EÖTVÖS LORÁND TUDOMÁNYEGYETEM

TERMÉSZETTUDOMÁNYI KAR

Diofantikus egyenletekről

Szakdolgozat

Készítette:
Szoldatics Szandra
Matematika BSc, tanári szakirány

Témavezető:
Pappné dr. Kovács Katalin
egyetemi docens
Algebra és Számelmélet Tanszék

Budapest
2013.

Tartalomjegyzék

Bevezetés

Tanári szakirányos hallgatóként szeretném úgy összeállítani a szakdolgozatomat, hogy az használható legyen az iskola intézményében is. Véleményem szerint a diofantikus egyenletek sokszínűsége izgalmas lehet a matematika iránt érdeklődő diákok számára, így a téma bevihető szakkörökre, középiskolai tanórára kitekintésként, valamint mindenképpen hasznos ezzel foglalkozni matematika versenyre való készülés során is.

A diofantikus egyenleteket különböző szempontok szerint osztályozhatjuk – bár találkozhatunk besorolhatatlan diofantikus egyenletekkel is. A különböző típusokra alkalmazandó megoldási módszerek áttekintése azonban lehetetlen feladat lenne, nem tudunk minden megoldási módszert számba venni és általánosítani, ráadásul számos megoldatlan problémával találkozhatunk a témakört tanulmányozva.
A célom nem az, hogy ebben az írásban minél több megoldási módszert bemutassak. Szeretnék inkább olyan típusú diofantikus egyenleteket és feladatokat kiragadni, amelyek érdekességük miatt könnyen felkelthetik a diákok érdeklődését és kíváncsiságát.

Először a lineáris diofantikus egyenletekkel foglalkozom, mellyel egy középiskolás diák is gyakran találkozhat.
Külön fejezetben írok azokról a diofantikus egyenletekről, melyeknek végtelen sok megoldásuk van, itt említek meg olyan híresebb típusokat, mint például a Pell-egyenlet, vagy a pitagoraszi számhármasok.
Ezután bemutatok néhány olyan egyenletet, melyeknek nincs megoldása vagy véges sok megoldása van; szerepelnek köztük olyanok is, melyeknek bővebb számok körében már van megoldásuk. Ezek a feladatok általában trükkösek, ezek bizonyításait az adott könyvben szereplő "megoldó kulcs" segítségével, azt könnyen érthetővé téve írtam le.
Geometriai úton keresztül foglalkozom a két- és három-négyzetszám-tétellel, majd innen áttérek a Waring-problémakörre.

Diofantikus egyenletnek általában olyan *egész együtthatós* algebrai egyenletet nevezünk, melynek *megoldásait is az egész számok körében* keressük. Ezek megoldása igen változatos módszereket igényel. Univerzális megoldási módszer nem létezik, még arra sem, hogy egy tetszőlegesen adott diofantikus egyenletnek létezik-e megoldása vagy sem.

Ahhoz, hogy át tudjuk tekinteni az általam vizsgált különböző típusú diofantikus egyenleteket, valamint el tudjuk dönteni a megoldhatóságukat, megoldhatóság esetén meg tudjuk keresni a megoldást vagy megoldásokat, ismernünk kell a következő témakörök alapvető fogalmait, a hozzájuk kapcsolódó fontosabb tételeket, bizonyos algoritmusokat, illetve ezek alkalmazásait:
oszthatóság, legnagyobb közös osztó, euklideszi algoritmus, prímszámok, számelméleti függvények, kongruencia, a számelmélet alaptétele, kis Fermat-tétel.

I. Lineáris diofantikus egyenletek

I. 1 Kétismeretlenes lineáris diofantikus egyenletek

Ebben a fejezetben az ***ax* + *by* = *c*** alakú kétismeretlenes lineáris diofantikus egyenlettel foglalkozunk, megoldásokon *x*, *y* egész számokból álló számpárokat értünk.
Az ilyen típusú diofantikus egyenletek a legegyszerűbben kezelhető diofantikus egyenletek.
Ismerjük a megoldás szükséges és elégséges feltételét, a megoldásszámot és az összes megoldás leírását.

I. 1. 1 Tétel:

Legyenek *a*, *b* és *c* rögzített egész számok, ahol *a* és *b* közül legalább az egyik nem nulla, és tekintsük az *ax* + *by* = *c* diofantikus egyenletet.

(i) Az egyenlet akkor és csak akkor oldható meg, ha $(a, b) \mid c$.
Azaz (az egyenlet megoldható) $\Longleftrightarrow$ $(a, b) \mid c$.

(ii) Megoldhatóság esetén végtelen sok megoldás van. Ha x_0, y_0 egy rögzített megoldás, akkor az összes x', y' megoldást az alábbi képlet szolgáltatja:

$$x' = x_0 + t\frac{b}{(a,b)} \quad , \qquad y' = y_0 - t\frac{a}{(a,b)} \quad , \quad \text{ahol } t = 0, \pm 1, \pm 2, \dots$$
(1)

(iii) Az egyenlet egy megoldását az euklideszi algoritmus segítségével kaphatjuk meg. ◆

Bizonyítás: [F-Gy]

(i) Először ezt látjuk be: <u>(az egyenlet megoldható) $\Longrightarrow$ $(a, b) \mid c$</u> .
Tegyük fel, hogy x_0, y_0 megoldás.
Legyen $a = a_0 \cdot (a,b)$ és $b = b_0 \cdot (a,b)$
Tudjuk: $ax_0 + by_0 = c$
Ezt átírjuk az előzőek alapján: $a_0 \cdot (a,b) \cdot x_0 + b_0 \cdot (a,b) \cdot y_0 = c$
$(a,b) \cdot (a_0x_0 + b_0y_0) = ax_0 + by_0 = c$
Ebből látható: $(a, b) \mid ax_0 + by_0 = c$.

Megfordítva: <u>$(a, b) \mid c$ $\Longrightarrow$ (az egyenlet megoldható)</u>
Tehát tegyük fel, hogy $(a, b) \mid c$.
Tehát van olyan *t* egész, amelyre $(a, b)t = c$.
Segédtétel: [F-Gy: 1. 3. 5. Tétel]
$(a, b) = au + bv$ teljesül alkalmas *u*, *v* egészekkel. ◆

/Bizonyítása az euklideszi algoritmus sorait felhasználva történik./

Az egyenletet t-vel beszorozva kapjuk: $(a, b)t = c = aut + bvt = a(ut) + b(vt)$,
azaz $x = ut$, $y = vt$ megoldása az $ax + by = c$ diofantikus egyenletnek.

(ii) Először azt mutatjuk meg, hogy az (1)-ben megadott x', y' számok valóban az egyenlet egy megoldását szolgáltatják. Mivel x_0 és y_0 megoldás, azaz $ax_0 + by_0 = c$, *így*

$$ax' + by' = a\left(x_0 + t\frac{b}{(a,b)}\right) + b\left(y_0 - t\frac{a}{(a,b)}\right) =$$
$$= ax_0 + t\frac{ab}{(a,b)} + by_0 - t\frac{ab}{(a,b)} =$$
$$= ax_0 + by_0 = c$$

A megfordításhoz tegyük fel, hogy x', y' egy tetszőleges megoldás, és belátjuk, hogy x'és y' a kívánt alakú.
A feltétel szerint $ax_0 + by_0 = c$ és $ax' + by' = c$.
A két egyenlőséget egymásból kivonva

$$ax_0 + by_0 - ax' - by' = 0$$

$$a(x_0 - x') + b(y_0 - y') = 0$$

adódik.
Rendezzük az egyenletet, majd osztunk (a, b)-vel:

$$a(x_0 - x') = -b(y_0 - y')$$

$$a(x_0 - x') = b(y' - y_0)$$

$$\frac{a}{(a,b)}(x_0 - x') = \frac{b}{(a,b)}(y' - y_0) \qquad (2)$$

Mivel

$$\left(\frac{b}{(a,b)}, \frac{a}{(a,b)}\right) = 1,$$

ezért (2)-ből

$$\frac{b}{(a,b)} \mid x' - x_0$$

azaz alkalmas t egésszel

$$x' - x_0 = t\frac{b}{(a,b)}$$

$$x' = x_0 + t\frac{b}{(a,b)} \qquad (3)$$

következik.

A (3)-at (2)-be visszahelyettesítve a következőt kapjuk:

$$\frac{a}{(a,b)}\left(x_0 + t\frac{b}{(a,b)} - x_0\right) = \frac{b}{(a,b)}(y_0 - y')$$

$$\frac{a}{(a,b)} \cdot t\frac{b}{(a,b)} = \frac{b}{(a,b)}(y_0 - y')$$

$$t\frac{a}{(a,b)} = y_0 - y'$$

$$y' = y_0 - t\frac{a}{(a,b)}$$

Ezzel megmutattuk, hogy x'és y' valóban az (1)-ben előírt alakú.

(iii) Az (i)-ben szereplő segédtétel bizonyítja. ■

A diofantikus egyenletek megoldásakor érdemes az euklideszi algoritmusnak egy olyan variánsát alkalmazni, melynek segítségével egyszerre tudjuk az összes megoldást előállítani.
Az eljárás bemutatására nézzünk egy konkrét példát:

$\boxed{\text{I. } 1/1. \text{ Feladat}}$ [F-Gy: 7.1.2. feladat]

Egy szigeten 7- és 11-fejű sárkányok élnek.
Hány sárkány él a szigeten, ha összesen 118 fejük van?

