Számelméleti alapfogalmak

1. A maradékos osztás tétele

Legyen *a* és *b* két természetes szám, $b \neq 0$, és a>b. Akkor egyértelműen léteznek *q* és *r* természetes számok, amelyekre igaz: $a = b \cdot q + r$, $0 \leq r < b$.

Megnevezés: *a* – osztandó
b – osztó
q – hányados
r – maradék.

Például: minden természetes szám felírható: **1)** 2k vagy 2k+1 alakban **2)** 3k, 3k+1, 3k+2 alakban, **3)** 4k, 4k+1, 4k+2, 4k+3 alakban és így tovább

2. Az oszthatóság értelmezése

Ha a fenti kijelentésben $r = 0,\ akkor\ a = b \cdot q$. Ekkor *b*-t az *a osztójá*nak nevezzük.

Jelölés: $b|a$ „*b osztja a-t*”, vagy $a \vdots b$ „*a osztható b-vel*”, vagy $b \in D_a$ „*b* eleme *az a osztói* halmazának”.

A fenti értelmezést úgy is olvashatjuk, hogy *a többszöröse b-nek*.

Jelölés: Azt a tényt, hogy *a* többszöröse *b*-nek, így is jelölik: $a = M \cdot b$.

A *b* szám többszöröseinek halmazát. M_b-vel jelöljük.

Tehát ha *a* és *b* esetén $\exists\ q\ úgy,\ hogy:\ a = b \cdot q$, akkor *b* osztója *a*-nak, illetve *a* többszöröse *b*-nek ($a, b, q \in N, b \neq 0$).

3. Az oszthatóság tulajdonságai

1.) Az oszthatósági reláció rendezési reláció, mégpedig reflexív rendezési reláció.

$\forall a \in N^*,\ a|a$

$Ha\ \ a|b\ \ és\ \ b|a\ \Rightarrow a = b$

$Ha\ \ a|b\ \ és\ \ b|c\ \Rightarrow a|c$

A fenti tulajdonságok rendre: reflexivitás, antiszimmetria, tranzitivitás.

2.) A 0-nak minden nemnulla természetes szám osztója ($0 \vdots a,\ a \in N^*$).

3.) $a \vdots 1,\ \forall a \in N$ esetén.

4.) (additív tulajdonság) Ha $a|b\ \ és\ \ a|c\ \Rightarrow a|(b+c)$.

5.) $Ha\ c|a\ és\ c|b \Rightarrow c|(ax+by)$, ahol *x* és *y* tetszőleges természetes számok (additív és multiplikatív tulajdonság együttesen).

4. Oszthatósági kritériumok (szabályok)

Megjegyzés:
Az oszthatósági kritériumok igazolásánál a következő (előzőkben már felsorolt) tulajdonságokra alapozunk:
-Ha egy összeg minden tagja osztható egy számmal, akkor az összeg is osztható a számmal.
-Ha egy szorzat egyik tényezője osztható egy számmal, akkor a szorzat is osztható a számmal.
-Ha egy szám osztható egy másikkal, akkor a szám az utóbbi szám minden osztójával osztható.

(1) A 10-zel való oszthatóság kritériuma

$a \vdots 10^k \Leftrightarrow$ ha az *a* szám legalább *k* db. nullában végződik.

(2)A 2-vel, ill. 5-tel való oszthatóság kritériuma

$\left.\begin{array}{l} a \vdots 2 \\ a \vdots 5 \end{array}\right\} \Leftrightarrow$ ha az *a* szám utolsó számjegye osztható 2-vel, ill. 5-tel.

Bizonyítás
Az *a* szám felírható összeg-alakban 10 hatványai szerint:

$$a = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$$

A felírásból látható, hogy az összeg az utolsó tagig osztható 10-zel, vagyis 2-vel is és 5-tel is. Tehát ha az a_0 is osztható 2-vel, illetve 5-tel, akkor az *a* szám is osztható lesz.

(3) A 4-gyel, illetve25-tel való oszthatóság kritériuma

Egy szám akkor és csakis akkor osztható 4-gyel, illetve 25-tel, ha az utolsó két számjegyéből alkotott kétjegyű szám osztható 4-gyel, ill. 25-tel.

