3. Oszthatóság, oszthatósági szabályok és tételek. Prímszámok. Számrendszerek

Vázlat:

I. Számelméleti alapfogalmak: osztó, többszörös, oszthatóság fogalma, tulajdonságai, oszthatósági szabályok
II. Prímszám, összetett szám, számelmélet alaptétele, osztók száma
III. Legnagyobb közös osztó, legkisebb közös többszörös
IV. Számrendszerek
V. Alkalmazások, matematikatörténeti vonatkozások

Kidolgozás:

I. Oszthatóság

Az oszthatóság fogalmánál alaphalmaznak az egész számok halmazát tekintjük. Két egész szám hányadosa nem mindig egész szám, az oszthatóságnál azt vizsgáljuk, hogy egész számok osztásakor mikor lesz a hányados is egész szám, vagyis a maradék 0.

DEFINÍCIÓ: Egy a egész szám **osztó**ja egy b egész számnak, ha található olyan c egész szám, amelyre $a \cdot c = b$. Jelölés: $a \mid b$. (Természetesen $c \mid b$ is igaz). Ebben az esetben az is igaz, hogy b **osztható** a-val és c-vel. Ekkor azt is mondhatjuk, hogy b **többszörös**e a-nak.

A 0 szerepe a számelméletben:

- a 0 minden nemnulla egész számnak többszöröse (0-szorosa), azaz 0 minden nemnulla egész számmal osztható ugyanis $0 = 0 \cdot a$: $a \mid 0$, ha $a \neq 0$. Ez azt is jelenti, hogy a 0 páros szám. A 0-nak egyetlen többszöröse van a 0, viszont a 0 bármely egész számnak a többszöröse.
- a 0 nem osztója egyetlen nemnulla egész számnak sem, ugyanis ha 0 osztója lenne egy b nem nulla egész számnak, akkor létezne egy olyan c egész szám, amikre $b = c \cdot 0 = 0$ lenne, ami ellentmond azzal a feltétellel, hogy $b \neq 0$.

Oszthatósági tételek:

Ha $a, b, c \in \mathbb{Z}$, akkor

TÉTEL: $1 \mid a$, azaz az 1 minden egész számnak osztója.

BIZONYÍTÁS: $a = a \cdot 1$.

TÉTEL: $a \mid a$, azaz minden egész szám osztója önmagának.

BIZONYÍTÁS: $a = 1 \cdot a$.

TÉTEL: $a \mid b$ és $b \mid c \Rightarrow a \mid c$.

BIZONYÍTÁS: Az $a \mid b$ feltétel azt jelenti, hogy van olyan d egész szám, amire $b = a \cdot d$, a $b \mid c$ feltétel azt jelenti, hogy van olyan e egész szám, amire $c = b \cdot e$.
Ekkor $c = b \cdot e = (a \cdot d) \cdot e = a \cdot (d \cdot e)$ a szorzás asszociativitása miatt, ahol a $d \cdot e$ szorzat egész szám.
Ez azt jelenti, hogy van olyan egész szám, aminek a-szorosa a c szám, vagyis $a \mid c$.

TÉTEL: $a \mid b \Rightarrow a \mid b \cdot c$, azaz ha egy egész szám osztója egy másik egész számnak, akkor a többszöröseinek is osztója.

BIZONYÍTÁS: Az $a \mid b$ feltétel azt jelenti, hogy van olyan d egész szám, hogy $b = a \cdot d$. Ekkor $b \cdot c = (a \cdot d) \cdot c = a \cdot (b \cdot c)$ a szorzás asszociativitása miatt. A $(b \cdot c)$ szorzat egész, tehát találtunk megfelelő egész számot, így $a \mid b \cdot c$.

TÉTEL: $a \mid b$ és $a \mid c \Rightarrow a \mid b \pm c$, azaz ha egész egy szám osztója két egész számnak, akkor összegüknek és különbségüknek is osztója.

BIZONYÍTÁS: Az $a \mid b$ feltétel azt jelenti, hogy van olyan d egész szám, hogy $b = a \cdot d$. Az $a \mid c$ feltétel azt jelenti, hogy van olyan e egész szám, hogy $c = a \cdot e$. Ekkor $b \pm c = (a \cdot d) \pm (a \cdot e) = a \cdot (d \pm e)$ a disztributivitás miatt. A $(d \pm e)$ egész szám, tehát találtunk megfelelő egész számot, így $a \mid b$ és $a \mid c \Rightarrow a \mid b \pm c$.