A feladat szövege alapján a következő diofantikus egyenlet írható fel:

$$7x + 11y = 118$$

Vonatkoztassunk most el a feladat szövegétől, foglalkozzunk a felírt diofantikus egyenlettel, keressük az összes megoldást.
Fejezzük ki az egyenletből azt az ismeretlent, amelynek az együtthatója kisebb abszolút értékű (itt x), és a törtből válasszunk le olyan részeket, amelyek biztosan egész értékűek:

$$x = \frac{118 - 11y}{7} = 16 - y + \boxed{\frac{6 - 4y}{7}} \qquad \text{(A1)}$$

Ekkor az (A1) jobb oldalán álló keretezett tört is egész szám kell, hogy legyen, jelöljük u-val.
Innen $6 - 4y = 7u.$
Ez egy hasonló diofantikus egyenlet, mint az eredeti, csak itt y együtthatójának kisebb az abszolút értéke, mint az eredeti egyenletben x együtthatójáé volt.
Ismételjük meg most az előző eljárást a $6 - 4y = 7u$ egyenletre.

$$y = \frac{7u - 6}{-4} = \frac{6 - 7u}{4} = 1 - u + \boxed{\frac{2 - 3u}{4}} \qquad \text{(A2)}$$

A keretezett tört egész szám kell, hogy legyen, jelöljük v-vel, ismételjük az eljárást.

$$2 - 3u = 4v$$

$$u = \frac{4v - 2}{-3} = \frac{2 - 4v}{3} = -v + \boxed{\frac{2 - v}{3}} \tag{A3}$$

A keretezett tört egész szám kell, hogy legyen, jelöljük w-vel, ismételjük az eljárást.

$$2 - v = 3w$$

$$v = 2 - 3w \tag{A4}$$

Mivel (A4)-ben már nem szerepel tört, most elindulunk "visszafelé", és rendre (A3), (A2), (A1) felhasználásával u, y, x értékeket kifejezzük a w paraméter segítségével:

$$u = -v + w = (3w - 2) + w = 4w - 2 \tag{B3}$$

$$y = 1 - u + v = 1 - (4w - 2) + (2 - 3w) = 5 - 7w \tag{B2}$$

$$x = 16 - y + u = 16 - (5 - 7w) + (4w - 2) = 9 + 11w \tag{B1}$$

A módszerből világos, hogy az $x = 9 + 11w,\ \ y = 5 - 7w$ képletek szolgáltatják a $7x + 11y = 118$ diofantikus egyenlet összes megoldását, ahol w paraméter tetszőleges egész szám. Hiszen ha egy x, y egész számpár megoldás, akkor az (A1)-(A3) lépéseken keresztül eljutunk w-hez, majd ennek segítségével x-re és y-ra a (B2)-(B1) képletpár adódik. Valamint tetszőleges egész w-re az így képzett x és y számok egészek lesznek és kielégítik az egyenletet.

Térjünk most vissza a feladat szövegéhez.
Különböző w paramétereket kipróbálva láthatjuk, hogy egy esetet kivéve x és y valamelyike mindenképpen negatív előjelű lesz. Ez ellentmond a feladat szövegével, mert negatív előjelű nem lehet a sárkányok száma. Így csak az a megoldás kielégítő, melyben x és y is nemnegatív, azaz:

$w = 0\ esetén$: $\qquad x = 9 + 11 \cdot 0 = 9 \qquad és \qquad y = 5 - 7 \cdot 0 = 5$

Ez alapján tudjuk, hogy 9 7-fejű és 5 11-fejű sárkány, azaz *összesen 14 sárkány él a szigeten*. ✓

A fenti módszer lényege tehát, hogy az ismeretlenek együtthatóinak az abszolút értékeit megfelelően csökkentve végül a törteket teljesen kiküszöbölhetjük.

Nem szükséges a megoldhatóság feltételét előre külön ellenőrizni, az eljárásból is automatikusan kiderül, ha nincs megoldás. Ekkor egy olyan törthöz jutunk, amelyben már nem szerepel ismeretlen, azonban a tört értéke nem egész szám. Ehhez példafeladat (megoldás nélkül):

$\boxed{\text{I. 1/2. Feladat}}$ [Saját]

Bolondóciában csak 9 és 24 forintos pénzérmék léteznek.
Hányféleképpen lehet pontosan 70 Forintot kifizetni?

I. 1/3. Feladat [Saját]

Határozzuk meg a 6x+8y=10 egyenes egész koordinátájú pontjait.

Emlékeztető: *Kongruenciák*

Definíció: a és b egész számok, m pozitív egész. Azt mondjuk, hogy "*a kongruens b –vel modulo m*", ha $m \mid a-b$.

Jelölés: $a \equiv b \pmod{m}$

A kongruencia reflexív, szimmetrikus és tranzitív reláció, azaz ekvivalenciareláció.
Az ugyanazon modulus szerinti kongruenciák "összeadhatók", "kivonhatók" és "összeszorozhatók". Egy kongruencia mindkét oldalához hozzáadhatjuk ugyanazt a számot, ugyanez vonatkozik a kivonásra és a szorzásra is, továbbá egy kongruenciát szabad pozitív egész kitevős hatványra emelni. Ha a kongruencia mindkét oldala osztható egy pozitív egésszel, akkor azzal oszthatunk is. Ekkor a modulust is el kell osztanunk az osztó szám és a modulus legnagyobb közös osztójával.

I. 1. 2 Tétel:

Az $ax \equiv b \pmod{m}$ kongruencia akkor és csak akkor oldható meg, ha megoldható az $ax + my = b$ lineáris diofantikus egyenlet. ◆

Bizonyítás:

Az $ax \equiv b \pmod{m}$ kongruencia megoldhatósága azt jelenti, hogy van olyan s egész, melyre $as \equiv b \pmod{m}$.
Ez tovább ekvivalens azzal, hogy van olyan t egész, amelyre $as + mt = b$ teljesül, vagyis s és t kielégíti az $ax + my = b$ lineáris diofantikus egyenletet. ■

Ez azt jelenti, hogy az $ax \equiv b \pmod{m}$ lineáris kongruencia és az $ax + my = b$ lineáris diofantikus egyenlet kölcsönösen visszavezethetők egymásra.

A feladat megoldása:
Egy egyenes egész koordinátájú pontjait meghatározó koordinátákat keressük, azaz azokat az x, y egész számokat, melyek kielégítik az adott egyenletet.
A **I. 1. 2 Tétel** alapján az adott lineáris diofantikus egyenlet kongruenciával is megoldható:

$$6x \equiv 10 \pmod{8}$$
$$6x \equiv 18 \pmod{8}$$
$$x \equiv 3 \pmod{4}$$

Tehát az x koordináta $4k + 3$ alakú. Ezt behelyettesítve az egyenletbe kifejezhetjük y-t:

$$6(4k + 3) + 8y = 10$$

$$y = \frac{10 - 24k - 18}{8} = -3k - 1\,.$$

Tehát az összes egész koordinátájú pontot a következőképpen adhatjuk meg:

$$x' = 4k + 3 \qquad\qquad y' = -3k - 1$$

I. 2 Kettőnél több ismeretlenes lineáris diofantikus egyenletek

Kettőnél több ismeretlenes lineáris diofantikus egyenletekre is a kétismeretlenes esethez hasonló állítások érvényesek.

I. 2 Tétel:

Legyen $k \geq 2$, $a_1, \dots, a_k$ nem csupa 0 egész számok, c tetszőleges egész, és tekintsük az

$$a_1 x_1 + \cdots + a_k x_k = c$$

diofantikus egyenletet.

(i) Az egyenlet akkor és csak akkor oldható meg, ha $(a_1, \dots, a_k) | \, c$.

(ii) Megoldhatóság esetén végtelen sok megoldás van. Az összes megoldás k-1 egész paraméter segítségével adható meg. A megoldások meghatározása a két ismeretlen esetén látott módszer értelemszerű általánosításával történik. ◆

(Bizonyítás nélkül.)

$\boxed{\text{I. 2/1. Feladat}}$ [Saját]

Adjuk meg a $7x + 10y + 15z = 6$ *diofantikus egyenlet összes megoldását.*

$7x + 5(2y + 3z) = 6$

Vezessük be a p paramétert: $2y + 3z = p$

Ezt egy önálló diofantikus egyenletként vizsgálva megállapíthatjuk, hogy létezik megoldása, hiszen $(2, 3) = 1$, amely biztosan osztója p –nek.

Tekintsük most az eredeti egyenletet a p paraméterrel:

$$7x + 5p = 6$$

Keressünk egy x_0, p_0 megoldást: $x_0 = 3$; $p_0 = -3$

Ezek ismeretében fel tudjuk írni az összes megoldást:

$$x' = x_0 + q\frac{5}{(5,7)} = 3 + 5q$$

$$p' = p_0 - q\frac{7}{(5,7)} = -3 - 7q$$

ahol q tetszőleges egész.

p -be visszahelyettesítve: $p = 2y + 3z = -3 - 7q$

Az **I. 1. 2 Tétel** alapján a $2y + 3z = -3 - 7q$ diofantikus egyenlet a következő kongruenciává “alakítható”:

$$3z \equiv -3 - 7q \quad (mod\ 2)$$
$$z \equiv 1 + q \quad (mod\ 2),$$

tehát $z = 2r + q + 1$.
Ezt a $2y + 3z = -3 - 7q$ egyenletbe visszahelyettesítve megkapjuk, hogy $y = -5q - 3r - 3$.

Tehát $\boldsymbol{x = 5q + 3}$, $\boldsymbol{y = -5q - 3r - 3}$, $\boldsymbol{z = q + 2r + 1}$.

Ellenőrizzük le:

$$7x + 10y + 15z = 7(5q + 3) + 10(-5q - 3r - 3) + 15(q + 2r + 1) =$$

$$= 35q + 21 - 50q - 30r - 30 + 15q + 30r + 15 = 6. \checkmark$$

II. Magasabb fokú diofantikus egyenletek Különböző megoldásszámok

II. 1 Végtelen sok megoldás van

A lineáris diofantikus egyenleteknél láttuk, hogy megoldhatóság esetén végtelen sok megoldás van. Tekintsük most a magasabb fokú diofantikus egyenleteket. Ezek között is vannak olyan egyenletek, melyeknek végtelen sok megoldásuk van. Tekintsünk most néhány ilyen diofantikus egyenletet.

