

# Diofantoszi egyenletek

**Diofantoszi egyenletr**l akkor beszélünk, ha az egyenletben szerepl együtthatók egész számok, és a megoldásokat is az egész számok körében keressük. Ha az egyenletben szerepl ismeretlenek első hatványon szerepelnek, akkor az egyenletet **lineárisnak** nevezzük. Ebben a fejezetben olyan lineáris diofantoszi egyenletekkel foglalkozunk, amelyekben az ismeretlenek száma kettő. Ezek a egyenletek tehát **kétismeretlenesek**.

Egy a diofantoszi egyenletek megoldására szolgáló algebrai módszer ismertetése után kidolgozzuk az euklideszi algoritmus kiterjesztett változatát, ami nemcsak meghatározza két egész szám legnagyobb közös osztóját, hanem megadja azokat az együtthatókat is, amelyekkel a legnagyobb közös osztót a két egész lineáris kombinációjaként állíthatjuk elő. A kiterjesztett euklideszi algoritmus adja kezünkbe az általános módszert a lineáris két ismeretlenes diofantoszi egyenletek megoldásához.

## Algebrai megközelítés

Tekintsük elsőként a

$$2 \cdot x + y = 3$$

egyenletet. Keressük azokat az  $x$  és  $y$  egész számokat, amelyeket az egyenletbe helyettesítve azonossághoz jutunk. Az ilyen  $[x, y]$  párokról azt mondjuk, hogy az **egyenlet megoldásai**. Jelen esetben nem lesz nehéz dolgunk az  $x$  és  $y$  meghatározásával. Fejezzük ki  $y$ -t az egyenletből

$$y = 3 - 2 \cdot x$$

és vegyük észre, hogy az  $x$  változónak adott tetszőleges egész érték meghatározza az  $y$  változó egy szintén egész értékét. Például  $x = 0$  esetén  $y = 3$ , így azt mondhatjuk, hogy a  $[0, 3]$  pár megoldása egyenletünknek. Ha  $x$ -nek a  $-5$  értéket adjuk, akkor  $y$ -ra  $13$  adódik, tehát a  $[-5, 13]$  pár is megoldása az egyenletnek.

## Példák

Soroljunk fel további megoldásokat

| $x$ | $y = 3 - 2 \cdot x$ | Megoldás :<br>$[x, y]$ | Behelyettesítés     |
|-----|---------------------|------------------------|---------------------|
| 1   | 1                   | $[1, 1]$               | $2 \cdot 1 + 1 = 3$ |
| 2   | -1                  | $[2, -1]$              | $2 \cdot 2 - 1 = 3$ |
| 3   | -3                  | $[3, -3]$              | $2 \cdot 3 - 3 = 3$ |
| 4   | -5                  | $[4, -5]$              | $2 \cdot 4 - 5 = 3$ |

Ezzel az eljárással, mármint azzal, hogy  $x$ -nek tetszőleges értéket adunk, majd kiszámítjuk a neki

megfelel  $y$  értéket, végtelen sok megoldást tudunk előállítani. Mivel  $x$ -nek szabadon adhatunk értékeket, ezért azt **szabad változónak** hívjuk, és általánosságban azt mondjuk, hogy az egyenlet megoldása  $[x = t, y = 3 - 2 \cdot t]$ .

Az elég világos, hogy  $y$ -t nem választhattuk volna szabad változónak, hiszen például az  $y = 0$  értékadás nem határoz meg  $x$ -nek egész értéket. Valóban, ha az egyenletben  $y$  helyére 0-t helyettesítünk, akkor az  $2 \cdot x = 3$  egyenlethez jutunk, olyan egész szám pedig nincs, amelynek a kétszerese 3-mal egyenlő. E tekintetben tehát az egyenlet két változójának szerepe nem felcserélhető. Azt a változót kell kifejeznünk, amelynek együtthatója 1 abszolút érték (ha van ilyen), és a másik változót tekinthetjük szabad változónak. Eddigi megfigyeléseinket az alábbi tételben foglalhatjuk össze.

### ▼ 11.1.1. Tétel

Ha az  $a$  és a  $b$  számok közül valamelyik 1 abszolút érték, akkor az

$$a \cdot x + b \cdot y = c$$

egyenletnek végtelen sok megoldása van.

### Bizonyítás

Tegyük fel, hogy  $|a| = 1$ . Ekkor egyenletünk  $a$  eljelének függvényében

$$x + b \cdot y = c$$

vagy pedig

$$-x + b \cdot y = c$$

alakú. Mindkét esetben úgy járunk el, hogy  $x$ -et kifejezzük,  $y$ -t pedig szabad változónak tekintjük. Legyen tehát  $y = t$ , és ekkor az első esetben a megoldások

$$x = c - b \cdot t, \quad y = t,$$

a másodikban pedig

$$x = b \cdot t - c, \quad y = t.$$

A  $|b| = 1$  eset ugyanígy látható be.

Most térjünk rá az olyan két ismeretlenes egyenletek vizsgálatára, amelyekben mindkét együttható abszolút értéke különbözik 1-től. Példaként vegyünk a

$$2 \cdot x + 7 \cdot y = 3$$

egyenletet, és fejezzük ki az egyenletből  $x$ -et. Azért ezt, mert ennek együtthatója a kisebb abszolút érték. Kapjuk az

$$x = \frac{3 - 7 \cdot y}{2}$$

egyenletet, melyet  $x = \frac{3}{2} - \frac{7}{2} \cdot y$  alakba írva, könnyen támadhat olyan ötletünk, hogy válasszuk szét a két tört egész és tört részét. Ehhez végezzünk el a  $3 = 2 \cdot 1 + 1$  és  $7 = 2 \cdot 3 + 1$  maradékos osztásokat. Behelyettesítés után

$$x = \frac{(2 \cdot 1 + 1) - (2 \cdot 3 + 1) \cdot y}{2} = \frac{(2 \cdot 1 - 2 \cdot 3 \cdot y) + (1 - y)}{2} = (1 - 3 \cdot y) + \frac{1 - y}{2}.$$

Mivel  $x$  egész, valamint a  $1 - 3 \cdot y$  is az, ezért a jobboldali tört sem lehet más, mint egész szám. Azt írhatjuk tehát, hogy valamely  $x_1$  egészre

$$x_1 = \frac{1 - y}{2}.$$

Bevezetve az  $y = y_1$  jelölést, átrendezéssel a

$$2 \cdot x_1 + y_1 = 1$$

egyenlethez jutunk. Ez pedig már egy olyan egyenlet, amelyben az  $y_1$  együtthatójának abszolút értéke 1. Ilyenkor pedig, mint láttuk, nincs más dolgunk, mint  $y_1$ -et kifejezni, a  $x_1$ -et pedig szabad változónak tekinteni. Tehát

$$x_1 = t, \quad \text{és} \quad y_1 = 1 - 2 \cdot t,$$

melyből az  $x$  és  $y$  értéke már az  $y = y_1$  és az  $x = \frac{3 - 7 \cdot y}{2}$  egyenlőségek felhasználásával kiszámítható:

$$y = 1 - 2 \cdot t, \\ x = \frac{3 - 7 \cdot y}{2} = \frac{3 - 7 \cdot (1 - 2 \cdot t)}{2} = \frac{-4 + 14 \cdot t}{2} = -2 + 7 \cdot t.$$

Azt mondhatjuk tehát, hogy kiindulási egyenletünk megoldásai  $[5 - 7 \cdot t, 2 \cdot t - 1]$ , ahol  $t$  tetszőleges egész. Hogy valóban megoldásokkal állunk szemben, arról egyszer behelyettesítéssel könnyen meg is győződhetünk:

$$2 \cdot x + 7 \cdot y = 2 \cdot (-2 + 7 \cdot t) + 7 \cdot (1 - 2 \cdot t) = -4 + 14 \cdot t + 7 - 14 \cdot t = 3.$$

Nézzünk most vissza, és foglaljuk össze, hogy milyen lépésekkel jutottunk el a vizsgált egyenlet megoldásáig. Magát a megoldást az a szerencsés tény véletlen szolgáltatta, hogy a kiindulási egyenletet egy redukciós lépéssel sikerült visszavezetni olyan egyenletre, melyben valamelyik együttható már 1 abszolút érték. De hogy jutottunk ehhez az egyenlethez? Ezt foglalja össze az alábbi táblázat, melynek els három oszlopát felülről lefelé, míg negyedik oszlopát lentől felfelé kell olvasni, ahogy ezt az egyes lépések feltüntetett sorszámai is mutatják.

| A megoldandó egyenlet                                           | A megoldás lépései                                                                 | Új változók               | A megoldások                                                |
|-----------------------------------------------------------------|------------------------------------------------------------------------------------|---------------------------|-------------------------------------------------------------|
| Legyen a megoldandó egyenlet<br>$20 \cdot x + 15 \cdot y = -10$ | 1. Az egyenletben szerepl mindhárom egész szám osztható 5-tel.                     | 2. $x = x_1$<br>$y = y_1$ | 10. $x = x_1 = -2 - 3 \cdot t$<br>$y = y_1 = 2 + 4 \cdot t$ |
| Az új egyenlet<br>$4 \cdot x_1 + 3 \cdot y_1 = -2$              | 3. Mivel $y_1$ együtthatója a kisebb abszolút érték, ezt kifejezzük az egyenletből |                           |                                                             |

|                                                              |                                                                                                                                                                                                                                                          |                                                                               |                                                                                                                                                                                                                                                                   |
|--------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                              | $y_1 = \frac{-2-4 \cdot x_1}{3}.$ <p>5. Válasszuk szét a jobboldali tört egész és törtrészét</p> $y_1 = -x_2 + \frac{-2-x_2}{3}.$ <p>6. A jobboldali tört szükségképpen egész szám ezért alkalmas <math>y_2</math> egészre</p> $y_2 = \frac{-2-x_2}{3}.$ | <p>4. <math>x_1 = x_2</math></p> $y_1 = 1 \mid -2-4 \cdot x_2 = -2-3 \cdot t$ | <p>9. Az <math>x_2</math> és az <math>y_2</math> értéke már ismert (lásd. az alsó cella), így azokat behelyettesítve kapjuk <math>x_1</math>-et és <math>y_1</math>-et</p> $y_1 = \frac{-2-4 \cdot x_2}{3} = \frac{-2-4 \cdot (-2-3 \cdot t)}{3} = 2 + 4 \cdot t$ |
| <p>Az új egyenletet <math>x_2 + 3 \cdot y_2 = -2</math>.</p> | <p>7. Ez az egyenlet már megoldható, hiszen egyik változójának együtthatója 1 abszolút érték. Ezt kifejezzük, a másik változót pedig szabad változónak tekintjük.</p>                                                                                    |                                                                               | <p>8. <math>x_2 = -2-3 \cdot t</math></p> $y_2 = t$                                                                                                                                                                                                               |

## Példák

```
> restart;
```

```
> with(ant):
```

"Az ANT (Algorithmic Number Theory) csomag üdvözlí Önt!"

