# Diofantikus egyenletek

## Definíció

Az $ax + by = c$ alakú egyenleteket (ahol $a, b, c \in \mathbb{Z}$ ismertek, $x, y \in \mathbb{Z}$ ismeretlenek) lineáris diofantikus egyenleteknek nevezzük.

## Tétel

Az $ax + by = c$ lineáris diofantikus egyenlet pontosan akkor oldható meg, ha $(a, b)|c$.

## Tétel

Ha az $ax + by = c$ diofantikus egyenlet megoldható, akkor végtelen sok megoldása van, ezek

$$x = x_0 + t\frac{b}{(a, b)}, \quad y = y_0 - t\frac{a}{(a, b)}, \quad t \in \mathbb{Z},$$

alakban írhatók fel, ahol $(x_0, y_0)$ egy adott megoldás.

# Példa

$154x - 980y = 42$

$\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ $\begin{bmatrix} -6 \\ 1 \end{bmatrix}$ $\begin{bmatrix} u \\ v \end{bmatrix}$ : $154u + 980v$

$980 = 6 \cdot 154 + 56$

$\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ $\begin{bmatrix} -6 \\ 1 \end{bmatrix}$ $\begin{bmatrix} 13 \\ -2 \end{bmatrix}$

$154 = 2 \cdot 56 + 42 \longrightarrow 42 = \underset{\uparrow \atop x_0 = 13}{13} \cdot 154 - \underset{\uparrow \atop y_0 = 2}{2} \cdot 980$

$\begin{bmatrix} -6 \\ 1 \end{bmatrix}$ $\begin{bmatrix} 13 \\ -2 \end{bmatrix}$ $\begin{bmatrix} -19 \\ 3 \end{bmatrix}$

$56 = 1 \cdot 42 + \boxed{14}$

$42 = 3 \cdot 14 + 0$

$(980, 154) = 14 \mid 42 \implies$ az egyenlet megoldható

$$x = x_0 + t \cdot \frac{b}{(a,b)} \qquad t \in \mathbb{Z}$$

−980

14

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

154

14

$$x = 13 - t \cdot 70$$

$$y = 2 - t \cdot 11 \qquad t \in \mathbb{Z}$$

# Példa

$286x + 693y = 33$

$$\begin{bmatrix} u \\ v \end{bmatrix} : \quad 286u + 693v$$

$$\overset{\begin{bmatrix} 0 \\ 1 \end{bmatrix}}{693} = 2 \cdot \overset{\begin{bmatrix} 1 \\ 0 \end{bmatrix}}{286} + \overset{\begin{bmatrix} -2 \\ 1 \end{bmatrix}}{121}$$

$$\overset{\begin{bmatrix} 1 \\ 0 \end{bmatrix}}{286} = 2 \cdot \overset{\begin{bmatrix} -2 \\ 1 \end{bmatrix}}{121} + \overset{\begin{bmatrix} 5 \\ -2 \end{bmatrix}}{44}$$

$$\overset{\begin{bmatrix} -2 \\ 1 \end{bmatrix}}{121} = 2 \cdot \overset{\begin{bmatrix} 5 \\ -2 \end{bmatrix}}{44} + \overset{\begin{bmatrix} -12 \\ 5 \end{bmatrix}}{33}$$

$$33 = -12 \cdot 286 + 5 \cdot 693$$

$x_0 = -12 \qquad y_0 = 5$

$$44 = 1 \cdot 33 + \boxed{11}$$

$$33 = 3 \cdot 11 + 0$$

$(286, 693) = 11 \mid 33 \Rightarrow$ megoldható

$$x = x_0 + t \cdot \frac{b}{(a,b)} = -12 + t \cdot \frac{693}{11} = -12 + 63 \cdot t$$

$$y = y_0 - t \cdot \frac{a}{(a,b)} = 5 - t \cdot \frac{286}{11} = 5 - 26 \cdot t$$

$$t \in \mathbb{Z}$$

# Prímszámok

Minden $n > 1$, $n \in \mathbb{N}$ számnak van két pozitív osztója: az 1 és az $n$, ezeket triviális osztóknak nevezzük. A többi pozitív osztó $n$ nem triviális osztója.