II. 1. 1 Pitagoraszi számhármasok

*Pitagoraszi számhármas*oknak az $x^2 + y^2 = z^2$ egyenlet pozitív egész megoldásait nevezzük. Már a középiskolás diákok is könnyen felismerhetik az egyenletben a Pitagorasz-tételt, így ők is láthatják, hogy geometriai megfogalmazásban a pitagoraszi számhármasok olyan derékszögű háromszögek oldalhosszai, mely oldalhosszak egész számok.

Azonnal látszik, hogy ha van egy x, y, z megoldás, akkor az egyenletet tetszőleges d pozitív egésszel beszorozva a kapott dx, dy, dz számhármas is megoldás. Ezért külön érdemes vizsgálni azokat a megoldásokat, ahol $(x, y, z) = 1$. Ezeket *alapmegoldások*nak vagy *primitív pitagoraszi számhármasok*nak nevezzük.

II. 1. 1 Tétel:

(i) Az $x^2 + y^2 = z^2$ egyenletnek az $(x, y, z) = 1$ feltételt kielégítő összes pozitív megoldását a következő képlet szolgáltatja (itt az x és y felcseréléséből adódó megoldásokat azonosnak tekintjük):

$$x = 2mn, \qquad y = m^2 - n^2, \qquad z = m^2 + n^2,$$

ahol az m és n paraméterek tetszőleges olyan pozitív egészek, amelyekre

$$m \text{ és } n \text{ különböző paritású}, \qquad m > n \qquad \text{és} \qquad (m, n) = 1. \tag{1}$$

(ii) Az $x^2 + y^2 = z^2$ egyenlet összes pozitív egész megoldását (azaz az összes pitagoraszi számhármast) az alapmegoldások többszöröseiként kapjuk meg, tehát

$$x = 2mnd, \qquad y = (m^2 - n^2)d, \qquad z = (m^2 + n^2)d,$$

ahol d tetszőleges pozitív egész, az m és n pozitív egészekre pedig teljesül (1). ◆

$\boxed{\text{II. 1.1/1. Feladat}}$ [F-Gy: 7.2.1. feladat]

Mutassuk meg, hogy ha egy derékszögű háromszög oldalai egész számok, akkor az oldalhosszak szorzata osztható 60-nal.

Elég az alapmegoldásokra szorítkozni.
A háromszög befogói legyenek x és y, az átfogó legyen z.
A **II. 1. 1 Tétel** miatt: $x = 2mn$, $y = m^2 - n^2$, $z = m^2 + n^2$, m és n különböző paritású egészek, $m > n$ és $(m, n)=1$.
A következőt kell bizonyítanunk:

$$60 \mid xyz = 2mn(m^2 - n^2)(m^2 + n^2)$$

Elég belátni, hogy

$$30 \mid mn(m-n)(m+n)(m^2 + n^2)$$

Azt kell vizsgálnunk, hogy 30 prímosztói osztói-e a

$$mn(m-n)(m+n)(m^2 + n^2) \qquad (*)$$

kifejezésnek.

$$30 = 2 \cdot 3 \cdot 5$$

- Igaz, hogy $2 \mid mn(m-n)(m+n)(m^2+n^2)$?
  Mivel m és n különböző paritású, így a szorzatuk páros, tehát $2 \mid mn$, így $2 \mid mn(m-n)(m+n)(m^2+n^2)$. ✓
- Igaz, hogy $3 \mid mn(m-n)(m+n)(m^2+n^2)$?
  - $3 \mid m$ vagy $3 \mid n \Rightarrow 3 \mid mn(m-n)(m+n)(m^2+n^2)$ ✓
  - $3 \nmid m$ és $3 \nmid n$:
    Ha $m = 3k+1$ és $n = 3l+1$, vagy $m = 3k-1$ és $n = 3l-1$,
    akkor $m - n = 3k - 3l = 3(k-l)$, tehát $3 | m - n$, így
    $3 \mid mn(m-n)(m+n)(m^2+n^2)$ ✓
- Igaz, hogy $5 \mid mn(m-n)(m+n)(m^2+n^2)$?
  - $5 \mid m$ vagy $5 \mid n \Rightarrow 5 \mid mn(m-n)(m+n)(m^2+n^2)$ ✓
  - $5 \nmid m$ és $5 \nmid n$:
    Ha $m = 5k+1$ és $n = 5l+1$, vagy $m = 5k-1$ és $n = 5l-1$, akkor $m - n = 5k - 5l = 5(k-l)$, tehát $5 | m - n$, így $5 \mid mn(m-n)(m+n)(m^2+n^2)$.
    Ha $m = 5k+1$ és $n = 5l-1$, vagy $m = 5k-1$ és $n = 5l+1$, akkor $m + n = 5k + 5l = 5(k+l)$, tehát $5 | m + n$, így $5 \mid mn(m-n)(m+n)(m^2+n^2)$.

    Ha $m = 5k+2$ és $n = 5l+2$, vagy $m = 5k-2$ és $n = 5l-2$, akkor $m - n = 5k - 5l = 5(k-l)$, tehát $5 | m - n$, így $5 \mid mn(m-n)(m+n)(m^2+n^2)$.
    Ha $m = 5k+2$ és $n = 5l-2$, vagy $m = 5k-2$ és $n = 5l+2$, akkor $m + n = 5k + 5l = 5(k+l)$, tehát $5 | m + n$, így $5 \mid mn(m-n)(m+n)(m^2+n^2)$.

    Ha $m = 5k \pm 1$ és $n = 5l \pm 2$, akkor
    $m^2 + n^2 = (5k \pm 1)^2 + (5l \pm 2)^2 = 25k^2 \pm 10k + 1 + 25l^2 \pm 20l + 4 =$
    $= 5 \cdot (5k^2 \pm 2k + 5l^2 \pm 4l + 1)$, tehát $5 \mid m^2 + n^2$,
    így $5 \mid mn(m-n)(m+n)(m^2+n^2)$.
    Ha $m = 5k \pm 2$ és $n = 5l \pm 1$, akkor az előzőhöz hasonló módon tudjuk bizonyítani, hogy $5 \mid mn(m-n)(m+n)(m^2+n^2)$. ✓

Tehát 2, 3 és 5 osztják a $mn(m-n)(m+n)(m^2+n^2)$ kifejezést. Mivel ezek páronként relatív prímek, ezért a szorzatuk is osztja $mn(m-n)(m+n)(m^2+n^2)$ -t. ✓

$\boxed{\text{II. 1. 1/2. Feladat}}$ [F-Gy: 7.2.2. feladat]

Számítsuk ki a derékszögű háromszög oldalait, ha tudjuk, hogy az oldalak egész számok és a háromszög területe 60.

A háromszög befogói legyenek x és y, az átfogó legyen z.
Tudjuk, hogy a háromszög területe 60, emiatt

$$\frac{x \cdot y}{2} = 60 \qquad \Rightarrow \qquad x \cdot y = 120$$

A **II. 1. 1 Tétel** miatt: $x = 2mnd$, $y = (m^2 - n^2)d$, m és n különböző paritású egészek, $m > n$ és $(m, n)=1$.
Az előző egyenletet átalakítva a következőt kapjuk:

$$d^2 2mn(m-n)(m+n) = 120$$

$$d^2 mn(m-n)(m+n) = 60$$

Látjuk, hogy $d^2 \mid 60$. Ez csak $d = 1$ vagy $d = 2$ esetében igaz.

Tegyük fel, hogy $d = 2$. Ekkor a következő eset állna fenn: $mn(m-n)(m+n) = 15$
Ez azonban nem, lehetséges m és n különböző paritása miatt.
Tehát $d = 1$.

Keressük tehát azt az m-et és n-et, melyekre igaz az $mn(m-n)(m+n) = 60$ egyenlet.
Bontsuk fel a 60-at prímtényezők szorzatára: $60 = 2^2 \cdot 3 \cdot 5$.
A felbontást figyelembe véve próbálgatással is könnyen megkaphatjuk az eredményt: $m = 4$, $n = 1$.
Tehát $x = 2 \cdot 4 \cdot 1 = 8$, $y = 4^2 - 1^2 = 15$, $z = 4^2 + 1^2 = 17$.
A háromszög oldalai tehát 8, 15 és 17.

II. 1. 2 Pell-egyenlet

“Pell-egyenletnek egy

$$x^2 - my^2 = 1$$

(1)
alakú diofantikus egyenletet nevezünk, ahol az m (rögzített) pozitív egész és nem négyzetszám.
Az (1) egyenlet triviális megoldása az $x = \pm 1$, $y = 0$, az ezektől különböző megoldások a nemtriviális megoldások.

Az (1) bal oldalát szorzattá bonthatjuk:

$$\left(x + y\sqrt{m}\right)\left(x - y\sqrt{m}\right) = 1.$$

(2)

Ebből következik, hogy ha x, y megoldása (1)-nek, akkor az $a + b\sqrt{m}$ alakú számok körében (ahol a és b egészek) az $x + y\sqrt{m}$ és $x - y\sqrt{m}$ számok osztói az 1-nek, és így mindketten egységek. Mivel egy egység tetszőleges egész kitevős hatványa is egység, ezért ha létezik egy $\varepsilon \neq \pm 1$ egység, akkor az ε hatványai végtelen sok egységet adnak.
Ez a Pell-egyenlet esetében azt jelenti, hogy ha (1)-nek létezik nemtriviális megoldása, akkor végtelen sok megoldás van." [F-Gy: 7.8.]

