I. megoldás: A számelmélet alaptétele értelmében d prímszámhatványok szorzatára történő felbontásában csak azok a prímszámok szerepelhetnek, amelyek pn^2 felbontásában szerepelnek, és legfeljebb akkora kitevőn, mint az utóbbi felbontásban. Így két esetet különböztethetünk meg. Ha p nem szerepel d felbontásában, akkor d osztója n^2-nek is, ha pedig szerepel, akkor $d = pd'$, ahol d' osztója n^2-nek.

Feltétel szerint van olyan m pozitív egész, amelyre az első esetben

$$d + n^2 = m^2, \quad \text{a másodikban} \quad pd' + n^2 = m^2.$$

Véve d, illetőleg d' egy tetszés szerinti q prím osztóját, azzal n^2 és m^2 is osztható. Mivel a prímtényezős felbontás lényegében egyértelmű, ez csak úgy lehetséges, ha az alapok is oszthatók q-val, és így n^2 és m^2 osztható q^2-tel.

Ekkor d, illetőleg d' is osztható q^2-tel, kivéve a második esetben, ha $q = p$. Az említett eset kivételével tehát egyszerűsíthetünk q^2-tel, és

$$d^* + n'^2 = m'^2, \quad \text{illetőleg} \quad pd^* + n'^2 = m'^2$$

alakú összefüggésekhez jutunk, ahol d^* osztója n'^2-nek.

Ha a második esetben $q = p$, akkor is oszthatunk q^2-tel, csak akkor a fenti első típusú egyenlethez jutunk, ahol d^* most is osztója lesz n'^2-nek.

Az eljárást megismételhetjük sorra d^* minden prím osztójára, és így azt kapjuk, hogy van olyan pozitív egész n_1 és m_1, amelyekkel fennáll, hogy

$$1 + {n_1}^2 = {m_1}^2 \quad \text{vagy} \quad p + {n_1}^2 = {m_1}^2. \tag{1}$$

Az eljárás során minden lépésben n egy q prím osztójának a négyzetével egyszerűsítettünk, tehát végül is egy olyan ${n_2}^2$ egésszel, amelyikre

$$n = n_1 n_2 \quad \text{és} \quad d = {n_2}^2, \quad \text{illetőleg} \quad d = p{n_2}^2.$$

Az (1) alatti első egyenlet nem állhat fenn, mert két pozitív négyzetszám különbsége legalább 3. A második egyenlőségből

$$p = (m_1 + n_1)(m_1 - n_1).$$

Mivel p prímszám, így ebből

$$m_1 + n_1 = p, \quad m_1 - n_1 = 1, \quad \text{tehát} \quad 2n_1 = p - 1.$$

Ezzel azt kaptuk, hogy a feladat feltételei akkor teljesülhetnek, ha

$$n = \frac{1}{2}(p-1)n_2 \quad \text{és} \quad d = p{n_2}^2.$$

Ezekre

$$d + n^2 = \left\{p + \left[\frac{1}{2}(p-1)\right]^2\right\}n_2^2 = \left[\frac{1}{2}(p+1)\right]^2 n_2^2 = \left[\frac{1}{2}(p+1)n_2\right]^2$$

valóban négyzetszám.

Eszerint valóban legfeljebb egy megfelelő d van, éspedig akkor van ilyen, ha n osztható $\frac{1}{2}(p-1)$-gyel.

Megjegyzés: Nem használtuk ki a megoldás során, hogy p páratlan, viszont $p = 2$ esetben az (1) alatti második egyenlőség sem állhat fenn, tehát nincs a feladat feltételeit kielégítő d szám. Ennek bizonyítását kívánta az 1953. évi verseny 2. feladata.[1]

Valamivel rövidebb megoldást kapunk, ha felhasználjuk az úgynevezett eukleidészi lemmát, amelyik szerint ha egy szám osztója egy szorzatnak, de relatív prím az egyik tényezőhöz, akkor osztója a másik tényezőnek.

II. megoldás: Feltétel szerint van olyan k és m egész, amelyekre

$$pn^2 = dk \quad \text{és} \quad d + n^2 = m^2.$$

Jelöljük n és m legnagyobb közös osztóját d'-vel. Ekkor $n = d'n'$, $m = d'm'$, ahol m' és n' egymáshoz relatív prím.