## Definíció

Azokat az 1-nél nagyobb természetes számokat, amelyeknek csak triviális osztóik vannak, prímszámoknak nevezzük. Azokat, amelyeknek van nem triviális osztójuk is, összetett számoknak hívjuk. Az 1 az egységelem.

## Tétel

Egy $p > 1$ egész szám pontosan akkor prímszám, ha $a, b \in \mathbb{Z}$ esetén $p|ab$ teljesülése $p|a$ vagy $p|b$ fennállását vonja maga után.

## Tétel – a számelmélet alaptétele

Minden 1-nél nagyobb természetes szám felbontható véges sok prímszám szorzatára, és a felbontás a tényezők sorrendjétől eltekintve egyértelmű. A tételből adódó egyértelmű szorzatot a természetes számok kanonikus vagy prímtényezős alakjának nevezzük, formája: $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, ahol $p_1, p_2, \dots, p_r$ páronként különböző prímek, $\alpha_1, \alpha_2, \dots, \alpha_r \in \mathbb{N}$.

# Osztók száma

## Tétel

Egy $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ kanonikus alakú természetes szám pozitív osztóinak a száma

$$d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_r + 1).$$

Példa: $\underline{1260} = 2^2 \cdot 3^2 \cdot 5 \cdot 7$ és $14850 = 2 \cdot 3^3 \cdot 5^2 \cdot 11$

| | |
|---|---|
| 1260 | 2 |
| 630 | 5 |
| 126 | 2 |
| 63 | 3 |
| 21 | 3 |
| 7 | 7 |
| 1 | |

0,1,2    0,1,2    0,1    0,1

$$2^{\square} \cdot 3^{\square} \cdot 5^{\square} \cdot 7^{\square}$$

$\Rightarrow 3 \cdot 3 \cdot 2 \cdot 2 = 36$ osztó

Pl:

$2^0 \cdot 3^0 \cdot 5^0 \cdot 7^0 \longrightarrow 1$

$2^1 \cdot 3^2 \cdot 5^0 \cdot 7^0 \longrightarrow 18$

$1260 = 2^2 \cdot 3^2 \cdot 5 \cdot 7$

Hány ps osztója van?

$$\overset{\cancel{0},1,2}{2^{\sqcup}} \cdot \overset{0,1,2}{3^{\sqcup}} \cdot \overset{0,1}{5^{\sqcup}} \cdot \overset{0,1}{7^{\sqcup}} \qquad 2 \cdot 3 \cdot 2 \cdot 2 = 24 \text{ db}$$

Ptn

$$2^0 \cdot 3^{\sqcup} \cdot 5^{\sqcup} \cdot 7^{\sqcup} \qquad 3 \cdot 2 \cdot 2 = 12 \text{ db}$$

ami a 15-tel relatív prím

$$\overset{0,1,2}{2^{\sqcup}} \cdot 3^0 \cdot 5^0 \cdot \overset{0,1}{7^{\sqcup}} \qquad 3 \cdot 2 = 6 \text{ db}$$

## Példa lnko lkkt

Határozzuk meg $(1260, 14850)$ és $[1260, 14850]$ értékét.

$1260 = 2^2 \cdot 3^2 \cdot 5 \cdot 7$ és $14850 = 2 \cdot 3^3 \cdot 5^2 \cdot 11$

**legnagyobb közös osztó:** vegyük a közös prímtényezőket, az előforduló kisebb hatványon.

$1260 = 2^2 \cdot 3^2 \cdot 5^1 \cdot 7$ and $14850 = 2^1 \cdot 3^3 \cdot 5^2 \cdot 11$

$(1260, 14850) = 2^1 \cdot 3^2 \cdot 5^1 = 90$

**legkisebb közös többszörös:** vegyük az összes előforduló prímtényezőt, a nagyobb hatványon

$1260 = 2^2 \cdot 3^2 \cdot 5 \cdot 7^1$ and $14850 = 2 \cdot 3^3 \cdot 5^2 \cdot 11^1$

$[1260, 14850] = 2^2 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11 = 207900$

**Tétel**

A prímszámok száma végtelen.