II. 1. 2/1. Tétel:

Legyen m olyan pozitív egész, amely nem négyzetszám. Ekkor az (1) diofantikus egyenletnek végtelen sok megoldása van. ◆

(Bizonyítás nélkül.)

II. 1. 2/2. Tétel:

Legyen m olyan pozitív egész, amely nem négyzetszám, és $x_0,\ y_0$ az (1) diofantikus egyenletnek a(z egyértelműen meghatározott) megoldása, amelyre $x_0 > 0,\ y_0 > 0$ és $x_0 + y_0\sqrt{m}$ minimális. Ekkor az összes megoldást az

$$x + y\sqrt{m} = \pm(x_0 + y_0\sqrt{m})^n, \qquad n = 0, \pm 1, \pm 2, \dots$$

képlettel meghatározott $x,\ y$ egész számpárok adják. ◆

(Bizonyítás nélkül.)

$\boxed{\text{II. 1.2/1. Feladat}}$ [Saját]

Határozzuk meg a $x^2 - 12y^2 = 1$ *egyenletű hiperbola egész koordinátájú pontjait.*

Megállapítjuk, hogy a 12 nem négyzetszám, így az adott diofantikus egyenlet Pell-egyenlet.
A III. 2. 1. Tétel szerint ennek végtelen sok megoldása van. Most a III. 2. 2. Tétel alapján megadjuk az összes megoldást. Olyan x_0, y_0 megoldást keresünk, melyre $x_0 + y_0\sqrt{12}$ minimális.
Ez a megoldás a következő: $x_0 = 7,\ \ y_0 = 2.$
Az összes egész koordinátájú pont koordinátáit tehát az

$$x + y\sqrt{12} = \pm(7 + 2\sqrt{12})^n, \qquad n = 0, \pm 1, \pm 2, \dots$$

képlet segítségével kapjuk meg.
Pl. $n = 2$ -re:

$$\pm(7 + 2\sqrt{12})^2 = \pm\left(49 + 28\sqrt{12} + 48\right) = \pm(97 + 28\sqrt{12})$$

$$x_1 = \pm 97, \qquad y_0 = \pm 28$$

(Ellenőrizve a megoldást:

$$97^2 - 12 \cdot 28^2 = 9409 - 9408 = 1 \ \checkmark\ )$$

$\boxed{\text{II. 1.2/2. Feladat}}$ [F-Gy: 7.8.4/a1 feladat]

Hány olyan négyzetszám van, amely 1-gyel nagyobb egy négyzetszám kétszeresénél?

A feladat szövege alapján pl. a következő egyenlet írható fel:

$$x^2 = 2y^2 + 1,$$

amelyet átrendezve Pell-egyenletet kapunk, melyről tudjuk, hogy végtelen sok megoldása van, tehát végtelen sok olyan négyzetszám van, amely 1-gyel nagyobb egy négyzetszám kétszeresénél.

II. 1. 3 Egyéb végtelen megoldásszámú diofantikus egyenletek

Számos olyan diofantikus egyenlettel találkozhatunk, amelyek megoldásához nem elég az eddigi tételeket ismerni és alkalmazni, hanem egy ügyes ötlet is szükséges. Erre nézünk most néhány példát.

$\boxed{\text{II. 1. 3/1. Feladat}}$ [S: 123.]

Bizonyítsuk be, hogy az

$$(x-1)^2 + (x+1)^2 = y^2 + 1 \tag{1}$$

egyenletnek végtelen sok x, y megoldása van a természetes számok körében.

Tekintsük a következő egyenletet:

$$(2y + 3x - 1)^2 + (2y + 3x + 1)^2 = (3y + 4x)^2 + 1 \tag{2}$$

A zárójelek felbontása és összevonás után a következőt kapjuk:

$$8y^2 + 18x^2 + 24xy + 2 = 9y^2 + 24xy + 16x^2 + 1$$

$$2x^2 + 1 = y^2 \tag{3}$$

Most alakítsuk át az (1)-es egyenletet:

$$(x-1)^2 + (x+1)^2 = y^2 + 1$$

$$x^2 - 2x + 1 + x^2 + 2x + 1 = y^2 + 1$$

$$2x^2 + 1 = y^2$$

Láthatjuk, hogy az (1) –es és (2) – es egyenletet is a (3) – as alakra tudjuk hozni, ezzel bebizonyítottuk, hogy az (1) – es és (2) – es egyenlet ekvivalens egymással.
Tehát az (1) egyenlet bármely x, y pozitív egész megoldásából származtatható a nagyobb természetes számokból álló $2y + 3x$ és $3y + 4x$ megoldása.

Mivel pedig $x = 2$ és $y = 3$ kielégítik az egyenletet, ezért valóban végtelen sok pozitív egész megoldása létezik. ✓

$\boxed{\text{II. 1. 3/2. Feladat}}$ [S: 123 b.]

Bizonyítsuk be, hogy minden n természetes számra az

$$(x+1)^3 + (x+2)^3 + \ldots + (x+n)^3 = y^3$$

egyenletnek x-re és y-ra van egész megoldása.

1. eset: $n = 2k - 1, \quad k \in \mathbb{N}$

Ekkor $x = -k,\ y = 0$ megoldása az egyenletnek. Ellenőrizzük le!
Helyettesítsük be az egyenletbe a megoldásokat:

$$(-k+1)^3 + \ldots + (-k+k-1)^3 + (-k+k)^3 + (-k+k+1)^3 + \ldots + (-k+2k-1)^3 = 0$$

$$(-k+1)^3 + \ldots + (-1)^3 + 0^3 + 1^3 + \ldots (k-1)^3 = 0$$

Ilyen alakban már könnyen látható, hogy az egyenlőség igaz. ✓

2. eset: $n = 2k,\ k \in \mathbb{N}$

Ekkor $x = -k,\ y = k$ megoldása az egyenletnek. Ellenőrizzük le!
Helyettesítsük be az egyenletbe a megoldásokat:

$$(-k+1)^3 + \ldots + (-k+k)^3 + \ldots + (-k+2k-1)^3 + (-k+2k)^3 = k^3$$

$$(-k+1)^3 + \ldots + 0^3 + \ldots + (k-1)^3 + k^3 = k^3$$

Az előzőhöz hasonló módon, az egyenlőség baloldalán a tagok kiesése után könnyen látható, hogy az egyenlőség igaz. ✓

Megjegyzés: az egyenletnek vannak más megoldásai is:

ha $n = 8$: $x = -3,\quad y = 6$
ha $n = 25$: $x = -11,\quad y = 20$
ha $n = 1000$: $x = 1333,\quad y = 16830$

II. 2 Nem létezik pozitív egész megoldás

A következőkben olyan diofantikus egyenletekkel foglalkozunk, melyeknek nincs pozitív egész megoldásuk. A megoldhatatlanságot fogjuk bizonyítani, illetve azt vizsgáljuk, hogy más számok körében van-e megoldás.

$\boxed{\text{II. 2/1. Feladat}}$ [S: 129]

Bizonyítsuk be, hogy az

$$x^2 - 2y^2 + 8z = 3$$

egyenletnek nem létezik x, y, z egész megoldása.

1. eset: *y* páros, legyen $y = 2k,$ $k \in \mathbb{Z}$.

Ekkor $$x^2 = 3 - 8z + 8k^2, \qquad (*)$$

amiből az következik, hogy x^2 –et 8 – cal elosztva 3 maradékot kapunk, ami pedig lehetetlen, ugyanis (*) egyenlet alapján könnyen látható, hogy x^2 páratlan, azaz x is páratlan. Legyen $x = 2l + 1,$ $l \in \mathbb{Z}$. Így $x^2 = 4l^2 + 4l + 1$, amelyből már könnyen látszik, hogy 8-cal osztva nem adhat 3 maradékot.

2. eset: y páratlan, legyen $y = 2k + 1,$ $k \in \mathbb{Z}$.

$x^2 = 3 - 8z + 2(4k^2 + 4k + 1) = 3 - 8z + 8k^2 + 8k + 2 = 8(-z + k^2 + k) + 5.$
Tehát x^2 –et 8 – cal elosztva 5 maradékot kapunk, ami szintén lehetetlen, mivel páratlan szám négyzetét 8-cal osztva nem kaphatunk 5-öt maradékul. ✓

II. 2. 1 Megoldhatatlanság bizonyítása kongruencia segítségével

“Ha egy diofantikus egyenlet esetén az egyenlet két oldala valamely alkalmas modulus szerint sohasem lehet kongruens egymással, akkor az egyenlőség biztosan nem teljesülhet (ez fordított irányban nem igaz).” [F-Gy: 7.3.III.]

Példa: [Saját]

Bizonyítsuk be, hogy a $3x^2 - 5y^2 = 5$ *egyenletű hiperbolának nincs egész koordinátájú pontja.*

Indirekt tegyük fel, hogy létezik olyan *x* és *y* egészek, melyek kielégítik az egyenletet.
Ekkor a következő állna fenn:

$$3x^2 - 5y^2 \equiv \;\; 5 \quad (mod\ 3)$$
$$-5y^2 \equiv \;\; 5 \quad (mod\ 3)$$
$$y^2 \equiv -1 \quad (mod\ 3)$$
$$y^2 \equiv \;\; 2 \quad (mod\ 3)$$

Ezzel ellentmondásra jutottunk, hiszen négyzetszám 3-mal osztva csak 0 vagy 1 maradékot adhat, tehát semmilyen egész y-ra nem teljesülhet a $y^2 \equiv 2 \pmod 3$ kongruencia.
Ezzel a feladat állítását bebizonyítottuk.

$\boxed{\text{II. 2. 1/1. Feladat}}$ [F-Gy: 7.3.13/d feladat]

Oldjuk meg a következő diofantikus egyenletet:

$$x^2 - 230y^2 = 7z^2$$

Az egyenletnek megoldása az $x = y = z = 0$. Megmutatjuk, hogy más megoldás nincs.