(1.1.1)

```
> LinDioAlg(2,3,4,cal);
```

Részletek megjelenítése(LinDioAlg):

| Egyenlet          | Új változó                 | Új változó  | $x$            | $y$         |
|-------------------|----------------------------|-------------|----------------|-------------|
| $2x + 3y = 4$     | $x = x_1$                  | $y = y_1$   | $x = 2 + 3t$   | $y = -2t$   |
| $2x_1 + 3y_1 = 4$ | $x_1 = 2 - \frac{3}{2}y_2$ | $y_1 = y_2$ | $x_1 = 2 + 3t$ | $y_1 = -2t$ |
| $2x_2 + y_2 = 0$  |                            |             | $x_2 = t$      | $y_2 = -2t$ |

Eredmény(LinDioAlg):

$$\{x = 2 + 3t, y = -2t\}$$

(1.1.2)

```
> LinDioAlg(20,15,-10,cal);
```

Részletek megjelenítése(LinDioAlg):

| Egyenlet           | Új változó  | Új változó                            | $x$             | $y$            |
|--------------------|-------------|---------------------------------------|-----------------|----------------|
| $20x + 15y = -10$  | $x = x_1$   | $y = y_1$                             | $x = -2 - 3t$   | $y = 2 + 4t$   |
| $4x_1 + 3y_1 = -2$ | $x_1 = x_2$ | $y_1 = -\frac{2}{3} - \frac{4}{3}x_2$ | $x_1 = -2 - 3t$ | $y_1 = 2 + 4t$ |
| $x_2 + 3y_2 = -2$  |             |                                       | $x_2 = -2 - 3t$ | $y_2 = t$      |

Eredmény(LinDioAlg):

$$\{x = -2 - 3t, y = 2 + 4t\}$$

(1.1.3)

### 11.1.2. Tétel

Tegyük fel, hogy az

$$a \cdot x + b \cdot y = c \quad (1)$$

kétismeretlenes diofantoszi egyenletben sem  $a$  sem  $b$  nem 1 abszolút érték. Ekkor megadható olyan

$$a_1 \cdot x_1 + b_1 \cdot y_1 = c_1 \quad (2)$$

linéris diofantoszi egyenlet, amelyre

$$|a_1| < |a| \text{ vagy } |b_1| < |b|.$$

Továbbá a (2) egyenlet minden megoldása egyértelműen meghatározza az (1) egyenlet egy-egy megoldását és (1) minden megoldása eláll ilyen módon.

### Bizonyítás

Az áttekinthetbb formalizmus kedvéért tételezzük fel, hogy az  $a \cdot x + b \cdot y = c$  egyenletben  $1 < a \leq b$ . Osszuk el  $b$ -t és  $c$ -t maradékosan  $a$ -val

$$b = a \cdot q_b + b_1 \quad (0 \leq b_1 < a),$$

$$c = a \cdot q_c + c_1 \quad (0 \leq c_1 < a),$$

ezután fejezzük ki  $x$ -et az  $a \cdot x + b \cdot y = c$  egyenletből és helyettesítsük be  $b$  és  $c$  most kapott kifejezését

$$x = \frac{c - b \cdot y}{a} = \frac{a \cdot q_c + c_1 - (a \cdot q_b + b_1) \cdot y}{a} = \frac{a \cdot (q_c - q_b \cdot y) + (c_1 - b_1 \cdot y)}{a} = q_c - q_b \cdot y + \frac{c_1 - b_1 \cdot y}{a}.$$

Az egyenlőség jobb oldalán lévő tört szükségképpen egész, mivel két egész számnak, nevezetesen  $x$ -nek és  $(q_c - q_b \cdot y)$ -nak a különbsége. Így bevezetve az

$$y = y_1$$

jelölést azt írhatjuk, hogy alkalmas  $x_1$  egész számra

$$x_1 = \frac{c_1 - b_1 \cdot y_1}{a},$$

amiből átrendezéssel kapjuk, hogy

$$a \cdot x_1 + b_1 \cdot y_1 = c_1.$$

Feltételezéseinket figyelembe véve a  $b_1$  együtthatóra a

$$b_1 < a \leq b,$$

becslés adódik, és ezzel a tétel első állítását beláttuk.

Ha  $[x_1, y_1]$  megoldása a második egyenletnek, akkor

$$x = q_c - q_b \cdot y_1 + x_1, \quad y = y_1$$

megoldása az első egyenletnek. Tehát az második egyenlet  $[x_1, y_1]$  megoldása meghatározza az eredeti egyenlet  $[x, y]$  megoldását. Az pedig, hogy az első egyenlet minden megoldását megkapjuk ilyen módon, az az elvégzett redukciós lépés alapján nyilvánvaló.

A most igazolt tétel rendkívül hasznos, mert megadja kulcsot tetszőleges lineáris diofantoszi egyenlet megoldásához. Ugyanis korábban bemutatott példáinkkal ellentétben korántsem biztos, hogy egy redukciós lépéssel sikerül olyan egyenlethez jutnunk, amelyben valamelyik együttható 1 abszolút értékű.

Ám tételünk alapján azt biztosan tudjuk, hogy redukciós lépés eredményeként adódó egyenletben valamelyik együttható abszolút értékben határozottan kisebb a kiindulási egyenlet megfelelő együtthatójánál. Így ha a redukciós lépést újra és újra megismételjük kapott egyenletekre, akkor a keletkező egyenletek együtthatói abszolút értékben egyre kisebbek, így szükségképpen elbb-utóbb olyan egyenlethez kell jutnunk, amelyben már valamelyik együttható abszolút értéke 1. Ezt pedig már könnyen meg tudjuk oldani. Ezután nincs más tennivalónk, mint az utolsó egyenlet megoldásainak birtokában visszafelé haladva egyenként meghatározni a folyamatban résztvevő egyenletek megoldásait, köztük a legelsőét, melynek megoldásait keressük.

Az alábbiakban egy olyan egyenletet oldunk meg, melynek megoldásához két redukciós lépéssel tudunk eljutni.

| A megoldás menete                                                |                                                                                           | Új változók               | A megoldások                           |
|------------------------------------------------------------------|-------------------------------------------------------------------------------------------|---------------------------|----------------------------------------|
| Legyen a megoldandó egyenlet<br>$62 \cdot x + 42 \cdot y = 3540$ | 1. Az egyenletben szerepl mindhárom egész szám osztható 2-tel.                            | 2. $x = x_1$<br>$y = y_1$ | 15. $x = -12 + 21t$<br>$y = 102 - 31t$ |
| Az új egyenlet<br>$31 \cdot x_1 + 21 \cdot y_1 = 1770$           | 3. Mivel $y_1$ együtthatója a kisebb abszolút értékű, $y_1$ -et kifejezzük az egyenletből |                           |                                        |

|                                                         |                                                                                                                                                                                                                                                                                                                                              |                                                                      |                                                             |
|---------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|-------------------------------------------------------------|
|                                                         | $y_1 = \frac{1770 - 31 \cdot x_1}{21}.$ <p>5. Válasszuk szét a jobboldali tört egész és tört részét</p> $y_1 = 84 - x_2 + \frac{6 - 10 \cdot x_2}{21}.$ <p>6. Mivel a jobboldali tört szükségképpen egész szám ezért alkalmas <math>y_2</math> egész számra</p> $y_2 = \frac{6 - 10 \cdot x_2}{21}.$                                         | <p>4. <math>x_1 = x_2</math></p> $y_1 = 1 / 2 (1770 - 31 \cdot x_2)$ | <p>14. <math>x_1 = -12 + 21 t</math></p> $y_1 = 102 - 31 t$ |
| <p>Az új egyenlet</p> $10 \cdot x_2 + 21 \cdot y_2 = 6$ | <p>7. Mivel <math>x_2</math> együtthatója a kisebb abszolút érték, <math>x_2</math>-t kifejezzük az egyenletből</p> $x_2 = \frac{6 - 21 \cdot y_2}{10}.$ <p>9. Válasszuk szét a jobboldali tört egész és tört részét</p> $x_2 = -2 \cdot y_2 + \frac{6 - y_2}{10}.$ <p>10. Alkalmas <math>x_3</math> egészre</p> $x_3 = \frac{6 - y_3}{10}.$ | <p>8. <math>y_2 = y_3</math></p> $x_2 = 1 / 10 (6 - 21 \cdot y_3)$   | <p>13. <math>x_2 = -12 + 21 t</math></p> $y_2 = 6 - 10 t$   |
| <p>Az új egyenlet</p> $10 \cdot x_3 + y_3 = 6.$         | <p>11. Ez az egyenlet már megoldható, hiszen egyik változójának együtthatója 1 abszolút érték. Ezt kifejezzük, a másik változót pedig szabad változónak tekintjük.</p>                                                                                                                                                                       |                                                                      | <p>12. <math>x_3 = t</math></p> $y_3 = 6 - 10 \cdot t$      |

Figyeljük meg az els oszlopban fellép egyenletek együtthatóinak változását, ami jól szemlélteti a 10.1.2 tételben elmondottakat.