TÉTEL: $a \mid b$ és $a \mid b + c \Rightarrow a \mid c$, azaz ha egy egész szám osztója egy összegnek és az összeg egyik tagjának, akkor osztója a másik tagnak is.

BIZONYÍTÁS: Az $a \mid b$ feltétel azt jelenti, hogy hogy van olyan d egész szám, hogy $b = a \cdot d$. Az $a \mid c$ feltétel azt jelenti, hogy van olyan e egész szám, hogy $c = a \cdot e$. Ekkor $b \pm c = (a \cdot d) \pm (a \cdot e) = a \cdot (d \pm e)$ a disztributivitás miatt. A $(d \pm e)$ egész szám, tehát találtunk megfelelő egész számot, így $a \mid b$ és $a \mid c \Rightarrow a \mid b \pm c$.

Az oszthatóságot eddig az egész számokra értelmeztük, a továbbiakban leszűkítjük a természetes számokra, azaz a nemnegatív egész számokra. Egy adott problémánál tudjuk majd automatikusan alkalmazni az itt megfogalmazottakat az egész számokra.

TÉTEL: Ha $a, b \in \mathbb{Z}^+$, és $a \mid b$ valamint $b \mid a \Rightarrow a = b$, azaz ha két pozitív egész szám egymásnak osztója, akkor a két szám egyenlő.

BIZONYÍTÁS: Az $a \mid b$ feltétel azt jelenti, hogy van olyan d egész szám, amire $b = a \cdot d$, a $b \mid a$ feltétel azt jelenti, hogy hogy van olyan e egész szám, amire $a = b \cdot e$.
Ekkor $b = a \cdot d = (b \cdot e) \cdot d = b \cdot (d \cdot e)$ a szorzás asszociativitása miatt.
Osztva b-vel az egyenlet mindkét oldalát: $1 = b \cdot e$, aminek a pozitív egész számok halmazán csak a $d = e = 1$ a megoldása.
Ekkor viszont $a = b \cdot 1 = b$.

Oszthatósági szabályok:

Egy n egész szám osztható

- 2-vel, ha n páros, vagyis utolsó jegye $\in \{0; 2; 4; 6; 8\}$.
- 3-mal, ha a számjegyek összege osztható 3-mal.
- 4-gyel, ha a két utolsó jegyből képzett szám osztható 4-gyel.
- 5-tel, ha utolsó jegye $\in \{0; 5\}$.
- 6-tal, ha 2-vel és 3-mal osztható.
- 8-cal, ha a három utolsó jegyből képzett szám osztható 8-cal.
- 9-cel, ha számjegyek összege osztható 9-cel.
- 10-zel, ha utolsó jegye 0.

II. Prímszám, összetett szám, számelmélet alaptétele, osztók száma

DEFINÍCIÓ: Azokat a pozitív egész számokat, amelyeknek pontosan két pozitív osztója van, **prímszám**oknak nevezzük. Pl.: 2; 3; 5; 7; … Az 1 nem prímszám.

TÉTEL: Végtelen sok prímszám van.

BIZONYÍTÁS: Indirekt módon: Tegyük fel, hogy véges sok, azaz n db prímszám van. Legyenek ezek $p_1, p_2, p_3, ..., p_n$. Képezzük a következő számot: $A = p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_n + 1$.

Az A számnak a felsorolt n db prím egyike sem osztója. Ebből két lehetőség következhet: vagy az A szám is prím (az $n + 1$-edik), vagy létezik olyan prím, amit nem soroltunk fel (akkor ez a prím az $n + 1$-edik). Tehát mindkét esetben találtunk a felsorolásban nem szereplő prímszámot, ezzel ellentmondásra jutottunk, azaz nem véges sok, hanem végtelen sok prímszám van.

DEFINÍCIÓ: Azokat az 1-nél nagyobb számokat, amelyek nem prímszámok, **összetett szám**oknak nevezzük. Az összetett számoknak 2-nél több pozitív osztója van. Pl.: 4; 6; 8; 9; 10; …

TÉTEL: A számelmélet alaptétele: bármely összetett szám felírható prímszámok szorzataként, és ez a felbontás a tényezők sorrendjétől eltekintve egyértelmű.

Kanonikus alak: $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdot \ldots \cdot p_k^{\alpha_k}$, ahol $p_1, p_2, p_3, ..., p_k$ különböző prímek, $\alpha_1, \alpha_2, \alpha_3, ..., \alpha_k$ nemnegatív egész számok.

Ekkor az n szám prímosztói: $p_1, p_2, p_3, ..., p_k$.