Indirekt tegyük fel, hogy létezik olyan megoldás, ahol x, y, z nem mindegyike 0.
Ekkor feltehetjük azt is, hogy $(x, y, z) = 1$. Ugyanis ha $(x, y, z) = d > 1$, akkor az egyenletet d^2-tel elosztva a kapott x, y, z már relatív prímek.

Mivel $x^2 - 230y^2 = 7z^2$, ezért

$$x^2 - 230y^2 \equiv 7z^2 \quad (mod\ 7).$$

Könnyen leellenőrizhető, hogy bármely a egész számra

$$a^2 \equiv 0 \quad (mod\ 7) \qquad ha \quad a = 7k$$

$$a^2 \equiv 1 \quad (mod\ 7) \qquad ha \quad a = 7k \pm 1$$

$$a^2 \equiv 4 \quad (mod\ 7) \qquad ha \quad a = 7k \pm 2$$

$$a^2 \equiv 2 \quad (mod\ 7) \qquad ha \quad a = 7k \pm 3$$

Látható, hogy $7z^2 \equiv 0 \pmod 7$.
Tehát azt kell vizsgálnunk, hogy $x^2 - 230y^2 \equiv 0 \pmod 7$ lehetséges-e.

Elsőként tekintsük azt az esetet, amikor $7|x$ és $7|y$. Legyen $x = 7k,\ y = 7l$.
Ekkor $x^2 - 230y^2 = 49k^2 - 230 \cdot 49l^2 = 49(k^2 - 230l^2) = 7z^2$.
Látható, hogy ekkor szükségképpen fennáll: $49|7z^2$, ami csakis úgy lehetséges, ha $7|z$.
Ez pedig ellentmond a feltevésünknek, miszerint $(x, y, z) = 1$.
Tehát feltehetjük, hogy 7 nem osztója x-nek és y-nak is.

Tekintsük most x^2-et.

- Ha $x = 7k$, akkor $x^2 \equiv 0 \pmod 7$. Ez esetben csak a $230y^2$-et kell vizsgálnunk.
- Ha $7 \nmid x$, akkor $x^2 \equiv 1$ v. 4 v. 2 .

Nézzük most a kongruencia bal oldalának másik tagját, $230y^2$-et.

- Ha $y = 7k$, akkor $y^2 \equiv 0 \pmod 7$. Ez esetben $230y^2 \equiv 0 \pmod 7$.
- Ha $7 \nmid y$, akkor $y^2 \equiv 1$ v. 4 v. 2. Ez esetben $230y^2 \equiv 6$ v. 5 v. $3 \pmod 7$.

Miután végiggondoltuk a lehetséges eseteket, elegendő azt észrevenni, hogy x^2 és $230y^2$ a lehetséges esetek tekintetében bármivel is kongruens, különbségük, azaz $x^2 - 230y^2$ nem lehet kongruens 0-val modulo 7.

Tehát találtunk egy olyan modulust, mely szerint az adott egyenlet két oldala sohasem lehet kongruens egymással, ezzel bebizonyítottuk, hogy az egyenletnek $x = y = z = 0$ eseten kívül nincs más megoldása.

II. 2. 2 Megoldások keresése más számok körében

$\boxed{\text{II. 2. 2/1. Feladat}}$ [S: 124]

Bizonyítsuk be, hogy az

$$x(x+1) = 4y(y+1)$$

egyenletnek x-re és y-ra nincs megoldása a természetes számok körében.

Indirekt tegyük fel, hogy x és y természetes számok és kielégítik az

$$x(x+1) = 4y(y+1)$$

egyenletet.

Ekkor
$$x(x+1) - 4y(y+1) = 0 \qquad (*)$$
lenne, és a következő adódna:
$$3 = [2(2y+1)]^2 - (2x+1)^2 = (4y - 2x + 1)(4y + 2x + 3),$$
mivel

$$[2(2y+1)]^2 - (2x+1)^2 =$$

$$= 16y^2 + 16y + 4 - 4x^2 - 4x - 1 =$$

$$= 4 \cdot [4y(y+1) - x(x+1)] + 3 =$$

$$= 4 \cdot 0 + 3 = 3$$

/(*) miatt/

Tehát
$$3 = [2(2y+1)]^2 - (2x+1)^2 .$$

Mivel pedig

$$[2(2y+1)^2]-(2x+1)^2=[2(2y+1)+(2x+1)]\cdot[2(2y+1)-(2x+1)]=$$

$$=(4y+2x+3)\cdot(4y-2x+1)\ ,$$

így $$3=(4y+2x+3)\cdot(4y-2x+1)\ .$$

Ebből az következik, hogy $4y+2x+3\mid 3$,

ez pedig ellentmondás, mivel $4y+2x+3>3,$ mert $x,y\geq 1$ egész számok. ✓

Bizonyítsuk be, hogy a pozitív racionális számok között viszont végtelen sok megoldása van az

$$x(x+1)=4y(y+1)$$

egyenletnek!

Ha $n>1$ természetes szám, akkor

$$x=\frac{3^n-3^{1-n}-2}{4}\quad,\quad y=\frac{3^n+3^{1-n}-4}{8}$$

kielégíti az $x(x+1)=4y(y+1)$ egyenletet.

Ellenőrizzük le: tekintsük az egyenlet bal oldalát, helyettesítsünk be:

$$x(x+1)=\frac{3^n-3^{1-n}-2}{4}\cdot\frac{3^n-3^{1-n}+2}{4}=\frac{3^{2n}-3^{2-2n}-10}{16}$$

Nézzük most az egyenlet jobb oldalát, ide is helyettesítsünk be:

$$4y(y+1)=4\cdot\frac{3^n+3^{1-n}-4}{8}\cdot\frac{3^n+3^{1-n}+4}{8}=\frac{3^{2n}-3^{2-2n}-10}{16}$$

Például ha $n=2$, akkor:

$$x=\frac{3^2-3^{1-2}-2}{4}=\frac{5}{3}\quad,\quad y=\frac{3^2+3^{1-2}-4}{8}=\frac{2}{3}$$

Egyenletünknek tehát végtelen sok $x,\ y$ megoldása van a pozitív racionális számok körében.✓

$\boxed{\text{II. 2. 2/2. Feladat}}$ [S: 132]

Bizonyítsuk be Eulernek azt a tételét, mely szerint a

$$4xy-x-y=z^2$$

egyenletnek nincs x, y, z pozitív egész megoldása.

Indirekt tegyük fel, hogy *x, y, z* természetes számok kielégítik a

$$4xy - x - y = z^2$$

egyenletet, melyet a következőképpen alakítunk:

$$16xy - 4x - 4y = 4z^2$$

$$(4x-1)(4y-1) - 1 = (2z)^2$$

$$(4x-1)(4y-1) = (2z)^2 + 1 \qquad (*)$$

Mivel $x \geq 1$, így $4x - 1 \geq 3$.
Mivel $4x - 1$ alakú természetes számnak van $4k - 1$ alakú p prímosztója (indirekt feltevéssel könnyen belátható), így $\boxed{(2z)^2 \equiv -1 \pmod p}$.

Most egy ismert tételt fogunk felhasználni a feladat megoldásának folytatásához.

Tétel: A „kis" Fermat-tétel egyik alakja

Ha p prím, és $(a, p) = 1$, akkor $a^{p-1} \equiv 1 \pmod p$.

Megjegyzés: egy p prím esetén az $(a, p) = 1$, a $p \nmid a$ és az $a \not\equiv 0 \pmod p$ feltételek ekvivalensek. ◆

Alkalmazzuk a tételt:
Indirekt tegyük fel, hogy $p \mid 2z$.
Ebből következik: $p \mid (2z)^2 \Rightarrow p \nmid (2z)^2 + 1$. Ez ellentmondás, tehát $p \nmid 2z$.
A „kis" Fermat-tétel szerint p -re és $2z$ -re a következőt kellene kapnunk:

$$(2z)^{p-1} \equiv 1 \pmod p$$

Itt azonban

$$(2z)^{p-1} = (2z)^{4k-2} = (2z)^{2(2k-1)} \equiv -1 \pmod p.$$

Így ellentmondásra jutottunk, tehát *x, y, z* természetes számok nem elégítik ki az adott egyenletet. ✓

Bizonyítsuk be, hogy a

$$4xy - x - y = z^2$$

egyenletnek a negatív egész számok körében viszont végtelen sok megoldása van.

n legyen tetszőleges természetes szám.
Legyen $x = -1, \quad y = -5n^2 - 2n, \quad z = -5n - 1$.
Az x, y és z számok kielégítik a $4xy - x - y = z^2$ egyenletet.

(Ellenőrzés: behelyettesítés után az egyenlet mindkét oldala a következő alakra hozható: $25n^2 + 10n + 1$.)

Tehát végtelen sok negatív egész megoldása van az egyenletnek. ✓

II. 3 Legfeljebb véges sok megoldás van

II. 3. 1 “Négyzetszámok összege = n” –típus

Tekintsük most az

$$x_1{}^2 + x_2{}^2 \ldots + x_k{}^2 = n$$

típusú diofantikus egyenleteket.
Könnyen látható, hogy ha az ilyen típusú egyenletnek van megoldása, akkor csak véges sok megoldása lehet, hiszen biztosan igaz, hogy $|x_i| \leq \sqrt{n}$.
A IV – V. fejezetben néhány speciális eset külön is megvizsgálásra kerül, az általános feladat $k = 2$, 3 és 4 esetét vizsgáljuk majd részletesebben is.