## Példák

Az alábbi utasítás outputján szépen nyomon követhetjük a számítási eljárás lépéseit.

```
> LinDioAlg(62,42,3540,cal);
Részletek megjelenítése(LinDioAlg):
[[Egyenlet, Új változó, Új változó, x, y],
```

$$\left[ \begin{array}{l} 62x + 42y = 3540, x = x_1, y = y_1, x = -12 + 21t, y = 102 - 31t \\ 31x_1 + 21y_1 = 1770, x_1 = x_2, y_1 = \frac{590}{7} - \frac{31}{21}x_2, x_1 = -12 + 21t, y_1 = 102 - 31t \\ 10x_2 + 21y_2 = 6, x_2 = \frac{3}{5} - \frac{21}{10}y_3, y_2 = y_3, x_2 = -12 + 21t, y_2 = 6 - 10t \\ 10x_3 + y_3 = 6, x_3 = t, y_3 = 6 - 10t \end{array} \right]$$

Eredmény(LinDioAlg):

$$\{x = -12 + 21t, y = 102 - 31t\}$$

(1.1.4)

## A kiterjesztett euklideszi algoritmus (KEA)

Tekintsük az  $a$  és  $b$  egészeket. Vegyük  $a$ -nak  $b$ -vel való maradékos osztását

$$a = bq + r, (0 \leq r < b)$$

és fejezzük ki az egyenlőségbl a maradékot

$$r = a - b \cdot q = 1 \cdot a + (-q) \cdot b.$$

Mit fejez ki ez az egyenlőség? Azt, hogy az osztás maradékát el tudtuk állítani az osztandó és az osztó egy lineáris kombinációjával, vagyis találtunk olyan egész számokat ( $1$  és  $-q$ ), hogy egyikkel az osztandót ( $a$ -t), másikkal az osztót ( $b$ -t) megszorozva és a két szorzatot összeadva megkapjuk a maradékot.

Az euklideszi algoritmus maradékos osztások sorozata. Ebben a sorozatban minden egyes osztásra érvényes elbbi megjegyzésünk, vagyis, hogy az osztás maradéka eláll az osztandó és az osztó lineáris kombinációjaként. Igen ám, de az euklideszi algoritmus maradékos osztásai között szoros kapcsolat van, nevezetesen az, hogy a minden egyes osztást követően az osztót osztjuk a maradékkal. Ez az észrevétel kapcsolatot teremt az egyes lépésekben elálló lineáris kombinációk együtthatói között.

Példaként határozzuk meg 94 és 28 legnagyobb közös osztóját euklideszi algoritmussal! Írjuk fel a maradékos osztásokat, és minden egyes lépésben fejezzük ki a maradékot az osztandó és az osztó lineáris kombinációjaként.

| EA osztásai            | Maradékot kifejezzük           | Magyarázat                                      |
|------------------------|--------------------------------|-------------------------------------------------|
| $94 = 3 \cdot 28 + 10$ | $10 = 1 \cdot 94 - 3 \cdot 28$ | 10 eláll a 94 és a 28 lineáris kombinációjaként |
| $28 = 2 \cdot 10 + 8$  | $8 = 1 \cdot 28 - 2 \cdot 10$  | 8 eláll a 28 és a 10 lineáris kombinációjaként  |
| $10 = 1 \cdot 8 + 2$   | $2 = 1 \cdot 10 - 1 \cdot 8$   | 2 eláll a 10 és a 8 lineáris                    |



Fordítsuk most figyelmünket a középs oszlopra. Ennek utolsó cellájában a maradék (=2) van kifejezve az utolsó osztás osztandójának (=10) és osztójának (=8) lineáris kombinációjaként. Ám ez a 2 nem más, mint a kiindulási két egész legnagyobb közös osztója. Tehát úgy is fogalmazhatunk, hogy  $\text{lnko}(94, 28)$  eláll az utolsó osztás osztandójának és osztójának lineáris kombinációjaként, egész konkrétan

$$\text{lnko}(94, 28) = 1 \cdot 10 - 1 \cdot 8.$$

És most kihasználjuk azt, hogy az euklideszi algoritmusban az aktuális osztás osztója ez elz lépésben elvégzett osztás maradéka. A középs oszlop második cellájában éppen 8 van kifejezve a 28 és a 10 lineáris kombinációjaként. Ezt a fenti egyenlőségbe helyettesítve

$$\text{lnko}(94, 28) = 1 \cdot 10 - 1 \cdot (1 \cdot 28 - 2 \cdot 10) = -1 \cdot 28 + 3 \cdot 10,$$

ez pedig azt mutatja, hogy a legnagyobb közös osztót el tudtuk állítani a második osztás osztandójának (=28) és osztójának (=10) lineáris kombinációjaként is.

Ha a harmadik osztásról vissza tudunk lépni a másodikra, akkor jó okunk van bizakodni abban, hogy a másodikról is vissza tudunk lépni az elsőre. És valóban nem csalatkozunk reményeinkben, hiszen nincs más dolgunk, mint 10-nek a középs oszlop első cellájában található elállítását az elbb kapott egyenlőségbe helyettesíteni:

$$\text{lnko}(94, 28) = -1 \cdot 28 + 3 \cdot (1 \cdot 94 - 3 \cdot 28) = 3 \cdot 94 - 10 \cdot 28.$$

És ezzel elértük célunkat, nevezetesen azt, hogy 94 és 28 legnagyobb közös osztóját el tudjuk állítani 94 és 28 egy lineáris kombinációjaként. Az itt konkrét számokon bemutatott gondolatmenet általánosan is érvényes. Igaz ugyanis a következ

### ▼ 11.2.1. Tétel

Tetszleges  $a$  és  $b$  egészekhez  $\text{lnko}(a, b)$  elállítható az  $a$  és  $b$  egy lineáris kombinációjaként, vagyis létezik olyan  $x$  és  $y$  egész szám, hogy

$$\text{lnko}(a, b) = x \cdot a + y \cdot b.$$

### Bizonyítás

A bizonyítást elegend nem negatív számokra elvégezni, mert  $\text{lnko}(a, b) = \text{lnko}(|a|, |b|)$ . Az az eset is könnyen kezelhet, amikor  $b = 0$ . Ugyanis ekkor

$$\text{lnko}(a, 0) = a = 1 \cdot a + 0 \cdot 0.$$

Végül ha  $b \mid a$ , akkor

$$\text{lnko}(a, b) = b = 0 \cdot a + 1 \cdot b.$$

Feltehetjük tehát, hogy  $b$  pozitív és nem osztója  $a$ -nak. Ekkor az euklideszi algoritmus legalább két osztásból áll, és az utolsó eltti osztás maradéka, ami egyben az utolsó nem nulla maradék is, nem más, mint a legnagyobb közös osztó. És mint láttuk, a maradékos osztás maradéka kifejezhet az osztandó és az osztó egy lineáris kombinációjával.

Legyen az euklideszi algoritmus  $(i - 1)$ -edik osztása

$$a_{i-1} = b_{i-1} \cdot q_{i-1} + r_{i-1},$$

amiből a maradékot kifejezve

$$r_{i-1} = a_{i-1} - b_{i-1} \cdot q_{i-1}.$$

Az euklideszi algoritmus alapján az  $i$ -edik osztásban az  $(i-1)$ -edik osztás osztóját osztjuk az  $(i-1)$ -edik osztás maradékával. Tehát az  $i$ -edik osztás alakja

$$b_{i-1} = r_{i-1} \cdot q_i + r_i$$

alakú, és tegyük fel, hogy az utolsó eltti osztásra tett észrevételünk teljesül erre az osztásra is. Nevezetesen azt tesszük fel, hogy alkalmas  $x$  és  $y$  egészekre

$$\text{Inko}(a, b) = x \cdot b_{i-1} + y \cdot r_{i-1}.$$

Ebbe az egyenlőségbe az  $r_{i-1}$  elállítást helyettesítve az

$$\text{Inko}(a, b) = x \cdot b_{i-1} + y \cdot (a_{i-1} - b_{i-1} \cdot q_{i-1}) = y \cdot a_{i-1} + (x - y \cdot q_{i-1}) \cdot b_{i-1}.$$

egyenlőséghez jutunk, ami azt fejezi ki, hogy  $\text{Inko}(a, b)$  eláll az  $(i-1)$ -edik osztás osztandójának és osztójának lineáris kombinációjaként is.

Foglaljuk össze a bizonyítás lépéseit. Elsként rámutattunk arra, hogy az euklideszi algoritmus utolsó eltti osztásában szerepl maradék, vagyis a legnagyobb közös osztó, eláll ezen osztás osztandójának és osztójának lineáris kombinációjaként. Majd feltettük, hogy ez a tulajdonság az  $i$ -edik osztásra is teljesül, és megmutattuk, hogy ekkor az  $(i-1)$ -edik osztásra is teljesül.

Mindebből már következik, hogy az euklideszi algoritmus során elvégzett minden osztásra, és így speciálisan a legelsre is igaz, hogy az  $\text{Inko}(a, b)$  eláll az osztandó és az osztó lineáris kombinációjaként. Ám az els osztásban éppen  $a$ -t osztjuk  $b$ -vel, tehát  $\text{Inko}(a, b)$  az  $a$  és  $b$  lineáris kombinációjával lesz egyenl. Ezzel a tétel bizonyítását befejeztük.

## Példák

A következ táblázat els oszlopában az euklideszi algoritmus osztásait olvashatjuk. Mint látható 89 és 26 relatív prímek,  $\text{Inko}(89, 26) = 1$ . A második oszlopban sorról sorra kifejeztük az osztás maradékát az osztandó és az osztó lineáris kombinációjaként.

A két utolsó oszlop celláinak kitöltése alulról felfelé haladva történt, a bennük feltüntetett sorszámoknak megfelelen. Az 1. sorszámú cellába egyszeren áthoztuk az utolsó nem nulla maradék elállítást. Az ebben szerepl 3-at a felette lév sorban található elállítással helyettesítettük. Ez található a számolás oszlop 2. sorszámú cellájában. Az itt kijelölt mveleteket végeredményét az Eredmény oszlop 3. sorszámú cellájában tüntettük fel. Ezt az eljárást folytattuk a 7. lépésig.

| Maradékos osztás       | Maradék elállítása             | Számolás: az elz eredménybe helyettesítjük az aktuális osztás maradékának elállítást | Eredmény                                               |
|------------------------|--------------------------------|--------------------------------------------------------------------------------------|--------------------------------------------------------|
| $89 = 3 \cdot 26 + 11$ | $11 = 1 \cdot 89 - 3 \cdot 26$ | $6. \text{Inko}(89, 26) = 3 \cdot 26 - 7 \cdot (1 \cdot 89 - 3 \cdot 26) =$          | $7. \text{Inko}(89, 26) = -7 \cdot 89 + (-7) \cdot 28$ |
| $26 = 2 \cdot 11 + 4$  | $4 = 1 \cdot 26 - 2 \cdot 11$  | $4. \text{Inko}(89, 26) = -1 \cdot 11 + 3 \cdot (1 \cdot 26 - 2 \cdot 11) =$         | $5. \text{Inko}(89, 26) = 3 \cdot 26 - 7 \cdot 11$     |
| $11 = 2 \cdot 4 + 3$   | $3 = 1 \cdot 11 - 2 \cdot 4$   | $2. \text{Inko}(89, 26) = 1 \cdot 4 - 1 \cdot (1 \cdot 11 - 2 \cdot 4) =$            | $3. \text{Inko}(89, 26) = -1 \cdot 11 + 3 \cdot 4$     |

$$4 = 1 \cdot 3 + 1$$

$$1 = 1 \cdot 4 - 1 \cdot 3$$

$$1. \text{Inko}(89, 26) = 1 \cdot 4 - 1 \cdot 3$$

Figyeljük meg, hogy az Eredmény oszlop szépen mutatja a legnagyobb közös osztó elállításait az adott sorban elvégzett osztás osztandójának és osztójának lineáris kombinációjaként.

