétel* éppen azt mondja ki, hogy léteznek a (8) szerinti A, B, C és D egészek. (A tétel bizonyítása megtalálható pl. *Reiman István:* A geometria és határterületei c. könyvének (Gondolat, 1986) 268. oldalán.)

Vegyük most szemügyre a (9) jobb oldalán álló tényezőket. Könnyen ellenőrizhető, hogy ha A, B, C és D valamelyike nulla, akkor vagy azonos a két (4)-beli felírás, vagy pedig a, b, c és d között van nem pozitív, márpedig ezeket az eshetőségeket kizártuk. Ha $A=B=1$, akkor $x=z$ és $y=v$, azaz $a=d$ és $c=b$, tehát megint csak nem volna különböző a két (4)-beli felírás. Így $A^2B^2\geq 2^2+1^2=5$ és hasonlóan $C^2D^2\geq 5$. A (9)-ben tehát a $4p$-t két, 4-nél nagyobb egész szorzataként állítottuk elő, ami csak úgy lehetséges, ha a p összetett szám.

Harcos Gergely (Bp., Apáczai Cs. J. Gyak. Gimn., III. o. t.)
dolgozata nyomán