Példa: [Saját]

Oldjuk meg az $x^2 + y^4 = 10$ *diofantikus egyenletet.*

Tudjuk, hogy $|y| \leq \sqrt[4]{10}$, tehát $|y| = 0$ vagy $|y| = 1$ lenne lehetséges.
Azonban ha $|y| = 0$, akkor $x^2 = 10$ lenne, ennek pedig nincs egész megoldása.
Ha $|y| = 1$, akkor $x^2 = 9$, tehát $|x| = 3$.
Az adott diofantikus egyenletet tehát a következő számpárok elégítik ki: (3; 1), (-3; 1), (3; -1), (-3; -1).

$\boxed{\text{II. 3. 1/1. Feladat}}$ [Saját]

Bizonyítsuk be, hogy az $x^6 + y^2 = 3$ *diofantikus egyenletnek nincs megoldása az egész számok körében.*

Tudjuk, hogy $|x| \leq \sqrt[6]{3}$, tehát csak $|x| = 1$ lehetne megoldás. Ekkor $y^2 = 2$ lenne, viszont ennek az egyenletnek nincs egész y megoldása.
Tehát az adott diofantikus egyenletnek nincs egész megoldása. ✓

II. 3. 2 “Szorzat = n” –típus

Az ilyen típusú diofantikus egyenleteknél az egyenlőség egyik oldalán egy $n \neq 0$ egész szám, a másik oldalán egy szorzat áll.

Példa: [Saját]

Oldjuk meg az $(x-3)(y-4) = 7$ *diofantikus egyenletet.*

Tudjuk, hogy 7-et csak a következő alakokban állíthatjuk elő szorzatként:

$$7 = 1 \cdot 7 = 7 \cdot 1 = (-1) \cdot (-7) = (-7) \cdot (-1).$$

Tehát 4 esetet különíthetünk el aszerint, hogy $x-3$ -nak és $y-4$ -nek választjuk ezeket a tényezőket:

1. eset: $x-3=\ \ 1,\quad y-4=\ \ 7 \quad\Leftrightarrow\quad x=\ \ 4,\quad y=\ 11$
2. eset: $x-3=\ \ 7,\quad y-4=\ \ 1 \quad\Leftrightarrow\quad x=\ 10,\quad y=\ \ 5$
3. eset: $x-3=-1,\quad y-4=-7 \quad\Leftrightarrow\quad x=\ \ 2,\quad y=-3$
4. eset: $x-3=-7,\quad y-4=-1 \quad\Leftrightarrow\quad x=-4,\quad y=\ \ 3$

Tehát az egyenletet az alábbi számpárok elégítik ki: $(4;11),\ (10;5),\ (2;\ -3),\ (-4;3).$

Ugyanilyen módon oldható meg a következő példa is:

Oldjuk meg az $(x-2)(y-7)(z-5)=10$ *diofantikus egyenletet.*

(Megoldás nélkül.)

$\boxed{\text{II. 3. 2/1. Feladat}}$ [Saját]

Oldjuk meg az $x^2-y^2=11$ *diofantikus egyenletet.*

Alakítsuk szorzattá az egyenlet bal oldalát: $(x+y)(x-y)=11.$
11 a következő alakokban áll elő szorzatként: $11=11\cdot 1=1\cdot 11=(-11)\cdot(-1)=(-1)\cdot(-11).$
Próbálgatással is könnyen megkaphatjuk az egyenletet kielégítő számpárokat:
$(6;\ 5),\ \ (6;\ -5),\ \ (-6;\ -5),\ \ (-6;5).$

Most azt a problémát vizsgáljuk meg, hogy mely pozitív egészek állnak elő és hányféleképpen két négyzetszám különbségeként.

II. 3. 1 Tétel:

Tekintsük az $x^2-y^2=n$ diofantikus egyenletet, ahol n rögzített pozitív egész.

(i) Az egyenlet akkor és csak akkor oldható meg, ha $n\not\equiv 2 \pmod 4$.

(ii) A megoldásszám $2d(n)$, ha n páratlan, és $2d\left(\frac{n}{4}\right)$, ha $4\mid n$ (ahol $d(k)$ a k pozitív osztóinak száma). ◆

Az (i) bizonyítása:

"Az $(x+y)(x-y)=n$ egyenlőség pontosan akkor teljesül, ha $x+y$ és $x-y$ az n két komplementer osztója, azaz

$$x+y=d_1,\qquad x-y=d_2,\qquad \text{ahol}\qquad d_1d_2=n. \tag{1}$$

Az (1) egyenletrendszert megoldva

$$x=\frac{d_1+d_2}{2},\qquad y=\frac{d_1-d_2}{2}$$

adódik. Itt x-re és y-ra pontosan akkor kapunk egész értéket, ha d_1 és d_2 azonos paritású. Ennek megfelelően az $x^2 - y^2 = n$ diofantikus egyenlet akkor és csak akkor oldható meg, ha az n felírható két azonos paritású osztója szorzataként. " [F-Gy]

- 1. eset: n páratlan
  Ekkor n minden osztója páratlan, tehát minden osztópár megfelel.
- 2. eset: $4 \mid n$
  Ekkor azok az osztópárok felelnek meg, melyekben mindkét osztó páros szám.
- 3. eset: n páros, de nem osztható 4-gyel
  Ebben az esetben n nem írható fel két azonos paritású osztója szorzataként, hiszen két páratlan szám szorzata páratlan, két páros szám szorzata pedig osztható 4-gyel.
  Tehát az egyenlet nem oldható meg, ha $n \equiv 2 \pmod 4$. ■

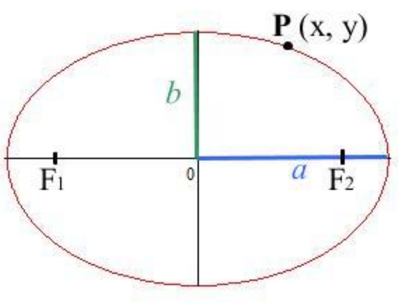
III. Geometria és diofantikus egyenletek

Az eddigiekben tehát megismertünk néhány nevezetes diofantikus egyenletet, láttunk példát megoldási módszerekre. Nézzünk most néhány geometriával kapcsolatos feladatot, ezzel is igazolva, hogy diofantikus egyenletekkel számos témakörben találkozhatunk.
Eddig a pitagoraszi számhármasok fejezeténél láttunk geometriával – azon belül is a derékszögű háromszögekkel kapcsolatos feladatokat.
Tekintsük most az *ellipszist* és *kört* és az euklideszi síkon, majd a *gömb*öt euklideszi térben.

III.1 Ellipszis és kör az euklideszi síkon

Két-négyzetszám-tétel

Az ellipszis:



Adott a síkon: $\mathrm{F}_1,\ \mathrm{F}_2$ fókuszok ($\mathrm{F}_1 \neq \mathrm{F}_2$)
$2a \in \mathbb{R}$ $(2a > d(\mathrm{F}_1,\ \mathrm{F}_2))$

Az $\mathrm{F}_1,\ \mathrm{F}_2$ fókuszú, $2a$ nagytengelyű ellipszis:

$$\{\mathrm{P} \in \mathbb{R}^2:\quad d(P,\mathrm{F}_1) + d(P,\mathrm{F}_2) = 2a\}$$

ponthalmaz.

Az ellipszis kanonikus helyzetű a koordinátarendszerhez képest, ha a koordinátatengelyek a szimmetria tengelyek, és a fókuszok az *x*-tengelyen vannak.

A kanonikus helyzetű ellipszis egyenlete:

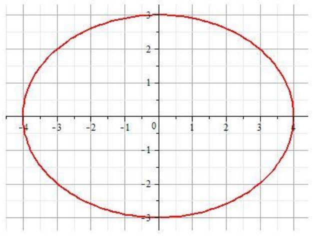
$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$$

$\boxed{\text{III. 1/1. Feladat}}$ [Saját]

Hány egész koordinátájú pont van az

$$\frac{x^2}{16} + \frac{y^2}{9} = 1$$

egyenletű ellipszisen?



Az egyenletből leolvasható, hogy $a=4$ és $b=3$,

azaz az ellipszist alkotó pontok koordinátáiról a következőt tudjuk:

$$|x| \leq 4, \qquad |y| \leq 3.$$

Olyan pontokat keresünk, melyek mindkét koordinátája egész szám. Elég tehát az egyik koordinátát az adott korlátok között végig ellenőrizni.
Előbb rendezzük át az egyenletet:

$$\frac{x^2}{16} + \frac{y^2}{9} = 1$$

$$9x^2 + 16y^2 = 144$$

$$y = \sqrt{\frac{144 - 9x^2}{16}}$$

Most x vegye fel az adott korlátok között lévő egész értékeket. Mely esetekben lesz y is egész?

$|x| = 0 \quad \Longrightarrow \quad |y| = 3$

$|x| = 1 \quad \Longrightarrow \quad y$ nem egész

$|x| = 2 \quad \Longrightarrow \quad y$ nem egész

$|x| = 3 \quad \Longrightarrow \quad y$ nem egész

$|x| = 4 \quad \Longrightarrow \quad y = 0$

Tehát az adott ellipszisnek 4 egész koordinátájú pontja van: (4, 0), (0, 3), (-4, 0), (0, -3).

Megállapíthatjuk, hogy bármely ellipszis 0 vagy véges sok egész koordinátájú pontot tartalmaz, a koordináták korlátossága miatt.