TÉTEL: Meghatározható az ***n* szám osztóinak száma** a következő módon: A fenti n számnak $(\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot (\alpha_3 + 1) \cdot ... \cdot (\alpha_k + 1)$ darab pozitív osztója van.

DEFINÍCIÓ: Két vagy több pozitív egész szám **legnagyobb közös osztó**ja a közös osztók közül a legnagyobb. Jele: $(a; b)$.

Előállítása: felírjuk a számok prímtényezős alakját, vesszük a közös prímtényezőket (amelyek az összes felbontásban szerepelnek), ezeket a hozzájuk tartozó legkisebb kitevővel vesszük és összeszorozzuk.

DEFINÍCIÓ: Ha két pozitív egész szám legnagyobb közös osztója 1, akkor a két szám **relatív prím**.

DEFINÍCIÓ: Két vagy több pozitív egész szám **legkisebb közös többszörös**e a közös többszörösök közül a legkisebb. Jele: $[a; b]$.

Előállítása: felírjuk a számok prímtényezős alakját, vesszük az összes prímtényezőt, ezeket a hozzájuk tartozó legnagyobb kitevővel vesszük és összeszorozzuk.

Összefüggés két pozitív egész szám legnagyobb közös osztója és legkisebb közös többszöröse között: $(a; b) \cdot [a; b] = a \cdot b$.

III. Számrendszerek

DEFINÍCIÓ: Az ***a* alapú számrendszer** helyi értékei: 1, a^1, a^2, a^3, a^4, ..., az a alapú számrendszerben a-féle számjegy van: 0, 1, 2, ..., $a - 1$ (alaki érték), ha $a > 10$, akkor betűket használunk számjegyként.

A helyi értékes ábrázolás azt jelenti, hogy a számjegyek értékén kívül a leírásuk helye is értékkel bír. Egymás után írjuk a számjegyeket és az adott ponthoz viszonyítjuk a helyüket.

Általában 10-es számrendszerben dolgozunk. Ez azt jelenti, hogy a helyi értékek 10 természetes kitevőjű hatványai (10^0, 10^1, 10^2, 10^3, ..., azaz egyesek, tízesek, százasok, ezresek, ...). A számok leírására 10-féle számjegyre van szükség: 0, 1, 2, ..., 9.

A 10-es számrendszeren kívül az informatikában gyakran használják a 2-es, vagyis bináris számrendszert (Neumann-elv), napjainkban pedig inkább a 16-os, azaz hexadecimális számrendszert. Ez utóbbinál merült fel az a probléma, hogyan írjunk le 16-féle számjegyet. Erre az a megoldás született, hogy a 10-nél nagyobb alapú számrendszerekben a 10, vagy annál nagyobb értékű számjegyeket betűkkel jelöljük. Így 16-os számrendszerben 10 helyett A, 11 helyett B, …, 15 helyett F a számjegy.

Áttérés 10-es számrendszerből más alapúba

1. módszer:

A számot osztjuk az új számrendszer alapszámával, majd az így kapott hányadost újra mindaddig, míg 0 hányadost nem kapunk. Az osztásoknál kapott maradékok lesznek az új szám alaki értékei az egyesektől kezdve.
Pl. 948_{10} a 7-es számrendszerbe átírva:

$$948 = 135 \cdot 7 + 3$$
$$135 = 19 \cdot 7 + 2$$
$$19 = 2 \cdot 7 + 5$$
$$2 = 0 \cdot 7 + 2$$

2. módszer:

A tízes számrendszerbeli számot maradékosan elosztjuk az új számrendszer legnagyobb, de a számnál kisebb helyiértékével, a kapott maradékkal ezt addig folytatjuk, amíg a mara-dék 0 nem lesz.

948 : 343 = 2, maradék 262,
262 : 49 = 5, maradék 17,
17 : 7 = 2, maradék 3,
3 : 1 = 3, maradék 0,

Így $948_{10} = 2523_7$.

Áttérés más alapúból 10-es számrendszerbe

A megfelelő helyi értékeknek és a hozzájuk tartozó alaki értékeknek a szorzatösszege adja a 10-es számrendszerbeli értéket:
Pl.: 2523_7 a 10-es számrendszerbe átírva:

$$2523_7 = 2 \cdot 7^3 + 5 \cdot 7^2 + 2 \cdot 7^1 + 3 \cdot 1 = 948_{10}$$

A műveletek elvégezhetők az adott számrendszerben, vagy tízes számrendszerben és az eredmény adott számrendszerbe való visszaírásával.