A fenti második egyenlőséget k-val végigszorozva és felhasználva az elsőt és az utolsó két egyenlőséget, az előbbi így írható:

$$(p+k)d'^2n'^2 = kd'^2m'^2, \quad \text{amiből} \quad (p+k)n'^2 = km'^2.$$

A prímtényezős felbontás egyértelműsége folytán m'^2-nek és n'^2-nek csak olyan prímek lehetnek osztói, és így közös osztói is, amelyek az alapoknak is osztói, ami esetünkben azt jelenti, hogy a két négyzet relatív prím. Az eukleidészi lemma szerint tehát n'^2, ami osztója a jobb oldalnak, kell, hogy az első tényezőnek legyen osztója. Alkalmas k' egésszel tehát

$$k = n'^2k'.$$

[1] Lásd, Hajós Gy. – Neukomm Gy. – Surányi J.: *Matematikai versenytételek II. köt.*, 3. kiad., Tankönyvkiadó, Budapest, 1988. 157-158.old.

Ezt beírva utolsó egyenlőségünkbe és egyszerűsítve azt kapjuk, hogy

$$p + n'^2k' = k'm'^2,$$

vagy átrendezve

$$p = k'(m'^2 - n'^2) = k'(m' - n')(m' + n').$$

Mivel p (pozitív) osztói csak 1 és p, így a jobb oldalon egy tényező értéke p, a másik kettőé 1, és mivel az utolsó tényező nagyobb az előtte állónál, így

$$m' + n' = p, \quad k' = m' - n' = 1, \quad \text{tehát} \quad n' = \frac{1}{2}(p-1), \quad n = \frac{1}{2}(p-1)d'.$$

Mindezeket beírva az első feltételi egyenlőségbe és egyszerűsítve azt kapjuk, hogy

$$d = pd'^2,$$

tehát p és n meghatározza d-t – feltéve, hogy egyáltalán létezik megfelelő d; ennek pedig az a feltétele, hogy n osztható legyen $\frac{1}{2}(p-1)$-gyel.

III. megoldás: Legyen m olyan egész szám, amelyikre $d + n^2 = m^2$, azaz

$$d = m^2 - n^2 = (m+n)(m-n).$$

Jelöljük $m+n$ és $m-n$ legnagyobb közös osztóját d'-vel. Ekkor alkalmas b és c egészekkel

$$m + n = bd', \qquad m - n = cd',$$

ahol b és c relatív prím egymáshoz, $b > c$ és

$$d = bcd'^2, \qquad 2n = (b-c)d'.$$

Az, hogy d osztója pn^2-nek, azt jelenti, hogy van olyan k egész, amellyel

$$pn^2 = dk,$$

vagyis 4-gyel szorozva és a fent találtakat beírva

$$p(b-c)^2d'^2 = 4bcd'^2k, \quad \text{amiből} \quad p(b-c)^2 = 4bck.$$

Mivel b-nek és c-nek nincs 1-nél nagyobb közös osztója, így b-nek és c-nek $b-c$-vel sem lehet 1-nél nagyobb közös osztója. Ekkor azonban mind a kettő p-nek kell, hogy osztója legyen, tehát

$$b = p, \quad c = 1, \quad \text{így} \quad k = \left[\frac{1}{2}(p-1)\right]^2, \quad d' = \frac{2n}{p-1};$$

ezekből pedig

$$d = p\left(\frac{2n}{p-1}\right)^2.$$

Ezzel azt kaptuk, hogy p és n már meghatározza d-t. Egyben azt is kaptuk, hogy ilyen d akkor van, ha n az $\frac{1}{2}(p-1)$ többszöröse.

Megjegyzések: 1. Ha $p = 2$, akkor csak annyi változik, hogy $\frac{1}{2}(p-1)$ nem egész, s így semmilyen n-hez nincs megfelelő d.

2. Mind a három megoldás módot ad az alkalmas d osztók megkeresésére akkor is, ha p helyébe tetszés szerinti összetett számot írunk. Ekkor lehet több ilyen d is.