$\boxed{\text{III. 1/2. Feladat}}$ [Saját]

Határozzuk meg az $5x'^2 + 5y'^2 + 6x'y' = 20$ *egyenletű ellipszis egész koordinátájú pontjait!*

Alakítsuk át az egyenletet a következő helyettesítéssel: $x' = x + y, \quad y' = x - y\,.$

$$5(x+y)^2 + 5(x-y)^2 + 6(x+y)(x-y) = 20$$
$$16x^2 + 4y^2 = 20$$
$$4x^2 + y^2 = 5. \qquad (*)$$

Itt $x = \frac{x'+y'}{2}, \qquad y = \frac{x'-y'}{2}.$

- Abban az esetben, ha x' és y' azonos paritású egészek, akkor x és y is egészek, tehát a $4x^2 + y^2 = 5$ egyenletű ellipszis egész koordinátájú pontjaiból meghatározhatjuk az eredeti ellipszis egész koordinátájú pontjait.
  A következő x, y számpárok elégítik ki a (*) egyenletet: (1; 1), (-1; 1), (1; -1), (-1; -1).
  Ezeket az x és y értékeket behelyettesítve az $x = \frac{x'+y'}{2}$, $y = \frac{x'-y'}{2}$ egyenletrendszerbe, a következő x' és y' számpárokat kapjuk:
  (2; 0), (0; -2), (0; 2), (-2; 0).

  Behelyettesítve ezeket a számpárokat az eredeti ellipszis egyenletébe leellenőrizhetjük, hogy valóban az eredeti ellipszis egész koordinátájú pontjait kaptuk.

- Ha viszont x' és y' különböző paritású egészek, akkor x és y olyan törtek, melyek nevezője 2.
  Helyettesítsük a (*) egyenletbe a következőt: $x = \frac{x''}{2}$, $y = \frac{y''}{2}$, ahol x'' és y'' páratlan egészek. (Azért szükséges, hogy páratlanok legyenek, mert csak ebben az esetben igaz az, hogy x' és y' különböző paritásúak, azaz csak ebben az esetben kapunk az előzőektől eltérő megoldásokat.)
  Az újabb helyettesítéssel tehát a következő egyenletet kapjuk: $4x''^2 + y''^2 = 20$,
  melyet a következő x'', y'' számpárok elégítenek ki: (2; 2), (2; -2), (-2; 2), (-2; -2).
  Nem szerepel közöttük páratlan koordináta, tehát ezeket visszavezetve x'-re és y'-re, nem kapunk új megoldásokat.

Tehát az eredeti ellipszis összes egész koordinátájú pontjai a következők:

(2; 0), (0; -2), (0; 2), (-2; 0).

Az ellipszis egyenlete a szokásos, origó középpontú **köregyenlet**té válik, ha $a = b = r$:

$$\boxed{\boxed{x^2 + y^2 = r^2}}$$

Keressünk most körökön egész koordinátájú pontokat.
Gondoljunk bele, hogy milyen r esetén tartalmaz a kör egész koordinátájú pontokat.

- 1. eset: $r \notin \mathbb{Z}$ $r^2 \notin \mathbb{Z}$

  Ha $x \in \mathbb{Z}$ és $y \in \mathbb{Z}$, akkor $x^2 + y^2 \in \mathbb{Z}$.
  Így azonban $x^2 + y^2 = r^2$ nem lehet igaz.
  Ebben az esetben tehát a kör nem tartalmaz egész koordinátájú pontot.

- 2. eset: $r \notin \mathbb{Z}$, $r^2 = R \in \mathbb{Z}$

  Ekkor az $\boxed{x^2 + y^2 = R}$ egyenletnek keressük az x, y megoldásait.

- 3. eset: $r \in \mathbb{Z}$
  $x^2 + y^2 = r^2$
  Ha $x = 0$, akkor $y = \pm r$. Ha $y = 0$, akkor $x = \pm r$.
  Ha x sem és y sem 0, akkor elég az $x > 0$, $y > 0$ esetre szorítkozni a megoldások vizsgálatánál, hiszen a többi ebből könnyen megkapható előjelezéssel. Ekkor x, y és z pitagoraszi számhármast alkotnak.
  Tudjuk, hogy ekkor az egyenletnek az $(x, y, r) = 1$ feltételt kielégítő megoldásait a következő képlet szolgáltatja:

  $$x = 2mn, \qquad y = m^2 - n^2, \qquad r = m^2 + n^2,$$

  ahol az m és n paraméterek tetszőleges olyan pozitív egészek, amelyekre
  m és n különböző paritású, $m > n$ és $(m, n) = 1$.
  Az r –rel kapcsolatban tehát a következőt tudjuk: $\boxed{r = m^2 + n^2}$

A keretezett egyenletekben az a közös, hogy mindkettőben két négyzetszám összege szerepel, azaz olyan számok tulajdonságaira vagyunk kíváncsiak, amelyek felírhatók két négyzetszám összegeként.

III.1 Tétel: Két-négyzetszám-tétel:

Legyen n pozitív egész kanonikus alakja

$$n = 2^{\alpha} p_1^{\beta_1} \dots p_r^{\beta_r} q_1^{\gamma_1} \dots q_s^{\gamma_s},$$

ahol a p_μ prímek $4k + 1$, a q_ν prímek $4k - 1$ alakúak, és a szereplő α, β_μ, γ_ν kitevők nemnegatív egészek.

Az

$$x^2 + y^2 = n$$

diofantikus egyenlet akkor és csak akkor oldható meg, ha minden γ_ν páros, és ebben az esetben a megoldásszám

$$4 \prod_{\mu=1}^{r} (\beta_\mu + 1).$$

◆

Itt a csak az előjelben eltérő megoldásokat is külön megoldásnak tekintjük.

Példa: [Saját]

Oldjuk meg az

$$x^2 + y^2 = 2205$$

egyenletet!

A 2205 kanonikus alakja $3^2 \cdot 5 \cdot 7^2$.
Itt a 3 és a 7 $4k-1$ alakú prímek. Ezek kitevője páros, tehát van megoldás.
A megoldásszám a $4k+1$ alakú prím, azaz az 5 kitevőjéből 4(1+1)=8.

A megoldások: $2205 = (\pm 21)^2 + (\pm 42)^2 = (\pm 42)^2 + (\pm 21)^2$.

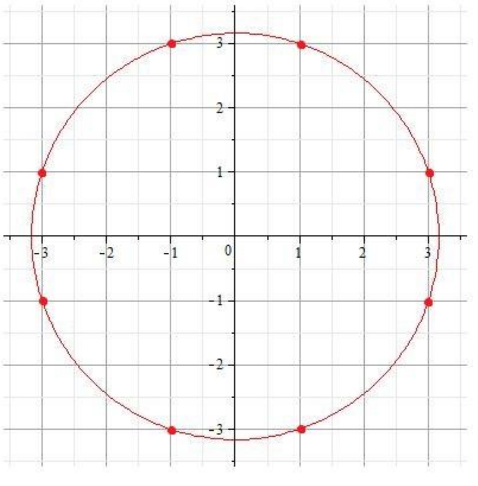
$\boxed{\text{III. } 1/3. \text{ Feladat}}$ [Saját]

Van-e egész koordinátájú pontja az origó középpontú, $\sqrt{10}$ sugarú körnek?
Ha igen, mennyi? Melyek ezek a pontok?

Az $x^2 + y^2 = 10$ diofantikus egyenlet x, y megoldásait keressük.
A 10 kanonikus alakja $2 \cdot 5$. Itt a $4k-1$ alakú prímek kitevője 0, azaz páros, így van megoldása az egyenletnek, van egész koordinátájú pontja a $\sqrt{10}$ körnek.

(Meggondolható, hogy ha van legalább egy egész koordinátájú pont a körön, akkor biztosan van több is. Pontosabban, ha találunk egy egész koordinátájú pontot a körön, mely az egyik koordinátatengelyen helyezkedik el (azaz az egyik koordinátája 0, pl. (3; 0)), akkor biztosan van rajta kívül még 3 egész koordinátájú pont, melyek mindegyike valamelyik koordinátatengely pontja (az előző példához kapcsolódva: (0; 3), (-3; 0), (-3; -3)). Ha olyan egész koordinátájú pontot találunk, mely nem illeszkedik egyik koordinátatengelyre sem (azaz egyik koordinátája sem 0), akkor biztosan van rajta kívül még 7 egész koordinátájú pont. Pl. ha a (3, 4) pont illeszkedik a körre, akkor a (-3; 4), (-3; -4), (3; -4), (4; 3), (-4; 3), (-4; -3), (4; -3) pontok is biztosan illeszkednek.)

A megoldásszám az 5 kitevőjéből 4(1+1)=8.



Könnyen rájöhetünk, hogy a megoldások a következők:

$$10 = (\pm 1)^2 + (\pm 3)^2 = (\pm 3)^2 + (\pm 1)^2.$$

Tehát a $\sqrt{10}$ sugarú kör egész koordinátájú pontjai:

(-1; 3), (-1; -3), (1; 3), (1; -3),
(-3; 1), (-3; -1), (3; 1), (3; -1).

III.2 Gömb az euklideszi térben

Három-négyzetszám-tétel

Ha a sík helyett térben kezdünk el gondolkodni, és az origó középpontú gömb felszínén keresünk olyan pontokat, melyek mindhárom koordinátája egész szám, akkor a következő egyenlet megoldásaira vagyunk kíváncsiak:

$$x^2 + y^2 + z^2 = r^2 ,$$

ahol r a gömb sugara és $r^2 \in \mathbb{Z}$.
Annak eldöntésében, hogy milyen r esetén lehet az általa meghatározott gömbnek egész koordinátájú pontja, azaz, hogy mely egész számok állnak elő három négyzetszám összegeként, a következő tétel lesz segítségünkre.

III. 2 Tétel: Három-négyzetszám-tétel:

Az n pozitív egész akkor és csak akkor **nem** áll elő három négyzetszám összegeként, ha

$$n = 4^k(8m + 7) \qquad (*)$$

alakú. ◆

Bizonyítás:

Az állításnak csak azt a részét igazoljuk, hogy a (*)-beli számok nem állnak elő három négyzetszám összegeként.