Bizonyítás

$$a = \underbrace{a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... + a_3 \cdot 10^3 + a_2 \cdot 10^2}_{\vdots 4,\ \vdots 25} + \underbrace{a_1 \cdot 10 + a_0}_{\text{az utolsó két szj.–ből alkotott sz.}}$$

Tehát, ha $\overline{a_1 a_0} \vdots 4$, *továbbá* $\overline{a_1 a_0} \vdots 25$, akkor az *a* is osztható 4-gyel, ill. 25-tel.

(4)A 8-cal, ill. 125-tel való oszthatóság kritériuma

Egy szám akkor és csakis akkor osztható 8-cal, illetve 125-tel, ha az utolsó három számjegyéből alkotott háromjegyű szám osztható 8-cal, ill. 125-tel.
(A bizonyítása az előzőhöz hasonló.)

(5)A 3-mal, ill. 9-cel való oszthatóság kritériuma

Ha egy számban a számjegyek összege osztható 3-mal, ill. 9-cel, akkor a szám is osztható 3-mal, ill. 9-cel.

Bizonyítás

$10^k = \underbrace{99...9}_{k\ db.} + 1$. Az a szám felbontásában 10 hatványait ilyen formában írjuk:

$$a = a_n \cdot (\underbrace{99...9}_{n\ db.} + 1) + a_{n-1} \cdot (\underbrace{99...9}_{n-1\ db.} + 1) + ... + a_3 \cdot (999+1) + a_2 \cdot (99+1) + a_1 \cdot (9+1) + a_0 =$$

$$= \underbrace{a_n \cdot 99...9 + a_{n-1} \cdot 99...9 + ... + a_3 \cdot 999 + a_2 \cdot 99 + a_1 \cdot 9}_{\vdots 3,\ \vdots 9} + \underbrace{a_n + a_{n+1} + ... + a_3 + a_2 + a_1 + a_0}_{a\ számjegyek\ összege}$$

Tehát $\left.\begin{matrix} a \vdots 3 \\ a \vdots 9 \end{matrix}\right\} \Leftrightarrow ha\ a\ számjegyek\ összege \vdots 3,\ ill.\ \vdots 9$.

(6) A 11-gyel való oszthatóság kritériuma

Egy szám akkor és csakis akkor osztható 11-gyel, ha váltakozó előjellel vett számjegyeinek összege osztható 11-gyel., az összeg felírását az egyesektől kell kezdeni.

Bizonyítás

$10 = 1 \cdot 11 - 1 \qquad 100 = 9 \cdot 11 + 1 \qquad 1000 = 91 \cdot 11 - 1 \qquad 10000 = 909 \cdot 11 + 1$

$$általánosítva: \begin{cases} 10^k = M11 + 1,\ ha\ k\ páros \\ 10^k = M11 - 1,\ ha\ k\ páratlan \end{cases}$$

$$Tehát\ a = a_0 + a_1 \cdot (M11 - 1) + a_2 \cdot (M11 + 1) + a_3 \cdot (M11 - 1) + ... + a_n \cdot (M11 + (-1)^n) =$$

$$= M11 + (a_0 - a_1 + a_2 - a_3 + ... \pm a_n)$$

A zárójelben tehát a számjegyek váltakozó előjellel vett összege van. Ez az összeg az egyesek számjegyével kezdődik, amely mindig pozitívként szerepel.

Pl. 70 521 osztható 11-gyel, mert 1 – 2 +5 – 0 + 7 =11, ami osztható 11-gyel.

(7) A 7-tel, 11-gyel, 13-mal való oszthatóság kritériuma

A kritériumot először magyarázzuk, majd példán mutatjuk be. A megfogalmazása elég körülményes.

A bizonyításhoz tudni kell, hogy $1001 = 7 \cdot 11 \cdot 13$.