Tekintsük a 3. lépésben található elállítást. Eszerint

$$\text{Inko}(89, 26) = -1 \cdot 11 + 3 \cdot 4,$$

tehát a legnagyobb közös osztó a **11** és a **4** lineáris kombinációjával úgy áll el, hogy az alkalmazandó együtthatók -1 és 3. Most térjünk rá a 4. lépésben elvégzett számításra, de most ne végezzük el a mveletek során keletkező összevonásokat. Az

$$\text{Inko}(89, 26) = -1 \cdot 11 + 3 \cdot (1 \cdot 26 - 2 \cdot 11) = 3 \cdot 26 + ((-1) - 3 \cdot 2) \cdot 11.$$

És most fogalmazzuk meg, hogy az elállításban szereplő konstansok értéke hogy alakul.

Az osztandó (26) együtthatója megegyezik az elz elállításban az osztó (4) együtthatójával. Ami a az osztó (11) együtthatóját illeti, abban (-1) az elz elállítás osztandójának együtthatója. A 3 az elz elállítás osztójának együtthatója, a 2 pedig az adott lépésben elvégzett osztás hányadosa. Tehát a következő két szabályt fedeztük fel. Az aktuális lépésben

- az osztandó együtthatója megegyezik az elz lépésbeli osztó együtthatójával, továbbá
- az osztó együtthatóját úgy kapjuk, hogy az elz elállítás osztójának együtthatójából levonjuk az elz osztás osztója együtthatójának és az aktuális osztás hányadosának szorzatát.

Kéretik ellenrizni, hogy ez a szabályosság a fenti táblázat minden sorára érvényben marad.

Ideje nekiállni a legnagyobb közös osztó lineáris kombinációként való elállítását elvégző algoritmus kidolgozásának. Az eddigiek alapján világos, hogy elsőként el kell végezni magát az euklideszi algoritmust. Másodikként az utolsó nem nulla maradékot adó osztásából kifejezzük a maradékot, vagyis legnagyobb közös osztót.

Azt is láttuk, hogy visszafelé kell haladnunk az euklideszi algoritmusban elvégzett maradékos osztások sorozatában mindaddig, amíg el nem érünk az első osztásig. Már csak egy kérdésre keressük a választ. Ha már kiszámítottuk az  $i$ -edik lépésben alkalmazandó együtthatókat (ezt az utolsó már gondolatban megtettük), akkor ezekből hogyan kell meghatározni az  $(i-1)$ -edik lépésben alkalmazandó együtthatókat?

Erre a kérdésre ugyan a 7.3 tétel bizonyítása választ ad, ám akkor másra figyeltünk. Mit is mondtunk a bizonyítás során? Ha az euklideszi algoritmus  $(i-1)$ -edik osztása

$$a_{i-1} = b_{i-1} \cdot q_{i-1} + r_{i-1},$$

akkor ennek az osztásnak a maradéka

$$r_{i-1} = a_{i-1} - b_{i-1} \cdot q_{i-1}.$$

Mi az alakja az  $i$ -edik osztásnak? Ennek osztandója az elz osztó, osztója pedig az elz maradék, tehát

$$b_{i-1} = r_{i-1} \cdot q_i + r_i.$$

Ha most rendre  $x$ -szel és  $y$ -nal jelöljük a legnagyobb közös osztó  $i$ -edik osztandóval és osztóval való elállításának együtthatóit, akkor

$$\text{Inko}(a, b) = x \cdot b_{i-1} + y \cdot r_{i-1} = x \cdot b_{i-1} + y \cdot (a_{i-1} - b_{i-1} \cdot q_{i-1}) = y \cdot a_{i-1} + (x - y \cdot q_{i-1}) \cdot b_{i-1}.$$

Tehát azt kaptuk, hogy az

$$x_{i-1} = y \text{ és } y_{i-1} = x - y \cdot q_{i-1}$$

választás mellett  $lnko(a, b) = x_{i-1} \cdot a_{i-1} + y_{i-1} \cdot b_{i-1}$  teljesül. Mindez azt jelenti, hogy az  $(i-1)$ -edik lépésben

- az osztandó együtthatója  $y$ , vagyis az  $i$ -edik osztás osztójának együtthatója,
- az osztó együtthatója pedig  $x - y \cdot q_{i-1}$ , vagyis vesszük a  $i$ -edik osztás osztójának együtthatóját ( $y$ ), azt összeszorozzuk az  $(i-1)$ -edik osztás hányadosával ( $q_{i-1}$ ) és az eredményt kivonjuk a  $i$ -edik osztás osztandójának együtthatójából ( $x$ ).

A számolást az euklideszi algoritmussal kezdjük, ám most szükség van a hányadosokra is.

| <i>osztan\</i><br><i>d\</i><br><i>ó</i> | <i>osztó</i> | <i>maradé\</i><br><i>k</i> | <i>hányado\</i><br><i>s</i> | <i>x</i> | <i>y</i> | <i>segédosz\</i><br><i>lop</i> |
|-----------------------------------------|--------------|----------------------------|-----------------------------|----------|----------|--------------------------------|
| 89                                      | 26           | 11                         | 3                           |          |          |                                |
| 26                                      | 11           | 4                          | 2                           |          |          |                                |
| 11                                      | 4            | 3                          | 2                           |          |          |                                |
| 4                                       | 3            | 1                          | 1                           |          |          |                                |
| 3                                       | 1            | 0                          | 3                           |          |          |                                |

A folytatás elkészítéséhez az  $x$  és  $y$  jel oszlopok utolsó soraiba rendre 0-t illetve 1-et írunk. Ez két okból is hasznos. Egyrészt megmarad az az összefüggés, hogy az osztandót  $x$ -szel, az osztót pedig  $y$ -nal szorozva az összeg kiadja a legnagyobb közös osztót:

$$1 = 0 \cdot 3 + 1 \cdot 1.$$

Másrészt ezekről a kezdértékekről indulva az  $x$  és  $y$  oszlopok képzési szabályait megtartva megkapjuk az utolsó nem nulla maradékot adó osztás sorára vonatkozó előállítást  
 $1 = 1 \cdot 4 + (0 - 1 \cdot 1) \cdot 3$ . Innentől kezdve pedig már az együtthatók előállítási szabálya működik.

| <i>osztan\</i><br><i>d\</i><br><i>ó</i> | <i>osztó</i> | <i>maradé\</i><br><i>k</i> | <i>hányado\</i><br><i>s</i> | <i>x</i> | <i>y</i> | <i>segédosz\</i><br><i>lop</i> |
|-----------------------------------------|--------------|----------------------------|-----------------------------|----------|----------|--------------------------------|
| 89                                      | 26           | 11                         | 3                           |          |          |                                |
| 26                                      | 11           | 4                          | 2                           |          |          | 3                              |
| 11                                      | 4            | 3                          | 2                           |          |          | 2                              |
| 4                                       | 3            | 1                          | 1                           |          |          | 2                              |
| 3                                       | 1            | 0                          | 3                           | 0        | 1        | 1                              |

A segédoszlopot azért vettük fel, hogy a számoló tábla kitöltési szabály egyszersődjön, és ezáltal könnyebben megjegyezhető legyen. A segédoszlop úgy keletkezik, hogy a hányados oszlopot eggyel lejjebb csúsztatjuk, a lecsorgó számot pedig elhagyjuk. Ezzel a lépéssel az érjük el, hogy az  $y$  oszlop kitöltése az alábbi alakot ölti.

- az aktuális sor  $y$  oszlopbeli elemét összeszorozzuk a mellette lévő segédoszlopbeli számmal, majd a szorzatot levonjuk a sor  $x$  oszlopából. Végül a kapott eredményt beírjuk a felette lévő sor  $y$  cellájába.

| $osztan \backslash$<br>$d \backslash$<br>$o$ | $osztó$ | $maradék$ | $hányados$ | $x$ | $y$ | $segédoszlop$ |
|----------------------------------------------|---------|-----------|------------|-----|-----|---------------|
| 89                                           | 26      | 11        | 3          | -7  | 24  |               |
| 26                                           | 11      | 4         | 2          | 3   | -7  | 3             |
| 11                                           | 4       | 3         | 2          | -1  | 3   | 2             |
| 4                                            | 3       | 1         | 1          | 1   | -1  | 2             |
| 3                                            | 1       | 0         | 3          | 0   | 1   | 1             |

Az  $x$  oszlop kitöltése is alulról felfelé haladva történik. Az aktuális értéket úgy kapjuk, hogy vesszük az eggyel alatta lévő sor  $y$  oszlopbeli elemét.