*Biz.:* Indirekt módon tegyük fel, hogy véges sok prímszám van, legyenek ezek $p_1, p_2, \ldots, p_k$. Tekintsük a $\boxed{b = p_1 \cdot p_2 \cdot \cdots \cdot p_k + 1}$ számot. Ekkor $b \neq 1$ és $b$ összetett szám, azaz valamely $i \in \{1, 2, \ldots, k\}$ indexre $p_i | b$. Azonban $p_i | \prod p_j$ is, így $p_i | 1$, ami ellentmondás.

**Megjegyzés**

Az $a$ és $b$ egészek relatív prímek, ha kanonikus alakjukban nincsenek közös prímtényezők.

# Kongruenciák

Legyen $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$.

**Definíció**

Azt mondjuk, hogy *$a$ kongruens $b$-vel modulo $m$*, ha $m | (a - b)$.
Jele: $a \equiv b \pmod{m}$, $m$: a *kongruencia modulusa*

Példa: $m = 4$ esetén $3 \equiv 11 \pmod{4}$

Azok az $a, b \in \mathbb{Z}$ számok kongruensek modulo $m$, amelyek az $m$-mel való osztáskor ugyanazt a maradékot adják.

**Tétel**

A mod $m$ kongruencia ekvivalenciareláció: reflexív, szimmetrikus, tranzitív.

$\rightsquigarrow$ a mod $m$ kongruencia osztályozást indukál, egy osztályban az egymással kongruens számok vannak.

**Definíció**

A mod $m$ kongruencia által indukált osztályokat *maradékosztályok*nak nevezzük. A maradékosztályok *reprezentánsai*: $0, 1, \ldots, m-1$. Azaz mod $m$ a kapott maradékosztályok száma $m$.

$2 \equiv 7 \pmod 5$ $\qquad$ $13 \equiv 28 \pmod 5$

$5 \mid (2-7)$ $\qquad$ $5 \mid (13-28)$

---

$m = 5$

0: $\{ \ldots, -10, -5, 0, 5, 10, 15, \ldots \}$

1: $\{ \ldots, -9, -4, 1, 6, 11, 16, \ldots \}$

2: $\{ , -8, -3, 2, 7, 12, 17, \ldots \}$

3: $\{ \ldots, -7, -2, 3, 8, 13, 18, \ldots \}$

4: $\{ \ldots, -6, -1, 4, 9, 14, 19, \ldots \}$

# A kongruencia tulajdonságai

## Állítás – a kongruencia tulajdonságai

Legyen $m \in \mathbb{N}$ $(m \geq 2)$ és $a, b, c, d \in \mathbb{Z}$.

1. Ha $a \equiv b$ és $c \equiv d \pmod{m}$, akkor

$$a \pm c \equiv b \pm d \pmod{m} \qquad \text{és} \qquad a \cdot c \equiv b \cdot d \pmod{m}.$$

2. Ha $a \cdot c \equiv b \cdot c \pmod{m}$ és $(c, m) = 1$, akkor $a \equiv b$.

Példa: $15 \equiv 63 \pmod{8}$ és $10 \equiv 18 \pmod{8}$

## Definíció

Az $a_1, a_2, \ldots, a_m$ szám $m$-est teljes reprezentáns rendszernek nevezzük, ha mindegyik maradékosztályból pontosan 1 fordul elő közöttük, azaz

$$a_i \not\equiv a_j \pmod{m}, \text{ ha } i \neq j.$$

Példa: $m = 5$ esetén: 5, 6, 12, 28, 9

## Állítás

Ha $a \equiv b \pmod{m}$, akkor $(a, m) = (b, m)$.