Az *a* számot így írjuk:

$$a = \overline{a_n a_{n-1} ... a_3 a_2 a_1 a_0} = \overline{a_n a_{n-1} ... a_3} \cdot 1000 + \overline{a_2 a_1 a_0} = \overline{a_n a_{n-1} ... a_3} \cdot (1001 - 1) + \overline{a_2 a_1 a_0} =$$

$$= \underbrace{\overline{a_n a_{n-1} ... a_3} \cdot 1001}_{\vdots 7,\ \vdots 11,\ \vdots 13} - \overline{a_n a_{n-1} ... a_3} + \overline{a_2 a_1 a_0}$$

Tehát, ha a $-\overline{a_n a_{n-1} ... a_3} + \overline{a_2 a_1 a_0}$ algebrai összeg osztható 7-tel, 11-gyel, 13-mal, akkor maga a szám is osztható ezekkel.

Pl. a 70 521 esetében

– 70 + 521 = 451, 451 osztható 11-gyel, tehát a 70 521 szám is osztható 11-gyel (mint azt az előző esetben is láttuk).

451 nem osztható sem 7-tel, sem 13-mal, tehát a 70 521 sem osztható ezekkel.

Pl. 59 488
488 – 59 = 429 $\quad 429 \not\vdots 7,\ 429 \vdots 11,\ 429 \vdots 13 \Rightarrow 59488 \not\vdots 7,\ 59488 \vdots 11,\ 59488 \vdots 13.$

5.Prímszámok
-Minden, nullától különböző természetes szám osztható 1-gyel és önmagával.
Ezeket a szám *nem valódi (triviális) osztó*inak nevezzük.
Minden, ezektől különböző osztót, *valódi osztó*nak nevezünk.
- D_a jelöli az *a* természetes szám természetes *osztóinak halmazá*t.
-Ha egy $a \neq 0,\ a \in N$ *esetén* $a = b \cdot c,$ akkor *b*-t és *c*-t az *a* szám *társosztó*inak nevezzük.
Megjegyzés
Ha meg kell határozni D_a elemeit, érdemes kéttőnként: a társosztókat felsorakoztatni, „amíg találkoznak”.
Pl.
$D_{24} = \{1,2,3,4,\ 6,8,12,24\}$. Tehát így töltjük ki a halmazt: 1 és 24, 2 és 12, 3 és 8, 4 és 6.
Értelmezés
- Azokat a 0-tól és 1-től különböző számokat, amelyeknek nincs valódi osztójuk, ***prímszámoknak (törzsszámok***nak) nevezzük.
Értelmezés
- Az összes olyan 0-tól és 1-től különböző számot, amely nem prímszám, ***összetett szám***nak nevezzük.

Tehát a természetes számok az osztóik száma szerint lehetnek:
- csak 1 db. osztója van: 1
- végtelen sok osztója van: 0
- csak két osztója van: az 1 és önmaga = prímszám (2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, …)
- kettőnél több osztójuk van: összetett számok.

***Fontos tulajdonság*:**
Ha egy szorzat osztható egy prímszámmal, akkor a szorzat egyik tényezője legalább osztható ezzel a prímszámmal.
(A tulajdonság nem érvényes, ha az osztó nem prímszám.)
Pl. $7 \mid 8 \cdot 21, \Rightarrow 7 \mid 8,$ *vagy* $7 \mid 21.$ *Az utóbbi igaz.*
de: $6 \mid 8 \cdot 21,$ *mégis* $8 \not\vdots 6$ *és* $21 \not\vdots 6.$
mert a 6 nem prím.

Tétel (a számelmélet alaptétele)
Minden összetett szám, a tényezők sorrendjétől eltekintve, felbontható egyértelműen véges sok prímszám szorzatára, vagyis léteznek olyan $p_1,\ p_2, \ldots,\ p_k$ különböző prímszámok és $\alpha_1,\ \alpha_2, \ldots,\ \alpha_k$ hatványkitevők amelyekre $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$

Tétel **(Euklidész, i.e. 300)**
Végtelen sok prímszám van.

Bizonyítás
Feltételezzük az ellenkezőjét, hogy csak véges darab prímszám van, ezek: $p_1, p_2, ..., p_k$.
Képezzük a $p = p_1 \cdot p_2 \cdot ... \cdot p_k + 1$ számot. Ez nem osztható $p_1, p_2, ..., p_k$ egyikével sem (más prímszám nincs), tehát ez egy újabb prímszám lenne, ami ellentmondás.