### 11.2.2. Algoritmus: Kiterjesztett euklideszi algoritmus (KEA)

| Szöveges leírás                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Maple metakód                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>1. <u>Input</u>: <math>a, b</math> pozitív egészek</p> <p>2. Legyen <math>n</math> a táblázat sorainak száma</p> <p>3. Az <math>i</math> változó <math>2, 3, \dots, n</math> értékeire hajtsuk végre az alábbi utasításokat</p> <p style="padding-left: 40px;">Legyen <math>T_{i,7} := T_{i-1,4}</math><br/>(segédoszlop feltöltése)</p> <p>4. Legyen <math>T_{n,5} := 0</math> és <math>T_{n,6} := 1</math><br/>(<math>x</math> és <math>y</math> kezd értéke)</p> <p>5. Az <math>i</math> változó <math>n-1, n-2, \dots, 1</math> értékeire hajtsuk végre az alábbi utasításokat</p> <p style="padding-left: 40px;">Legyen <math>T_{i,5} := T_{i+1,6}</math><br/>(<math>x</math> aktuális értéke)</p> <p style="padding-left: 40px;">Legyen <math>T_{i,6} := T_{i+1,5} - T_{i+1,6} \cdot T_{i+1,7}</math><br/>(<math>y</math> aktuális értéke)</p> <p>6. <u>Output</u>: <math>Inko(a, b) = T_{1,5} \cdot a + T_{1,6} \cdot b</math></p> | <p><u>Input</u>: <math>a, b</math> pozitív egészek</p> <p>A <math>T</math> táblázat első négyoszlopában végezzük el az euklideszi algoritmust</p> <p><math>n := \text{rowdim}(T)</math></p> <p><b>for</b> <math>i</math> <b>from</b> <math>2</math> <b>to</b> <math>n</math> <b>do</b></p> <p style="padding-left: 40px;"><math>T_{i,7} := T_{i-1,4}</math></p> <p><b>od</b>: <math>T_{n,5} := 0</math> és <math>T_{n,6} := 1</math></p> <p><b>for</b> <math>i</math> <b>from</b> <math>n-1</math> <b>to</b> <math>1</math> <b>by</b> <math>-1</math> <b>do</b></p> <p style="padding-left: 40px;"><math>T_{i,5} := T_{i+1,6}</math>;</p> <p style="padding-left: 40px;"><math>T_{i,6} := T_{i+1,5} - T_{i+1,6} \cdot T_{i+1,7}</math></p> <p><b>od</b>:</p> <p><u>Output</u>: <math>Inko(a, b) = a \cdot x_2 + b \cdot y_2</math></p> |

### 11.2.3. Maple implementáció

```
> restart;
```

```
> with(ant):
```

"Az ANT (Algorithmic Number Theory) csomag üdvözli Önt!"

(1.2.3.1)

A kiterjesztett algoritmus két paramétere az a két szám, amelyeknek a legnagyobb közös osztóját keressük. Az output pedig egy három elem lista, melynek els eleme az  $lnko$ , második és harmadik pedig a  $lnko$ -t előállító lineáris kombináció két együtthatója.

```
> KEA(8, 6);
```

[2, 1, -1]

(1.2.3.2)

Tehát  $lnko(8, 6) = 2$  és  $lnko(8, 6) = 1 \cdot 8 + (-1) \cdot 6$ . A szokásos **cal** opció megmutatja a számítás részleteit.

```
> KEA(88, 26, cal);
```

Euklideszi algoritmus eredménye(KEA):

| osztandó | osztó | maradék | hányados | x | y | segédoszlop |
|----------|-------|---------|----------|---|---|-------------|
| 88       | 26    | 10      | 3        |   |   |             |
| 26       | 10    | 6       | 2        |   |   |             |
| 10       | 6     | 4       | 1        |   |   |             |
| 6        | 4     | 2       | 1        |   |   |             |
| 4        | 2     | 0       | 2        |   |   |             |

Második rész elkészítése(KEA):

| osztandó | osztó | maradék | hányados | x | y | segédoszlop |
|----------|-------|---------|----------|---|---|-------------|
| 88       | 26    | 10      | 3        |   |   |             |
| 26       | 10    | 6       | 2        |   |   | 3           |
| 10       | 6     | 4       | 1        |   |   | 2           |
| 6        | 4     | 2       | 1        |   |   | 1           |
| 4        | 2     | 0       | 2        | 0 | 1 | 1           |

Részletek megjelenítése(KEA):

| osztandó | osztó | maradék | hányados | x  | y  | segédoszlop |
|----------|-------|---------|----------|----|----|-------------|
| 88       | 26    | 10      | 3        | -5 | 17 |             |
| 26       | 10    | 6       | 2        | 2  | -5 | 3           |
| 10       | 6     | 4       | 1        | -1 | 2  | 2           |
| 6        | 4     | 2       | 1        | 1  | -1 | 1           |
| 4        | 2     | 0       | 2        | 0  | 1  | 1           |

Eredmény(KEA):

[2, -5, 17]

(1.2.3.3)

A következ parancs azt mutatja, hogy a KEA akkor is jól dolgozik, ha az egyik bemen paraméter osztója a másiknak.

```
> KEA(80,10,cal);
```

Euklideszi algoritmus eredménye(KEA):

| osztandó | osztó | maradék | hányados | x | y | segédoszlop |
|----------|-------|---------|----------|---|---|-------------|
| 80       | 10    | 0       | 8        |   |   |             |

Második rész elkészítése(KEA):

| osztandó | osztó | maradék | hányados | x | y | segédoszlop |
|----------|-------|---------|----------|---|---|-------------|
| 80       | 10    | 0       | 8        | 0 | 1 |             |

Részletek megjelenítése(KEA):

| osztandó | osztó | maradék | hányados | x | y | segédoszlop |
|----------|-------|---------|----------|---|---|-------------|
| 80       | 10    | 0       | 8        | 0 | 1 |             |

Eredmény(KEA):

[10, 0, 1]

(1.2.3.4)

```
>
```

## Lineáris diofantoszi egyenlet partikuláris megoldása

### 11.3.1. Definíció

Az

$$a \cdot x + b \cdot y = c$$

alakú egyenletet **kétismeretlenes elsőfokú diofantoszi egyenletnek** nevezzük, ha együtthatói egészek, és a megoldásokat is az egész számok körében keressük. Ha az  $x_0$  és az  $y_0$  egészekre  $a \cdot x_0 + b \cdot y_0 = c$  teljesül, akkor azt mondjuk, hogy  $[x_0, y_0]$  a diofantoszi egyenlet **partikuláris megoldása**.

### Példák

Az alábbi egyenlet

$$2 \cdot x + 4 \cdot y = 5$$

kétismeretlenes elsőfokú diofantoszi egyenlet. Könnyen látható, hogy ennek az egyenletnek nem lehet megoldása, ugyanis a baloldalon mindig páros számot kapunk, akármit is helyettesítünk  $x$  és  $y$  helyébe, a jobb oldalon viszont páratlan szám áll. Ezzel szemben az

$$5 \cdot x + 8 \cdot y = 1$$

kétismeretlenes diofantoszi egyenletnek van megoldása,  $x = -3$  és az  $y = 2$ , ugyanis

$$5 \cdot (-3) + 8 \cdot 2 = -15 + 16 = 1.$$

Ugyankor  $x = 5$  és  $y = -3$  is megoldás, mert

$$5 \cdot (5) + 8 \cdot (-3) = 25 - 24 = 1.$$

Tehát mind  $[-3, 2]$ , mind pedig  $[5, -3]$  partikuláris megoldása az  $5x + 8y = 1$  egyenletnek.

Az elz fejezetben láttuk, hogy  $\text{lnko}(a, b)$  elállítható  $a$  és  $b$  lineáris kombinációjaként, vagyis alkalmas  $x_0$  és  $y_0$  egészekre

$$a \cdot x_0 + b \cdot y_0 = \text{lnko}(a, b).$$

Ám ami elttünk áll, az nem mást mutat, mint azt, hogy  $[x_0, y_0]$  partikuláris megoldása az

$$a \cdot x + b \cdot y = \text{lnko}(a, b)$$

kétismeretlenes elsőfokú diofantoszi egyenletnek. Eszerint az  $a \cdot x + b \cdot y = \text{lnko}(a, b)$  alakú diofantoszi egyenlet megoldható.

Most vegyünk egy olyan  $c$  egész számot, amelynek  $\text{lnko}(a, b)$  osztója. Ekkor  $\frac{c}{\text{lnko}(a, b)}$  egész. Ezzel az számmal az  $a \cdot x_0 + b \cdot y_0 = \text{lnko}(a, b)$  egyenlőséget megszorozva kapjuk, hogy

$$a \cdot \left( x_0 \cdot \frac{c}{\text{lnko}(a, b)} \right) + b \cdot \left( y_0 \cdot \frac{c}{\text{lnko}(a, b)} \right) = c.$$

Ez az egyenlőség pedig azt fejezi ki, hogy az

$$a \cdot x + b \cdot y = c$$

diofantoszi egyenletnek van megoldása, mégpedig

$$x = x_0 \cdot \frac{c}{\text{lnko}(a, b)} \quad \text{és} \quad y = y_0 \cdot \frac{c}{\text{lnko}(a, b)}.$$

Azt kaptuk tehát, hogy ha  $a$  és  $b$  legnagyobb közös osztója osztója  $c$ -nek, akkor az  $a \cdot x + b \cdot y = c$  diofantoszi egyenletnek van megoldása. Másrészt ez a megoldás megkapható oly módon, hogy az  $a \cdot x + b \cdot y = \text{lnko}(a, b)$  egyenlet megoldását megszorozzuk  $\frac{c}{\text{lnko}(a, b)}$ -vel.

Eszerint az, hogy  $\text{lnko}(a, b) \mid c$ , elégséges feltétele annak, hogy az  $a \cdot x + b \cdot y = c$  diofantoszi egyenlet megoldható legyen. Ám ez a feltétel szükséges is, ugyanis ha létezik olyan  $x$  és  $y$ , ami kielégíti az  $a \cdot x + b \cdot y = c$  diofantoszi egyenletet, akkor mivel  $\text{lnko}(a, b)$  osztója mind  $a \cdot x$ -nek, mind pedig  $b \cdot y$ -nak, így szükségképpen osztója azok összegének, tehát  $c$ -nek is. Ezzel beláttuk a következő tételt.

### ▼ 11.3.2. Tétel

Az

$$a x + b y = c$$

diofantoszi egyenlet akkor és csak akkor megoldható, ha  $\text{lnko}(a, b) \mid c$ . Az egyenlet egy partikuláris megoldását úgy kapjuk, hogy az

$$a \cdot x + b \cdot y = \text{lnko}(a, b)$$

egyenlet egy partikuláris megoldását megszorozzuk  $\frac{c}{\text{lnko}(a, b)}$ -vel.