Összeadás *n* alapú számrendszerben

Helyiérték szerint egymás alá írjuk a számokat, akár többet is. Az összeadást az $n^0 = 1$-es helyiértéken kezdjük, majd folytatjuk az n^1, n^2, n^3, ... helyiértékek felé. Mi 10-es számrendszerben tudunk összeadni, így az összegeket mindig 10-esben kapjuk meg, majd a kapott eredményt átváltjuk n-es számrendszerbe.
Ha az összeg n-nél kisebb, akkor leírjuk, mert n-nél kisebb számok minden számrendszerben azonos alakúak.
Ha az összeg nagyobb vagy egyenlő n-nél, akkor a kapott számot átírjuk 10-es számrendszerből n-es számrendszerbe. A kapott szám utolsó számjegyét leírjuk a megfelelő helyiértékre, az első számjegyét pedig az előző helyiérték fölé írjuk.
Ezt az eljárást addig folytatjuk, amíg a legelső számjegyig jutunk.

$$\begin{array}{r} {\scriptstyle 1\ \ 1\ \ \ \ } \\ 5726_{8} \\ +\ \ 315_{8} \\ \hline 6243_{8} \end{array} \qquad \begin{aligned} 6+5 &= 11_{10} = 13_{8} \\ 1+2+1 &= 4_{10} = 4_{8} \\ 7+3 &= 10_{10} = 12_{8} \\ 1+5 &= 6_{10} = 6_{8} \end{aligned}$$

$$\begin{array}{r} {\scriptstyle 2\,1\,1} \\ 2431_{(5)} \\ 10324_{(5)} \\ +\quad 430_{(5)} \\ \hline 14240_{(5)} \end{array}$$

$1+4+0=5_{(10)}=10_{(5)}$
$1+3+2+3=9_{(10)}=14_{(5)}$
$1+4+3+4=12_{(10)}=22_{(5)}$
$2+2+0=4_{(10)}=4_{(5)}$
$1=1_{(10)}=1_{(5)}$

$$\begin{array}{r} {\scriptstyle 1\;\;1\;\;} \\ A2F3_{(16)} \\ +\;\; 8B74_{(16)} \\ \hline 12D67_{(16)} \end{array}$$

$3+4=7_{(10)}=7_{(16)}$
$F+7=22_{(10)}=16_{(16)}$
$1+2+B=14_{(10)}=D_{(16)}$
$A+8=18_{(10)}=12_{(16)}$

Kivonás *n* alapú számrendszerben

Helyiérték szerint egymás alá írjuk a számokat. Az összeadást az $n^0 = 1$-es helyiértéken kezdjük, majd folytatjuk az n^1, n^2, n^3, ... helyiértékek felé.
Ha a kisebbítendő nagyobb vagy egyenlő a kivonandónál, akkor elvégezzük a kivonást, a különbséget leírjuk a megfelelő helyiértékre. Mivel n-nél kisebb értéket kapunk, nem kell átváltanunk, mert n-nél kisebb számok értéke minden számrendszerben egyenlő.
Ha a kisebbítendő (a) kisebb, mint a kivonandó (b), akkor $\overline{1a_n} = (n + a)_{10}$-ból vonjuk ki b-t, leírjuk a megfelelo helyiértékre az $(n + a - b)_{10}$ számot, az előző helyiértéken levő kivonandóhoz 1-et adunk és így végezzük el a kivonást.

$$\begin{array}{r} 6243_{(8)} \\ -5726_{(8)} \\ \hline 415_{(8)} \end{array}$$

$3 < 6 \Rightarrow 13-8=5_{(10)}=5_{(8)}$
$2+1=3 \Rightarrow 4-3=1_{(10)}=1_{(8)}$
$2<7+1 \Rightarrow 12-(7+1)=4_{(8)}$
$6=5+1 \Rightarrow 6-(5+1)=0_{(8)}$

$$\begin{array}{r} 12D67_{(16)} \\ -\;\; A2F3_{(16)} \\ \hline 8B74_{(16)} \end{array}$$

$7-3=4_{(10)}=4_{(16)}$
$6<F_{(16)} \Rightarrow \overline{16}-F=22-15=7_{(10)}=7_{(16)}$
$D_{(16)}-(2+1)_{(16)}=14-3_{(10)}=11_{(10)}=B_{(16)}$
$2<A_{(16)} \Rightarrow \overline{12}_{(16)}-A_{(16)}=18-10=8_{(10)}=8_{(16)}$