$a \equiv b \pmod{m}$ és $c \equiv d \pmod{m}$ $\Longrightarrow$

$$a+c \equiv b+d \pmod{m}$$
$$a-c \equiv b-d \pmod{m}$$

$m \mid (a-b)$ és $m = (c-d)$

$$m \mid a+c-(b+d) = \underbrace{(a-b)}_{m\mid} + \underbrace{(c-d)}_{m!}$$

$12 \equiv 17 \pmod{5}$ $\qquad$ $1 \equiv 11 \pmod{5}$

$$12+1 \equiv 17+11 \pmod{5}$$

ha $a \cdot c \equiv b \cdot c \pmod{m}$

és $(c, m) = 1 \implies a \equiv b \pmod{m}$

$m \mid (ac - bc)$

$m \mid c \cdot (a - b)$

mivel $(m, c) = 1$

ezért

$m \mid a - b$

$a \equiv b \pmod{m}$

$24 \equiv 9 \pmod{5}$

$\underset{c}{\underline{3}} \cdot \underset{a}{8} \equiv \underset{c}{\underline{3}} \cdot \underset{b}{3} \pmod{5}$

$8 \equiv 3 \pmod{5}$

# Redukált maradékosztályok

## Definíció

Egy maradékosztályt a redukált maradékrendszer eleménak, vagy redukált maradékosztálynak nevezünk, ha elemei relatív prímek a modulushoz.
Jele: a mod $m$ redukált maradékosztályok számát $\varphi(m)$-mel jelöljük.
Tehát
$$\varphi(m) = \#\{a \in \{1, \dots, m\} \mid (a, m) = 1\}.$$
A $\varphi$ függvény neve: Euler-féle $\varphi$-függvény.

A definícióból adódik, hogy $\varphi(1) = 1$.
A maradékosztályok száma „kis” pozitív egészekre:

| $m$ | teljes | redukált | $\varphi(m)$ |
|---|---|---|---|
| $m = 2$ | 0,1 | 1 | $\varphi(2) = 1$ |
| $m = 3$ | 0,1,2 | 1,2 | $\varphi(3) = 2$ |
| $m = 4$ | 0,1,2,3 | 1,3 | $\varphi(4) = 2$ |
| $m = 5$ | 0,1,2,3,4 | 1,2,3,4 | $\varphi(5) = 4$ |
| $m = 6$ | 0,1,2,3,4,5 | 1,5 | $\varphi(6) = 2$ |
| $m = 7$ | 0,1,2,3,4,5,6 | 1,2,3,4,5,6 | $\varphi(7) = 6$ |

# Az Euler-féle $\varphi$-függvény

## Állítás

Ha $p$ prím, akkor $\varphi(p) = p - 1$.

## Tétel

Az Euler-féle $\varphi$-függvény értéke (azaz a redukált maradékosztályok száma) kiszámolható a

$$\varphi(m) = m \cdot \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$

képlettel, ha $m$ prímtényezős alakja $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$.

Példa: $m = 24$, $\varphi(24) = ?$

$24 = 2^3 \cdot 3$

$$\varphi(24) = 24 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 24 \cdot \frac{1}{2} \cdot \frac{2}{3} = 8$$

## Tétel – Euler–Fermat-tétel

Ha $(a, m) = 1$, akkor $a^{\varphi(m)} \equiv 1 \pmod{m}$.

## Következmény – kis Fermat-tétel

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

Példa: 15-tel való osztáskor mennyi a $2^{2019}$ maradéka?

$$2^{2019} \equiv ? \pmod{15} \qquad (2, 15) = 1$$

$$2^{\varphi(15)} \equiv 1 \pmod{15}$$

$$15 = 3 \cdot 5 \Rightarrow \varphi(15) = 15 \cdot \underbrace{\left(1 - \frac{1}{3}\right)}_{\frac{2}{3}} \underbrace{\left(1 - \frac{1}{5}\right)}_{\frac{4}{5}} = 8$$

$$2^8 \equiv 1 \pmod{15}$$

$$2019 = 252 \cdot 8 + 3$$

$$2^{2019} = \underbrace{2^3}_{8} \cdot \Big(\underbrace{2^8}_{15N+1}\Big)^{252}$$

15-tel osztva 1 maradékot ad

$$2^{2019} \equiv 8 \pmod{15}$$

# Kongruencia egyenletek

**Tétel**

Az $ax \equiv b \pmod{m}$ (lineáris) kongruencia egyenlet pontosan akkor oldható meg az egész számok körében, ha $(a, m)|b$.