A kétismeretlenes lineáris diofantoszi egyenletek partikuláris megoldásának kereséséhez minden eszköz a rendelkezésünkre áll. A megoldás kulcsa a kiterjesztett euklideszi algoritmus. Az alábbi



lépések elvégzése vezet el bennünket a megoldáshoz.

1. Az euklideszi algoritmussal meghatározzuk  $\text{lko}(a, b)$  értékét.
2. Ha  $\text{lko}(a, b)$  nem osztója  $c$ -nek, akkor nincs megoldás.
3. Ellenkez esetben, a kiterjesztett euklideszi algoritmus segítségével meghatározzuk az  $a \cdot x + b \cdot y = \text{lko}(a, b)$  egyenlet egy partikuláris megoldását.
4. A 3. lépésben kapott  $x$  és  $y$  értékeket  $\frac{c}{\text{lko}(a, b)}$ -val megszorozva kapjuk az  $a \cdot x + b \cdot y = c$  diofantoszi egyenlet egy partikuláris megoldását.

Els példaként határozzuk meg, hogy a

$$120 \cdot x + 45 \cdot y = 20$$

diofantoszi egyenlet emegoldható-e? Végrehajtjuk a kiterjesztett euklideszi algoritmust  $a = 120$  és  $b = 45$ -re.

| Osztandó | Osztó | Maradék |  |
|----------|-------|---------|--|
| 120      | 45    | 30      |  |
| 45       | 30    | 15      |  |
| 30       | 15    | 0       |  |

Els lépésként csak az legnagyobb közös osztót határoztuk meg. Ez 15, ami nem osztója 20-nak, tehát a vizsgált egyenletnek nincs megoldása.

Most pedig oldjuk meg a

$$840 \cdot x + 33 \cdot y = 15$$

diofantoszi egyenletet. A kiterjesztett euklideszi algoritmust  $a = 840$  és  $b = 33$  számokra kezdjük végrehajtani.

| Osztandó                                                                                       | Osztó | Maradék |  |
|------------------------------------------------------------------------------------------------|-------|---------|--|
| 840                                                                                            | 33    | 15      |  |
| 33                                                                                             | 15    | 3       |  |
| 15                                                                                             | 3     | 0       |  |
| $\text{lko}(a, b) = \text{lko}(840, 33) = 3$ , $\frac{c}{\text{lko}(a, b)} = \frac{15}{3} = 5$ |       |         |  |

Elsör most is a legnagyobb közös osztót határoztuk meg. Mivel ez 3, ami osztója a megoldandó egyenlet jobb oldalán álló 15-nek, ezért egyenletünknek van megoldása. Így folytattuk a táblázat kitöltését az  $x$  és  $y$  oszlopokkal. Az eredmények alapján  $x = -2$  és  $y = 51$  megoldása a

$$840 \cdot x + 33 \cdot y = 3$$

diofantoszi egyenletnek. Valóban

$$840 \cdot (-2) + 33 \cdot 51 = -1680 + 1683 = 3.$$

Eddig rendben. Most vennünk kell a jobboldali konstans ( $c = 15$ ) és az  $\text{lko}(840, 33)$  hányadosát, ez

$$\frac{15}{\text{lko}(840, 33)} = \frac{15}{3} = 5.$$

Ezzel megszorozva a kapott  $-2$  és  $51$  értékeket egyenletünk megoldására

$$x = (-2) \cdot 5 = -10 \quad \text{és} \quad y = 51 \cdot 5 = 255$$

adódik. Ellenrizzük, hogy valóban megoldást kaptunk-e!

$$840 \cdot (-10) + 33 \cdot 255 = -8400 + 8415 = 15.$$

Az eredmény megnyugtató.

## Az általános megoldás

A diofantoszi egyelet partikuláris megoldásából kiindulva könny további megoldásokat találni. Tekintsük továbbra is a  $840 \cdot x + 33 \cdot y = 15$  egyenletet. Adjuk hozzá az  $x = -10$  partikuláris megoldáshoz az  $y$  együtthatójának ( $33$ ) és a baloldali együtthatók ( $840, 33$ ) legnagyobb közös osztójának ( $3$ ) hányadosát.

$$x_1 = -10 + \frac{33}{\text{lko}(840, 33)} = -10 + \frac{33}{3} = -10 + 11 = 1.$$

Az  $y$  értékebl pedig vonjuk le az  $x$  együtthatójának és az  $\text{lko}(840, 33)$ -nak a hányadosát

$$y_1 = 255 - \frac{840}{\text{lko}(840, 33)} = 255 - \frac{840}{3} = 255 - 280 = -25.$$

Végül helyettesítsük be ezeket az értékeket az eredeti egyenletbe:

$$840 \cdot 1 + 33 \cdot (-25) = 840 - 825 = 15.$$

Tehát az  $x_1$  és az  $y_1$  új megoldását adja az egyenletnek. Ebből is látszik, hogy az eljárást  $x_1$ -re és  $y_1$ -re megismételve további megoldásokhoz juthatunk. Így egyre újabb és újabb megoldásokat kreálva láthatjuk, hogy ha a kétismeretlenes lineáris diophantosi egyenletnek létezik megoldása, akkor végtelen sok megoldása van.

### 11.4.1. Tétel

Legyen  $a$  és  $b$  egész szám. Ha az

$$a x + b y = c$$

diofantoszi egyenletnek  $[x_0, y_0]$  partikuláris megoldása, akkor az összes megoldást a

$$x = x_0 + \frac{b}{\text{lko}(a, b)} \cdot t$$

$$y = y_0 - \frac{a}{\text{lko}(a, b)} \cdot t$$

formulák szolgáltatják, ahol  $t$  tetszleges egész.

## Bizonyítás

Arról egyszer behelyettesítéssel meggyőződhetünk, hogy az állításban szereplő  $x$  és  $y$  valóban megoldás. Ugyanis

$$a \cdot x + b \cdot y = a \cdot \left( x_0 + \frac{b}{\text{luko}(a, b)} \cdot t \right) + b \cdot \left( y_0 - \frac{a}{\text{luko}(a, b)} \cdot t \right) = a \cdot x_0 + \frac{a \cdot b}{\text{luko}(a, b)} \cdot t + b \cdot y_0 - \frac{a \cdot b}{\text{luko}(a, b)} \cdot t = a \cdot x_0 + b \cdot y_0 = c.$$

Ha pedig azt tesszük fel, hogy  $x$  és  $y$  megoldások, akkor teljesülnek a

$$a x_0 + b y_0 = c$$

$$a x + b y = c$$

egyenlőségek. Ezek különbségét képezve az

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

egyenlőséghez jutunk, amit átrendezve és  $\text{luko}(a, b)$ -vel elosztva az

$$\frac{a}{\text{luko}(a, b)} \cdot (x - x_0) = -\frac{b}{\text{luko}(a, b)} \cdot (y - y_0).$$

egyenlőséget kapjuk.

Mivel  $\frac{a}{\text{luko}(a, b)}$  relatív prím  $\frac{b}{\text{luko}(a, b)}$ -hez, ezért egyrészt  $\frac{a}{\text{luko}(a, b)}$  osztója  $(y - y_0)$ -nak, másrészt  $\frac{b}{\text{luko}(a, b)}$  osztója  $(x - x_0)$ . Tehát alkalmas  $q_1$  és  $q_2$  egészekre

$$y - y_0 = -\frac{a}{\text{luko}(a, b)} \cdot q_1 \text{ és } x - x_0 = \frac{b}{\text{luko}(a, b)} \cdot q_2.$$

Ebből

$$y = y_0 - \frac{a}{\text{luko}(a, b)} \cdot q_1 \text{ és } x = x_0 + \frac{b}{\text{luko}(a, b)} \cdot q_2.$$

Ez a két értéket az  $a \cdot x + b \cdot y = c$  egyenletbe helyettesítve

$$a \cdot \left( x_0 + \frac{b}{\text{luko}(a, b)} \cdot q_2 \right) + b \cdot \left( y_0 - \frac{a}{\text{luko}(a, b)} \cdot q_1 \right) = c$$

$$a \cdot x_0 + \frac{a \cdot b}{\text{luko}(a, b)} \cdot q_2 + b \cdot y_0 - \frac{a \cdot b}{\text{luko}(a, b)} \cdot q_1 = c$$

$$\frac{a \cdot b}{\text{luko}(a, b)} \cdot q_2 = \frac{a \cdot b}{\text{luko}(a, b)} \cdot q_1$$

$$q_2 = q_1.$$

Ezzel a bizonyítást befejeztük.

Az előfejezetben meghatároztuk a

$$840 \cdot x + 33 \cdot y = 15$$

diofantoszi egyenlet partikuláris megoldását:  $x = -10$  és  $y = 255$ . A most bizonyított tétel szerint

az egyenlet összes megoldását

$$x = -10 + \frac{33}{\text{lnko}(840, 33)} \cdot t = -10 + \frac{33}{3} \cdot t = -10 + 11 \cdot t$$

$$y = 255 - \frac{840}{\text{lnko}(840, 33)} \cdot t = 255 - \frac{840}{3} \cdot t = 255 - 280 \cdot t$$

formulák szolgáltatják. Lelkiismeretünk megnyugtató végett hajtsuk végre az ellenrzést.

$$840 \cdot (-10 + 11 \cdot t) + 33 \cdot (255 - 280 \cdot t) = 8400 + 9240 \cdot t + 8415 - 9240 \cdot t = 15.$$

Tehát minden rendben.