A k szerinti teljes indukcióval bizonyítunk.
A k =0 esetben azt kell megmutatni, hogy a $8m + 7$ alakú számok nem írhatók fel három négyzetszám összegeként. Ez abból következik, hogy egy négyzetszám 0, 1 vagy 4 maradékot ad 8-cal osztva, és három ilyen maradék összegeként sohasem kaphatunk 7 maradékot.
Tegyük most fel, hogy az állítás valamely k-ra igaz, és lássuk be, hogy ekkor $k + 1$ -re is teljesül. Indirekt feltesszük, hogy léteznek olyan a, b és c egész számok, amelyekre

$$4^{k+1}(8m + 7) = a^2 + b^2 + c^2 . \qquad (1)$$

Az (1) bal oldala osztható 4-gyel. Egy négyzetszám 4-gyel osztva 0-t vagy 1-et ad maradékul, attól függően, hogy páros, illetve páratlan számot emeltünk négyzetre. Ezért a jobb oldal csak csak úgy lehet osztható 4-gyel, ha a, b és c mindegyike páros, tehát $\frac{a}{2}, \frac{b}{2}$ és $\frac{c}{2}$ egész számok.
Így (1) –et 4-gyel elosztva

$$4^k(8m + 7) = \left(\frac{a}{2}\right)^2 + \left(\frac{b}{2}\right)^2 + \left(\frac{c}{2}\right)^2$$

adódik, ami ellentmond az indukciós feltevésnek. ■

$\boxed{\text{III. 2/1. Feladat}}$ [Saját]

Hány olyan legfeljebb 10 sugarú, origó középpontú gömb van az euklideszi térben, melynek nincs egész koordinátájú pontja és sugara egy egész számnak a négyzetgyöke?

Legyen $r^2 = R \in \mathbb{Z}$, a feladat szövege alapján $R \leq 100$.
Arra vagyunk tehát kíváncsiak, hogy az $x^2 + y^2 + z^2 = R$ egyenletnek milyen R –ekre nincs x, y, z megoldása. A három-négyzetszám-tétel alapján keressük meg ezeket az R-eket, azaz legyen $R = 4^k(8m + 7)$ alakú.
Először legyen $k = 0$, tehát keressük a 0-tól nagyobb, 100-tól nem nagyobb, $8m + 7$ -alakú számokat. Ezek a következők:
7, 15, 23, 31, 39, 47, 55, 63, 71, 79, 87, 95.
Most legyen $k = 1$, tehát az előbb megtalált $8m + 7$ –alakú számokat szorozzuk meg 4-gyel, és válasszuk ki azokat, melyek megfelelnek annak a feltételnek, hogy nem nagyobbak 100-nál:
28, 60, 92.
$k = 2$ -re már nincs olyan R, amely ne lenne nagyobb 100-nál.

Tehát a $\sqrt{7}, \sqrt{15}, \sqrt{23}, \sqrt{28}, \sqrt{31}, \sqrt{39}, \sqrt{47}, \sqrt{55}, \sqrt{60}, \sqrt{63}, \sqrt{71}, \sqrt{79}, \sqrt{87}, \sqrt{92}, \sqrt{95}$ sugarú origó középpontú gömböknek nincs egész koordinátájú pontja, tehát a válasz 15.

IV. Waring-problémakör

“A négyzetek után a magasabb hatványok összegeként történő előállítással foglalkozunk.
Ebben a pontban k végig 1-nél nagyobb pozitív egészt jelöl, és k-adik hatványon *nemnegatív* egész számok k-adik hatványát értjük.

Waring 1770-ben azt állította, hogy “minden szám felírható 4 négyzetszám, 9 köbszám, 19 negyedik hatvány stb. összegeként”. A nagyvonalúan odavetett “stb.” szócska két súlyos problémát is takar. Egyrészt a 4, 9, 19 számokról nemigen látszik valami jól folytatható szabályszerűség, másrészt az sem világos, hogy ez a számsor folytatható-e a végtelenségig. Ez utóbbihoz a következőt kell megmutatni:

Bármely k-hoz létezik olyan, csak k-tól függő r, hogy *minden* pozitív egész felírható r darab k-adik hatvány összegeként.
Ezt az állítást először Hilbert igazolta 1909-ben.

Ma már tudjuk, hogyan folytatódik a Waring-féle számsor. […]

Mivel bármely k-adik hatványok összegeként történő előállítását kiegészíthetjük tetszőleges számú 0^k taggal, ezért a *legkisebb* olyan darabszámot akarjuk meghatározni, hogy annyi k-adik hatvány már minden pozitív egész előállításához elegendő legyen.” [F-Gy.: 7.6.]

IV. 1 Definíció:

Legyen $k > 1$. Ekkor $g(k)$ a *legkisebb* olyan r, hogy minden pozitív egész felírható r darab nemnegatív egész szám k-adik hatványának összegeként. ◆

Példa: [F-Gy]

$g(2)=4$.

Az állítás belátásához ismernünk kell a következő tételt:

IV. 2 Tétel: Négy-négyzetszám-tétel:

Minden pozitív egész felírható négy négyzetszám összegeként. ◆

(Bizonyítás nélkül.)

Tehát a négy-négyzetszám-tétel szerint minden pozitív egész négy négyzetszám összege, valamint van olyan szám, amelynek az előállításához 3 négyzetszám nem elegendő (pl. a 7), ezzel bebizonyítottuk, hogy $g(2)=4$.

IV. 3 Tétel:

$$g(k) \geq 2^k + \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 2\,. \;\blacklozenge \tag{1}$$

A $g(k)$-ra vonatkozó legfontosabb eredmény az, hogy (1)-ben általában egyenlőség teljesül: csak véges sok olyan k létezhet, amelyre $g(k)$ nagyobb az (1) jobb oldalán megadott értéknél, sőt csaknem biztosra vehető, hogy minden k-ra

$$g(k) = 2^k + \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 2\,.$$

Ennek megfelelően (1) jobb oldala jelenti a Waring-féle számsor folytatását (speciálisan a $k = 2$, 3 és 4 esetben rendre a 4, 9, 19 értékeket kapjuk.

Érdemes azt is megvizsgálni, hogy minimálisan hány k-adik hatvány szükséges minden *elég* nagy n felírásához:

IV. 4 Definíció:

Legyen $k > 1$. Ekkor $G(k)$ a *legkisebb* olyan s, hogy minden *elég nagy* pozitív egész felírható s darab nemnegatív egész szám k-adik hatványának összegeként. ◆

Példa: [F-Gy]

$G(2) = 4$.

Ugyanis egyrészt $G(2) \leq g(2) = 4$, másrészt a három-négyzetszám-tétel szerint *végtelen sok* olyan szám létezik, amelynek az előállításához három négyzetszám nem elegendő.

Az alább táblázatban eredményeket láthatunk $g(k)$-ra és $G(k)$-ra vonatkozóan, néhány kis k esetén. [F-Gy]

k	2	3	4	5	6	7	8
$g(k)$	4	9	19	37	73	143	279
$G(k)$	4	4 - 7	16	6 - 18	9 - 28	8 - 45	32 - 57

Látható, hogy már kis k esetén is igen nagy a bizonytalanság a $G(k)$ pontos értékét illetően. A $G(k)$ pontos értékét eddig csak a $k = 2$ és 4 esetekben sikerült meghatározni. Az viszont kiderült, hogy $G(k)$ értéke jóval kisebb $g(k)$-nál (pl. $G(k) < 6k \log k$).

Az alábbiakban alsó becslést adunk $G(k)$-ra (bizonyítás nélkül).

IV. 5 Tétel:

Minden $k > 1$ esetén $G(k) \geq k+1$. ◆

IV. 6 Tétel:

$G(6) \geq 9$. ◆

Ha a számokat k-adik hatványok előjeles összegeként állítjuk elő, akkor általában $g(k)$-nál, illetve $G(k)$-nál kevesebb számú tag is elegendő.

IV. 7 "Definíció":

Legyen $k > 1$. Ekkor $g^*(k)$ a *legkisebb* olyan r, hogy minden pozitív egész felírható r darab nemnegatív egész szám k-adik hatványának előjeles összegeként.

$\boxed{\text{IV./1. Feladat}}$ [Saját]

Bizonyítsuk be, hogy $g^*(2)=3$.

Tudjuk, hogy $g^*(2)>2$, hiszen a két-négyzetszám-tétel alapján tudjuk, hogy nem minden pozitív egész szám áll elő két négyzetszám összegeként, a **II. 3. 1 Tétel** alapján pedig tudjuk, hogy két négyzetszám különbségeként sem írható fel minden pozitív egész szám.

Most bebizonyítjuk, hogy 3 négyzetszám elég ahhoz, hogy minden pozitív egészet felírjunk a segítségükkel.
A három-négyzetszám-tétel alapján tudjuk, hogy csak a $4^k(8m+7)$ alakú számok nem írhatók fel három négyzetszám összegeként.
Tekintsük tehát a $4^k(8m+7)$ alakú számokat.

- 1. eset: $k = 0$
  Ekkor $4^k(8m+7) = 8m+7$. Tudjuk, hogy $8m+7 \equiv 3 \pmod 4$.
- 2. eset: $k > 0$
  Ekkor $4^k(8m+7) \equiv 0 \pmod 4$.

Tehát az adott számok egyik esetben sem kongruensek 2-vel modulo 4, így a **II. 3. 1 Tétel** szerint felírhatók két négyzetszám különbségeként.✓

Irodalomjegyzék

[F-Gy] Freud Róbert - Gyarmati Edit: *Számelmélet*

Nemzeti Tankönyvkiadó, Budapest, 2000

[S] Waclaw Sierpinski: *200 feladat az elemi számelméletből*

(Középiskolai szakköri füzetek), Tankönyvkiadó, Budapest, 1968