*Biz.:* visszavezetjük a feladatot egy lineáris diofantikus egyenletre:

$$ax \equiv b \pmod{m} \;\Leftrightarrow\; m|(ax - b) \;\Leftrightarrow$$
$$\Leftrightarrow\; \exists y \in \mathbb{Z}:\; my = ax - b \;\Leftrightarrow\; \boxed{ax - my = b}$$

Megjegyzés: ha az egyenletnek $c \in \mathbb{Z}$ egy megoldása, akkor $c + km$ is az.

Példa: $12x \equiv 8 \pmod{16}$

$(12, 16)|8 \quad \Longrightarrow$ az egyenlet megoldható

$4 \mid 8$ végtelen sok megoldás

## Példa

Oldjuk meg a $12x \equiv 8 \pmod{16}$ lineáris kongruenciát.

$(12,16) = 4|8 \quad \Longrightarrow$ az egyenlet megoldható

**1. módszer**:
oldjuk meg a $12x - 16y = 8$ (azaz $3x - 4y = 2$) diofantikus egyenletet.

**2. módszer**:
Tekintsük a $\frac{12}{(12,16)}x \equiv \frac{8}{(12,16)} \pmod{\frac{16}{(12,16)}}$ egyenletet
Ekkor

$$\begin{aligned} 3x &\equiv 2 \pmod{4} \\ \underset{\cdot}{3}x &\equiv 2+4 = \underset{\cdot}{6} \pmod{\underset{\cdot}{4}} \\ x &\equiv 2 \pmod{4} \qquad (\text{mert } (3,4)=1) \end{aligned}$$

A megoldások:

$$x = \ldots, -10, -6, -2, 2, 6, 10, \ldots$$

$5x \equiv 24 \pmod{13}$

megoldható, mert $(5,13) \mid 24$

$5x \equiv \overset{24+2\cdot 13}{50} \pmod{13}$

mivel $(5,13) = 1$

$x \equiv 10 \pmod{13}$

$x$: $-16, -3, 10, 23, 36,$

---

$14x \equiv 8 \pmod{21}$

$(14,21) = 7 \nmid 8 \Rightarrow$ nem megoldható

?? $21 \mid 14x-8$

$$22x \equiv 24 \pmod{36}$$

$(22, 36) = 2 \mid 24 \implies$ megoldható

$$11x \equiv 12 \pmod{18}$$

$$11x \equiv \underset{\substack{\uparrow \\ 12+3\cdot 18}}{66} \pmod{18}$$

$(11, 18) = 1 \implies \qquad x \equiv 6 \pmod{18}$

$\left[\; 18 \mid (11x-66) = 11(x-6) \implies \qquad 18 \mid x-6 \;\right]$

$17^{18}$ 40-nel osztva mennyi maradékot ad?

$$a^{\varphi(m)} \equiv 1 \pmod{m} \quad \text{ha} \quad (a,m)=1$$

$$17^{\varphi(40)} \equiv 1 \pmod{40}$$

$40 = 2^3 \cdot 5$

$$\varphi(40) = 40 \cdot \left(1-\frac{1}{2}\right)\cdot\left(1-\frac{1}{5}\right) = 40\cdot\frac{1}{2}\cdot\frac{4}{5} = 16$$

$$17^{16} \equiv 1 \pmod{40}$$

$$17^{18} = 17^{16}\cdot 17^2$$

$$17^{18} \equiv \underset{289}{17^2} \pmod{40} \qquad 17^{18} \equiv 9 \pmod{40}$$