A kézi számolási sémát kiegészítjük egy új sorral. Ebben kiszámítjuk a  $\frac{b}{\text{lnko}(a, b)}$  és a  $\frac{a}{\text{lnko}(a, b)}$  értékeket, és az  $x$  és  $y$  jel oszlopba beírjuk az általános megoldást.

| Osztandó                                                                 | Osztó | Maradék |        |
|--------------------------------------------------------------------------|-------|---------|--------|
| 840                                                                      | 33    | 15      |        |
| 33                                                                       | 15    | 3       |        |
| 15                                                                       | 3     | 0       |        |
| $\text{lnko}(a, b) = 3$ , $\frac{c}{\text{lnko}(a, b)} = 5$              |       |         | Partik |
| $\frac{b}{\text{lnko}(a, b)} = 11$ , $\frac{a}{\text{lnko}(a, b)} = 280$ |       |         | Által  |

A most következ algoritmusban felhasználjuk a kiterjesztett euklideszi algoritmus Maple implementációját, a *KEA* nev eljárást. Emlékeztetünk rá, hogy ennek bemen paramétere két nem negatív egész ( $a$  és  $b$ ), outputja pedig három elem lista. A lista els eleme  $\text{lnko}(a, b)$  második és harmadik eleme pedig az  $\text{lnko}(a, b)$ -nek  $a$  és  $b$ -vel elállított lineáris kombinációjának együtthatói. Ha tehát  $z = \text{KEA}(a, b)$ , akkor  $z_1$  maga a legnagyobb közös osztó, továbbá

$$z_1 = a \cdot z_2 + b \cdot z_3.$$

### 11.4.2. Algoritmus: Lineáris diofantoszi egyenlet megoldása

| Szöveges leírás                                                                                                                                                                                                                                                                                                                                | Maple metakód                                                                                                                                                                                                                                                                |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>1. <u>Input</u>: <math>a, b, c</math> pozitív egészek (<math>a \cdot x + b \cdot y = c</math>)</p> <p>2. Legyen <math>z := \text{KEA}(a, b) : \text{lnko} = z_1</math></p> <p>3. Ha <math>z_1</math> osztója <math>c</math>-nek Akkor</p> <p><math>x_0 = z_2 \cdot \frac{c}{\text{lnko}} : y_0 = z_3 \cdot \frac{c}{\text{lnko}}</math></p> | <p><u>Input</u>: <math>a, b, c</math> pozitív egészek (<math>a \cdot x + b \cdot y = c</math>)</p> <p><math>z := \text{KEA}(a, b)</math> <b>if</b> <math>\text{irem}(z_1, c)</math> <b>then</b></p> <p><math>x := \frac{z_2 \cdot c}{z_1} + \frac{b}{z_1} \cdot t</math></p> |

Legyen  $x := x_0 + \frac{b}{\text{lnko}} \cdot t$

Legyen  $y := y_0 - \frac{a}{\text{lnko}} \cdot t$

Különben

"Nincs megoldás"

4. Output:  $[x, y]$

$$y := \frac{z_3 \cdot c}{z_1} - \frac{a}{z_1} \cdot t$$

**return**  $[x, y]$

**else**

*print*("Nincs megoldás")

**return**  $[]$

**fi**:

Output:  $\text{lnko}(a, b) = a \cdot x_2 + b \cdot y_2$

### 11.4.3. Maple implementáció

**> restart;**

**> with(ant):**

"Az ANT (Algorithmic Number Theory) csomag üdvözli Önt!"

**(1.4.3.1)**

A Diofantosz eljárást a már korábban kézzel megoldott egyenlettel mutatjuk be. Ám biztatjuk olvasónkat, hogy hívja meg az eljárást különböző együttthatókkal, figyelje meg az eredményeket és értelmezze azokat.

**> Diofantosz(840, 33, 15);**

$[x = -10 + 11t, y = 255 - 280t]$

**(1.4.3.2)**

**> Diofantosz(840, 33, 15, cal);**

Részletek megjelenítése(Diofantosz):

$\left[ \left[ \text{osztandó}, \text{osztó}, \text{maradék}, \text{hányados}, x, y \right], \right.$

$\left[ 840, 33, 15, 25, -2, 51 \right],$

$\left[ 33, 15, 3, 2, 1, -2 \right],$

$\left[ 15, 3, 0, 5, 0, 1 \right],$

$\left[ , \text{lnko}(a, b) = 3, \frac{c}{\text{lnko}(a, b)} = 5, \text{Partikuláris megoldás:}, -10, 255 \right],$

$\left[ , \frac{b}{\text{lnko}(a, b)} = 11, \frac{a}{\text{lnko}(a, b)} = 280, \text{Általános megoldás:}, -10 + 11t, \right.$   
 $\left. 255 - 280t \right]$

Eredmény(Diofantosz):

$[x = -10 + 11t, y = 255 - 280t]$

**(1.4.3.3)**

### Négyszög háromszögszámok

A második eladásban már találkoztunk a háromszög számokkal. Ezek azok a számok, amelyekre

az teljesül, hogy annyi darab kavics kirakható háromszög alakzatba. Ilyen számok például az 1, 3, 6 és 10. Azt is megmutattuk, hogy a háromszög számok kielégítik a  $T_{n+1} = T_n + (n + 1)$  rekurzív relációt, valamint azt, hogy az két elállító zárt formula

$$T_n = \frac{n \cdot (n + 1)}{2}.$$

A négyzetszámok négyzet alakban elrendezhet kavicsokat biztosítanak, és így az két elállító formula értelemszerűen

$$S_n = n^2.$$

Most arra kérdésre keressük a választ, hogy a háromszögszámok és a négyzetszámok halmazának vannak-e közös elemei? Vagyis a következő két kérdést tesszük fel.

- a) Melyek azok a háromszögszámok, amelyek egyidejleg négyzetszámok is?
- b) Van-e rekurzív formula a két halmaz közös elemeire?

Az els kérdésre a természetes reakciónk, hogy kísérletezzünk. Nézzük meg az els 20 háromszögszámot

1, 3, 6, 10, 15, 21, 28, 36, 45, 55, 66, 78, 91, 105, 120, 136, 153, 171, 190, 210 .

És máris megtaláltuk az els olyan egytl különböz háromszög számot, ami négyzetszám is, ez a 36. Érdemes tehát tovább menni, mert a két vizsgált halmaz metszete nem csak az 1-et tartalmazza. Ha azt akarjuk, hogy az  $n$ -edik háromszög szám legyen egyenl valamilyen  $m$ -re az  $m$ -edik négyzetszámmal, akkor  $n$  és  $m$ -nek egészeknek ki kell elégítenie az

$$\frac{n \cdot (n + 1)}{2} = m^2$$

egyenletet, melyen végezzük el a következő átalakításokat. Kettvel való szorzás után:

$$n^2 + n = 2 \cdot m^2.$$

Az egyenlet mindkét oldalát 4-gyel szorozzuk:

$$4 \cdot n^2 + 4 \cdot n = 4 \cdot 2 \cdot m^2,$$

majd a bal oldalt teljes négyzetté alakítjuk

$$(2 \cdot n + 1)^2 - 1 = 2 \cdot (2 \cdot m)^2.$$

Végül bevezetjük az

$$x = 2 \cdot n + 1 \text{ és } y = 2 \cdot m$$

jelölést, és ezzel az

$$x^2 - 2 \cdot y^2 = 1$$

diofantoszi egyenlethez jutunk, melyet **Pell egyenletnek** nevezünk. Mivel az eddig elvégzett átalakításaink visszafelé is elvégezhetk, ezért kimondhatjuk a következő tételt.

### ▼ 11.5.1. Tétel

Az  $n$  és  $m$  egész szám akkor és csak akkor megoldása az

$$\frac{n \cdot (n + 1)}{2} = m^2$$

egyenletnek, ha  $x = 2 \cdot n + 1$  és  $y = 2 \cdot m$  megoldása az

$$x^2 - 2 \cdot y^2 = 1$$

egyenletnek.

## Példák

Vizsgáljuk meg a 36-ot, ami háromszögszám is és négyzetszám is egyben. Mivel 36 a nyolcadik háromszögszám ( $36 = \frac{8 \cdot 9}{2}$ ), ezért  $n = 8$ . Ugyanakkor 36 a hatodik négyzetszám, tehát  $m = 6$ .

Ezeket az értékeket az

$$x = 2 \cdot n + 1 \text{ és } y = 2 \cdot m$$

formulákba helyettesítve az

$$x = 2 \cdot 8 + 1 = 17 \text{ és } y = 2 \cdot 6 = 12$$

értékekhez jutunk. Ez a két egész valóban kielégíti a Pell egyenletet ugyanis

$$17^2 - 2 \cdot 12^2 = 289 - 2 \cdot 144 = 289 - 288 = 1.$$

Most pedig keressünk próbálkozással megoldásokat a Pell egyenlethez! A feladat olyan négyzetszámok megkeresése, amelyek közül a kisebbet kettővel szorozva a nagyobbiknál 1-gyel kisebb számot kapunk. Ehhez írjunk fel néhány négyzetszámot:

$$1, 4, 9, 16, 25, 36, 49, 64.$$

Mindjárt az elején sikerélményünk van! Ugyanis a 4 kétszerese eggyel kisebb 9-nél. Ez a Pell egyenlet alakjában megjelenítve látjuk, hogy

$$3^2 - 2 \cdot 2^2 = 9 - 4 = 1,$$

ami azt mutatja, hogy  $x = 3$  és az  $y = 2$  kielégíti a Pell egyenletet. A nekik megfelel  $n$  és  $m$  értékek pedig az alábbiak szerint alakulnak

$$n = \frac{3-1}{2} = 1 \text{ és } m = \frac{2}{2} = 1.$$

Nos, megtaláltuk az 1-et, ami az els háromszögszám és egyben az els négyzetszám is.

A Pell egyenlet jobb oldalán 1 áll, melynek négyzete önmaga. Érdekes lenne megnézni, hogyan viselkedik a Pell egyenlet bal oldala négyzetre emelés esetén.

$$(x^2 - 2 \cdot y^2)^2 = x^4 - 4 \cdot x^2 \cdot y^2 + 4 \cdot y^4.$$

Ebbl bizony nem sok minden látszik, de ne adjuk fel! A jobb oldalon jó lenne olyasmit látni, ami emlékeztet a Pell egyenletre: "valaminek a négyzetébl le van vonva valami négyzetének a kétszerese". Ha a jobb oldali kifejezést  $(x^4 + 4 \cdot y^4) - 4 \cdot x^2 \cdot y^2$  alakba írjuk, akkor azt vehetjük észre, hogy a zárójelben lévő kifejezés emléketet két tag négyzetének a két négyzetes tagjára, hiányzik viszont a kétszeres szorzat. Erre els ötletünk a  $4 \cdot x^2 \cdot y^2$  hozzáadása és levonása lehet. És mint látni fogjuk, ez egyben elegendő utolsó ötletnek is. Ugyanis

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

ez pedig pontosan az az alak amire vágytunk. És mivel  $(x^2 - 2 \cdot y^2)^2 = 1$ , így

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

Kaptuk, hogy  $x^2 + 2 \cdot y^2$  és  $2 \cdot x \cdot y$  is megoldása a Pell egyenletnek, ha  $x$  és  $y$  is az volt.