***Érdekesség*:**
Bár végtelen sok prímszám van, mégis, igazolható, hogy megadható tetszőlegesen sok egymásutáni szám, melynek mindenike összetett. Vagyis a prímszámok között tetszőlegesen nagy „lyukak” is vannak.
(Igazolás
$n! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot ... \cdot n$ szám soha nem prím (n>2).
De $(n+1)!+2$ összetett, mert osztható 2-vel
$(n+1)!+3$ összetett, mert osztható 3-mal.
$(n+1)!+4$ összetett, mert osztható 4-gyel.
és így tovább…
$(n+1)!+n+1$ is összetett.
Ilyenformán pontosan *n* db egymásutáni összetett számot soroltunk föl.)

Példa prímtényezőkre való bontásra:
120|2·5
12|2
6|2
3|3
1|
$120 = 2^3 \cdot 3 \cdot 5$
Egy szám összes osztóinak a száma:
Ha $n = p_1^{s_1} \cdot p_2^{s_2} \cdot ... \cdot p_k^{s_k}$, akkor az osztók száma: $\tau(n) = (s_1 + 1) \cdot (s_2 + 1) \cdot ... \cdot (s_k + 1)$.

Az összes osztó megkeresése
a.) társosztók fölírásával
Az osztók száma:
420|2·5
42|2
21|3
7|7
1|

$420 = 2^2 \cdot 3 \cdot 5 \cdot 7$
$\tau(420) = (2+1) \cdot (1+1) \cdot (1+1) \cdot (1+1) = 3 \cdot 2 \cdot 2 \cdot 2 = 24$

$D_{420} = \{1,2,3,4,5,6,7,10,12,14,15,20, \quad 21,28,30,35,42,60,70,84,105,140,210,420\}$
b.) a tényezőre bontásból, kipárosítva:

$420 = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 7$

$$\left.\begin{array}{ll} 1,2,3,5,7 & 5\ db \\ 2\cdot 2, 2\cdot 3, 2\cdot 5, 2\cdot 7, 3\cdot 5, 3\cdot 7, 5\cdot 7 & 7\ db \\ 2\cdot 2\cdot 3, 2\cdot 2\cdot 5, 2\cdot 2\cdot 7, 2\cdot 3\cdot 5, 2\cdot 3\cdot 7, 2\cdot 5\cdot 7, 3\cdot 5\cdot 7 & 7\ db \\ 2\cdot 2\cdot 3\cdot 5, 2\cdot 2\cdot 3\cdot 7, 2\cdot 2\cdot 5\cdot 7, 2\cdot 3\cdot 5\cdot 7 & 4\ db \\ 2\cdot 2\cdot 3\cdot 5\cdot 7 & 1\ db \end{array}\right\} ö = 24\ db$$

6.Közös osztók. Legnagyobb közös osztó

Két, vagy több szám *közös osztó*inak halmaza egyenlő az osztóik halmazának metszetével.

Pl. $D_{24} = \{1,2,3,4,6,8,12,24\}$

$D_{36} = \{1,2,3,4,6,9,12,18,36\}$

$D_{42} = \{1,2,3,6,7,14,21,42\}$

24 és 36 közös osztói: $D_{24} \cap D_{36} = \{1,2,3,4,6,12\}$

24 és 42 közös osztói: $D_{24} \cap D_{42} = \{1,2,3,6\}$

24, 36 és 42 közös osztói: $D_{24} \cap D_{36} \cap D_{42} = \{1,2,3,6\}$

A közös osztók halmaza véges, mert maga az osztók száma is véges.
Tehát ebben a halmazban van legnagyobb elem, ez a **ln.k.o.**

Pontosan:

Két, *a* és *b* szám ln.k.o.-ja az a *d* szám, amellyel mind a két szám osztható, és az *a* és *b* számok minden más osztója osztja a ln.k.o.-t.

Jelöléssel:

Ha *d = (a, b)*, akkor

(1) $d|a$ *és* $d|b$

(2) *ha* $d_1 \in N$, $d_1|a$ *és* $d_1|b \Rightarrow d_1|d$

Tehát a fenti példánál: (24, 36) = 12, (24, 42) = 6, (24, 36, 42) = 6.