IV. Alkalmazások:

- Legnagyobb közös osztó: törtek egyszerűsítése
- Legkisebb közös többszörös: törtek közös nevezőre hozása
- Kétismeretlenes egyenlet megoldása a természetes számok halmazán (oszthatóság felhasználásával) pl.:

$$\begin{aligned} 3x+2y&=xy \\ 3x&=xy-2y \\ 3x&=y(x-2) \\ y&=\frac{3x}{x-2}=\frac{3x-6}{x-2}+\frac{6}{x-2}=3+\frac{6}{x-2}\in\mathbb{N} \;\Rightarrow\; x-2\mid 6 \end{aligned}$$

Ez a következő esetekben lehetséges:

$x-2$	1	2	3	6	–1	–2	–3	–6
x	**3**	**4**	**5**	**8**	1	**0**	–1	–4
y	**9**	**6**	**5**	**4**	–3	**0**	1	2

A táblázatban szerepel az összes megoldás, az 5 megjelölt számpár felel meg a feltételnek.

- Számítógépekben a 2-es számrendszer a két jegyével jól használható: folyik áram = 1, nem folyik áram = 0 (Neumann-elv). Ma már inkább a 16-os, hexadecimális számrendszert használják, ami felépíthető a kettesből.

Matematikatörténeti vonatkozások:

- Az egyiptomi **Rhind-papiruszon** (Kr. e. 2000–1700) a „törzstörtek” felsorolásában csak a páratlan nevezőjű törtek szerepeltek, tehát az egyiptomiak különbséget tettek a páros és a páratlan számok között.
- Az öttel való oszthatóságot az **ókori hinduk** is ismerték.
- A hárommal való oszthatóság szabályát először a pizai **Leonardo** (1200 körül) írta le.
- A tizeneggyel való oszthatóság szabályát a XI. századi **arab** matematikusok ismerték, viszont szabatosan csak **Lagrange** (1736–1813) francia matematikus fogalmazta meg: a páros helyi értéken álló számjegyeinek összege megegyezik a páratlan helyi értéken álló számjegyek összegével, vagy a kettő különbsége 11-nek a többszöröse.
- **Pascal** (1623–1662) francia matematikus teljes általánosságban vizsgálta az oszthatóságot a természetes számok körében.
- Prímszámok meghatározás az **eratoszthenészi** (Kr. e. III. század) szitával: Felírjuk 2-től kezdődően az egész számokat (ő 100-ig csinálta). A 2-t bekeretezzük, ez az első prímszám, majd kihúzzuk az összes olyan számot, ami 2 többszöröse (minden másodikat). Bekeretezzük az első át nem húzott számot, a 3-at, ez a következő prímszám. Innen kezdve áthúzzuk a 3 többszöröseit (minden harmadikat). Ezt az eljárást folytatva megkapjuk a prímszámokat (bekeretezett számok).
- A **sumérok** (Kr. e. 2000 előtt) a 10-es, 12-és és 60-as alapú számrendszer kombinációját használták az asztronómiai és egyéb számításaiknál. Ezt a rendszer átvették a **görögök**, a **rómaiak** és az **egyiptomiak**. A 60-as számrendszer maradványait felismerhetjük a mai idő- (órák, percek) és a szögmérésben (szögpercek).
- A **12-es számrendszer** nagyon népszerű volt, mert a 12 maradék nélkül osztható 2-vel (felezhető), 3-mal (harmadolható), 4-gyel (negyedelhető), 6-tal (hatodolható). A ma használt naptárban az év 12 hónapra oszlik, 12 óra a nappal és 12 óra az éjszaka az év mind a 365 napján. Csaknem minden nyelvben külön szó van a 12 dologból álló csoportra, például a magyar „tucat”, az angol „dozen”, a német „das Dutzend”, az orosz „djuzsina” stb.
- Nyelvészeti kutatások szerint az ősmagyarok a hetes számrendszert ismerték, használták: mesék hétfejű sárkánya, hetedhét ország, hétmérföldes csizma, hétpecsétes titok, hétszerte szebb lett, stb.
- A 2-es alapú bináris számrendszert már a XVII. században **Leibniz** ismertette, aki Kínában hallott róla, de általános használata a XX. században, a számítógépek megjelenésével terjedt el.
- **Neumann János** (1903–1957) magyar származású matematikus a róla elnevezett elvben megfogalmazta a számítógépek működési elvét. Ebben a számítógépek használjanak kettes számrendszert, az összes művelet kettes számrendszerbeli logikai műveletre redukálható.