Ez annyira izgalmas eredmény, hogy példákkal is meg kell gyzni magunkat. Azt láttuk, hogy  $x = 3$  és  $y = 2$  megoldás. Lássuk a számolást

$$x^2 + 2 \cdot y^2 = 3^2 + 2 \cdot 2^2 = 9 + 8 = 17,$$

valamint

$$2 \cdot x \cdot y = 2 \cdot 3 \cdot 2 = 12.$$

Valóban megoldást kaptunk? Nem kell mást tenni, mint behelyettesíteni

$$17^2 - 2 \cdot 12^2 = 289 - 2 \cdot 144 = 289 - 288 = 1.$$

Tehát az  $x = 3$  és  $y = 2$  megoldásból a kapott összfüggés alapján le tudunk gyártani egy újabb megoldást:  $x = 17$  és  $y = 12$ . Ha a felismert összefüggés jól működik, akkor ebből a megoldásból kiindulva is egy újabb megoldást kaphatunk, és így tovább, az eljárást minden határon túl folytathatjuk. Ezzel megoldások egy  $x_k, y_k$  sorozatát állíthajtuk el, melyre az alábbi rekurzív reláció teljesül

$$1. x_1 = 3 \text{ és } y_1 = 2$$

$$2. x_{k+1} = x_k^2 + 2 \cdot y_k^2 \text{ és } y_{k+1} = 2 \cdot x_k \cdot y_k \quad (k \geq 1).$$

Kaptunk tehát végtelen sok megoldást a Pell egyenletre. És mivel megmutatható, hogy ezeken kívül nincs más megoldás, úgy is fogalmazhatunk, hogy a most rekurzív módon bevezetett sorozat a Pell egyenlet összes megoldását tartalmazza.

Az alábbi táblázatban kiszámítottuk a Pell egyenlet megoldásainak sorozatából néhány elemet

| $k$ | $x_k$  | $y_k$  | Magyarázat                                                            |
|-----|--------|--------|-----------------------------------------------------------------------|
| 1   | 3      | 2      |                                                                       |
| 2   | 17     | 12     | $17 = 3^2 + 2 \cdot 2^2,$<br>$12 = 2 \cdot 3 \cdot 2$                 |
| 3   | 577    | 408    | $577 = 17^2 + 2 \cdot 12^2,$<br>$408 = 2 \cdot 17 \cdot 12$           |
| 4   | 665857 | 470832 | $665857 = 577^2 + 2 \cdot 408^2,$<br>$470832 = 2 \cdot 577 \cdot 408$ |

Figyeljük meg, hogy a Pell egyenlet megoldásai milyen rohamosan nőnek!

Most már fel tudjuk sorolni a Pell egyenlet megoldásainak sorozatát, ám minket azok a háromszög számok érdekelnek, amelyek egyben négyzetszámok is. A megoldás a kezünkben van, csak formába kell önteni. A 7.10 tétel kapcsolatot létesít a Pell egyenlet  $[x, y]$  megoldásai és az  $[n, m]$  számpárok között. Itt az  $n$  jelenti a háromszögszámok sorozatában azt az indexet, amelyre az  $n$ -edik háromszögszám egyben  $m$ -edik négyzetszám is. A kapcsolatot az



$$x = 2 \cdot n + 1 \text{ és } y = 2 \cdot m$$

egyenlségek írják le. Mivel most  $x$ -et és  $y$ -t ismerjük, így  $n$ -et és  $m$ -et rendre kifejezzük ezekből az egyenlségekből:

$$n = \frac{x-1}{2} \text{ és } m = \frac{y}{2}.$$

Ezt a két egyenlséget felhasználva a Pell egyenlet sorozatára nyert rekurzív összefüggés az  $n$  és  $m$  értékek alábbi rekurzív meghatározásához vezet

$$1. n_1 = 1 \text{ és } m_1 = 1,$$

$$2. n_{k+1} = 4 \cdot n_k^2 + 2 \cdot n_k + 4 \cdot m_k^2 \text{ és } m_{k+1} = 4 \cdot n_k \cdot m_k + 2 \cdot m_k$$

Az alábbi táblázatban kiszámítottuk az  $[n_k, m_k]$  sorozat első négy elemét, és kiszámítottuk az  $n_k$ -adik háromszög számot valamint az  $m_k$ -adik négyzet számot.

| $k$ | $n_k$  | $m_k$  | Ellenőrzés                                                 | Ellenőrzés                            |
|-----|--------|--------|------------------------------------------------------------|---------------------------------------|
| 1   | 1      | 1      | $T_1 = 1$                                                  | $S_1 = 1$                             |
| 2   | 8      | 6      | $T_8 = \frac{8 \cdot 9}{2} = 36$                           | $S_6 = 6^2 = 36$                      |
| 3   | 288    | 204    | $T_{288} = \frac{288 \cdot 289}{2} = 41616$                | $S_{204} = 204^2 = 41616$             |
| 4   | 332928 | 235416 | $T_{332928} = \frac{332928 \cdot 332929}{2} = 55420693056$ | $S_{235416} = 235416^2 = 55420693056$ |

### 11.5.2. Algoritmus: Négyzög háromszög számok

| Szöveges leírás                                                                                                                                                                                                                                                                                                                                                                                                               | Maple metakód                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>1. <u>Input</u>: <math>k</math> természetes szám</p> <p>2. <math>n = 1 : m = 1</math></p> <p>4. Az <math>i</math> változó 2, 3, ..., <math>k</math> értékeire hajtsuk végre az alábbi utasításokat</p> $xn := 4 \cdot n^2 + 2 \cdot n + 4 \cdot m^2$ $xm := 4 \cdot n \cdot m + 2 \cdot m$ $n = xn : m := xm$ <p>7. <u>Output</u>: <math>\frac{n \cdot (n + 1)}{2}</math> a <math>k</math>-adik négyszög háromszögszám</p> | <p><u>Input</u>: <math>k</math> természetes szám</p> $n := 1 : m := 1$ <p><b>for</b> <math>i</math> <b>from</b> 2 <b>to</b> <math>k</math> <b>do</b></p> $xn := 4 \cdot n^2 + 2 \cdot n + 4 \cdot m^2$ $xm := 4 \cdot n \cdot m + 2 \cdot m :$ $n = xn : m := xm$ <p><b>od</b>:</p> <p><u>Output</u>: <math>\frac{n \cdot (n + 1)}{2}</math> a <math>k</math>-adik négyszög</p> |

### 11.5.3. Maple implementáció

```
> restart;
```

```
> with(ant):
```

"Az ANT (Algorithmic Number Theory) csomag üdvözlí Önt!" (1.5.3.1)

Az **m34** eljárás állítja el a négyszög háromszögszámokat. Outputjának els eleme a keresett számnak háromszög számok sorozatában elfoglalt helyének indexe. A második paraméter a a szám négyszög számokbeli indexe, végül a harmadik eleme maga a keresett négyszög háromszög szám.

```
> m34(4,cal);
```

Részletek megjelenítése(m34):

| 4 | <i>n</i> -edik háromszögszám | <i>n</i> -edik négyzetszám |
|---|------------------------------|----------------------------|
| 1 | $T_1 = 1$                    | $S_1 = 1$                  |
| 2 | $T_8 = 36$                   | $S_6 = 36$                 |
| 3 | $T_{288} = 41616$            | $S_{204} = 41616$          |
| 4 | $T_{332928} = 55420693056$   | $S_{235416} = 55420693056$ |

Eredmény(m34):

[332928, 235416, 55420693056] (1.5.3.2)

Legyünk óvatosak az m34 használatával. Már a 6 inputra is óriási számokat eredményez.

```
> m34(6);
```

[786292024016459316676608, 555992422174934068969056, 309127573515950117423442905473334441338685531136] (1.5.3.3)

```
> 786292024016459316676608*(786292024016459316676608+1)/2;
```

309127573515950117423442905473334441338685531136 (1.5.3.4)

```
> 555992422174934068969056^2;
```

309127573515950117423442905473334441338685531136 (1.5.3.5)

### Ellenrz kérdések

1. Mit nevezünk diofantoszi egyenletnek? Mikor mondjuk, hogy a diofantoszi egyenlet lineáris?
2. Oldjuk meg algebrai módszerrel az alábbi lineáris diofantoszi egyenleteket!
  - a)  $x + 5y = 4$
  - b)  $28x + 80y = 40$
3. Hajtsuk végre a kiterjesztett euklideszi algoritmust az alábbi számpárokon!
  - a) [130,85]
  - b) [36,11]
  - c) [345, 123]
  - e) [2432, 460]

4. Állítsuk el az alábbi számpárok legnagyobb közös osztóját a számok lineáris kombinációjaként!

a) [25,5]      b) [76, 24]      c) [354, 120]      e) [24032, 4060]

5. Írjuk le a KEA egyes lépéseit! Hogy töltjük ki az  $x$  és  $y$  jel oszlopokat?

6. Ha nem használnánk a segédoszlopot a KEA-ban, hogy módosulna az  $x$  és  $y$  oszlopok kitöltési szabálya?

7. Mi a feltétele az  $a \cdot x + b \cdot y = c$  diofantoszi egyenlet megoldhatóságának?

8, Milyen lépéseket kell elvégezni ahhoz hogy megkapjuk az  $a \cdot x + b \cdot y = c$  egy megoldását!

9. Döntsük el, hogy az alábbi diofantoszi egyenleteknek van-e megoldása, és ha igen, adjunk meg egy megoldást!

a)  $12x + 4y = 5$     b)  $210x + 84y = 1240$     c)  $44x + 3x = 7$     d)  $51x + 21y = 82$

10. Hogy áll el az  $a \cdot x + b \cdot y = c$  diofantoszi egyenlet általános összes megoldása egy konkrét megoldásból?

11. Adjuk meg az alábbi diofantoszi egyenletek összes megoldását!

a)  $11x + 5y = 4$     b)  $238x + 84y = 40$     c)  $44x + 33x = 22$     d)  $51x + 21y = 82$

12. Mi a kapcsolat a négyszög háromszögszámok és a Pell egyenlet között?