A ln.k.o. meghatározása prímtényezőkre bontással:

-csak a közös tényezők és azok a legkisebb hatványon.

Pl. $24 = 2^3 \cdot 3$ $\quad (24,36) = 2^2 \cdot 3 = 12$

$36 = 2^2 \cdot 3^2$ $\quad (24,42) = 2 \cdot 3 = 6$

$42 = 2 \cdot 3 \cdot 7$ $\quad (24,36,42) = 2 \cdot 3 = 6$

A ln.k.o. meghatározása (két szám esetén) Euklideszi-algoritmussal:

Legyen *a*> *b*, a maradékos osztás tétele szerint rendre felírhatók, hogy:

$a = bq_1 + r_1$, $b = r_1 q_2 + r_2$, $r_1 = r_2 q_3 + r_3$,…, $r_{n-2} = r_{n-1} q_n + r_n$, $r_{n-1} = r_n q_{n+1}$.

Ekkor $(a,b) = r_n$.

Az algoritmus szavakban: a nagyobbik számot osztjuk a kisebbikkel, aztán az osztó osztva az előző osztás maradékával, míg a maradék 0 lesz. Az utolsó 0-tól különböző maradék lesz a ln.k.o.

Pl. $\underline{42} : 24 = 1$ $\quad \underline{24} : 18 = 1$ $\quad \underline{18} : 6 = 3$

$18 \qquad = 6 \qquad ==$

Itt a ln.k.o.= (36, 24) = 6.

Pl. (720,500) = ?

Törzstényezőkre bontással:

$$\begin{array}{r||l} 720 & 2\cdot 5 \\ 72 & 2 \\ 36 & 2 \\ 18 & 2 \\ 9 & 3 \\ 3 & 3 \\ 1 & \end{array} \qquad \begin{array}{r||l} 500 & 2\cdot 5 \\ 50 & 2\cdot 5 \\ 5 & 5 \\ 1 & \end{array}$$

$$720 = 2^4 \cdot 3^2 5$$
$$500 = 2^2 \cdot 5^3$$
$$\overline{(720,500) = 2^2 \cdot 5 = 20}$$

Euklideszi-algoritmussal:

$\underline{720} : 500 = 1$ $\quad \underline{500} : 220 = 2$ $\quad \underline{220} : 60 = 3$ $\quad \underline{60} : 40 = 1$ $\quad \underline{40} : 20 = 2$

$220 \qquad = 60 \qquad = 40 \qquad 20 \qquad ==$

Megjegyzés

Ha több szám ln.k.o.-ját akarjuk meghatározni Euklideszi-algoritmussal, akkor a két szám ln.k.o.-ját visszük be az algoritmusba a harmadik számmal, és így tovább.

Értelmezés

Ha két szám ln.k.o.-ja 1, akkor a számokat ***relatív prím számok***nak (*viszonylagos törzsszámok*nak) nevezzük.

Pl. 15 és 22

De 15, 22 és 91 is relatív prímek. Ezek páronként is relatív prímek, mert (15, 22) = 1, (15, 91) = 1, (22, 91) = 1, míg külön-külön egyik sem prím. (15 = 3 · 5, 22 = 2 · 11, 91 = 7 · 13.)

7.Közös többszörösök. Lk.k.t.

Két szám *közös többszöröseinek* a halmaza egyenlő a többszörösök halmazának a metszetével.

Pl. $M_6 = \{6,12,18,24,30,36,42,48,54,60,66,...\}$

$M_8 = \{8,16,24,32,40,48,56,64,72,...\}$

$M_6 \cap M_8 = \{24,48,72,...\}$

A közös többszörösök halmaza végtelen. Van legkisebb eleme. Ez a ***lk.k.t.***

Jelen esetben [6, 8] = 24 (a 6 és a 8 legkisebb közös többszöröse a 24).

Tehát a lk.k.t. a közös többszörösök közül a legkisebb.

Pontosabban:
A lk.k.t. mind a két számnak a többszöröse és a számnak minden többszöröse a lk.k.t.-nek is többszöröse.
Jelöléssel: Ha m = [a,b], akkor:
(1) $m \vdots a$ *és* $m \vdots b$
(2) *ha pedig* $m_1 \vdots a,\ \ m_1 \vdots b \Rightarrow m_1 \vdots m$

A lk.k.t. meghatározása tényezőre bontással:
Pl. $[6,8] = 24,\ mert\ 6 = 2 \cdot 3$

$$\begin{array}{l} 8 = 2^3 \\ \hline [6,\ 8] = 2^3 \cdot 3 = 24 \end{array}$$

A lk.k.t.meghatározása a ln.k.o. segítségével:

Számelméleti tétel:

$$(a,b) \cdot [a,b] = a \cdot b \qquad \Rightarrow \qquad [a,b] = \frac{a \cdot b}{(a,b)}$$

A tétel szerint: $[6,8] = \dfrac{6 \cdot 8}{(6,8)} = \dfrac{48}{2} = 24, \qquad (6,8) = 2$.

Más pl.

$$\begin{array}{l} 720 = 2^4 \cdot 3^2 \cdot 5 \\ 500 = 2^2 \cdot 5^3 \\ \hline [720.500] = 2^4 \cdot 3^2 \cdot 5^3 = 1000 \cdot 18 = 18000 \end{array}$$

A tétel alapján: $[720,500] = \dfrac{720 \cdot 500}{20} = 18000$

Diofantikus egyenletek megoldása

Az $ax + by = c$ **egyenlet megoldása a Z×Z halmazon**

1. <u>Tétel:</u>
Az $ax + by = c$ egyenletnek ha van megoldása a Z×Z halmazon, akkor $(a,b) = d \,|\, c$.
Bizonyítás:
Ha x_0, y_0 megoldás, akkor $ax_0 + by_0 = c$. De $d \,|\, a$ és $d \,|\, b$, ezért $d \,|\, ax_0 + by_0 = c$ vagyis $d \,|\, c$

2. <u>Tétel:</u>
Legyen $(a,b) = 1$. Az $ax + by = c$ egyenlet összes egész megoldása $x = x_0 + bt$ és $y = y_0 - at$ y, ahol $t \in Z$ és $x_0, y_0 \in Z$ az egyenlet egy partikuláris megoldása.

Bizonyítás:

1) Igazoljuk, hogy $x = x_0 + bt$ és $y = y_0 - at$ megoldás.

   Valóban, $ax + by = a(x_0 + bt) + b(y_0 - at) = ax_0 + by_0 = c$

2) Igazoljuk, hogy minden egész megoldás $x = x_0 + bt$ és $y = y_0 - at$ alakú.

Mivel $ax + by = c$ és $ax_0 + by_0 = c$, ezért $a(x - x_0) + b(y - y_0) = 0$ ahonnan $a(x - x_0) = -b(y - y_0)$, tehát $b \mid a(x - x_0)$ és $a \mid b(y - y_0)$. De $(a,b) = 1$, ezért $b \mid (x - x_0)$ és $a \mid (y - y_0)$, ezért létezik olyan $t \in Z$ amelyre $x - x_0 = bt$ és így $y - y_0 = -at$, tehát $x = x_0 + bt$ és $y = y_0 - at$.

Pl:

Oldjuk meg az egész számok halmazán a $2x + 3y = 12$ egyenletet.

1. Megoldás:

Kifejezzük a kisebbik együtthatójú ismeretlent: $2x = 12 - 3y$ ahonnan $x = \frac{12 - 3y}{2} = 6 - \frac{3y}{2} = 6 - y - \frac{y}{2} \in Z$ kell legyen, ezért $y = 2k$ és így $x = 6 - 2k - k$ tehát $x = 6 - 3k$ ahol $k \in Z$. Tehát végtelen sok megoldás van!

2. Megoldás:

Észrevehető, hogy $x_0 = 3$ és $y_0 = 2$ megoldása az egyenletnek. A tétel értelmében $x = x_0 + bt = 3 + 3t$ és $y = y_0 - at = 2 - 2t$ ahol $t \in Z$.

Megjegyzések:

1) Bár a megoldások különböző alakúak, mégis ugyanazokaz a számokat származtatják.
2) A természetes megoldások csak: *x= 3, y= 2 ; x=0, y= 4; x=6, y=0.*