32. tétel

Maradékos osztás és euklidészi algoritmus $\mathbb{Z}$-ben. Oszthatóság fogalma, tulajdonságai. Lnko, elkt. Indukciós, ill. prímelem. Számelmélet alaptétele és következményei.

$(\mathbb{Z}; +; \cdot)$ integritástartomány

- additív zérusa és zéruseleme : 0.
- multiplikatív egységeleme : 1
- „$\leq$" rendezési reláció szerint rendezett
- $\forall a \in \mathbb{Z}$ $\quad |a| = \begin{cases} a, & \text{ha } a \geq 0 \\ -a, & \text{ha } a < 0 \end{cases}$

  – $|a+b| \leq |a| + |b|$

  – $|a \cdot b| = |a| \cdot |b|$

Tétel: (Maradékos osztás tétele). $\forall a, b (\neq 0) \in \mathbb{Z}$-hez egyértelműen $\exists$-nek olyan q és r egész számok, amelyekre:

$$a = b \cdot q + r \quad \text{és} \quad 0 \leq r < |b|$$ teljesül.

Biz.: $H : \{m \mid m = a - b \cdot \xi \geq 0, \xi \in \mathbb{Z}\}$

$H \neq 0$, $H \subseteq \mathbb{N}$.

Mivel $\mathbb{N}$ rendezett ($\leq$ szerint) $\Rightarrow$ H-nek $\exists$ legkisebb eleme, ami legyen r.

$r = a - b\xi \qquad \xi = q \Rightarrow r = a - bq$.

$r < |b|$, mert $r \geq |b|$ lenne $\Rightarrow$

$$r) \; r - |b| = a - bq - |b| = \begin{cases} (a-bq) - b \geq 0, & \text{ha } b > 0 \\ (a-bq) + b \geq 0, & \text{ha } b < 0 \end{cases}$$

ez ellentmond r minimális mivoltának.

Tétel: $\forall a, b (\neq 0) \in \mathbb{Z}$-hez $\exists$-uek olyan q' és r' egészek, amelyekre

$$a = bq' + r' \quad \text{és} \quad |r'| < |b|$$

pl.: $13 = 5 \cdot 2 + 3 \qquad 3 < 5$

$13 = 5 \cdot 3 - 2 \qquad |-2| < 5$

$\forall a, b (\neq 0)$ egészekhez léteznek olyan q'' és r'' egészek, amelyekre:

$$a = bq'' + r'' \quad \text{és} \quad |r''| \leq \frac{|b|}{2}$$

$14 = 4 \cdot 3 + 2 \qquad 2 \leq 2$

$14 = 4 \cdot 4 - 2 \qquad |-2| \leq 2$

Euklidészi algoritmus:

Legyen $a, b (\neq 0) \in \mathbb{Z}$. A maradékos osztás szerint:

$$a = bq_0 + r_1 \text{, ahol } 0 \leq r_1 < |b|$$

Ha $r_1 \neq 0 \Rightarrow$ b és $r_1 \in \mathbb{Z}$-vel elvégezve a maradékos osztást:

$$b = r_1 q_1 + r_2 \text{, ahol } 0 \leq r_2 < r_1$$

$\vdots$

A maradékok a term. számok nig. [illegible]-csökkenő sorozatát alkotják $\Rightarrow$ a fenti algoritmus nem lehet végtelen hosszú. = Véges sok lépés után a maradéknak (r_{n+1}) 0-nak kell lennie. Mivel $|b| > r_1 > r_2 \ldots > r_n > 0 \Rightarrow$ legfeljebb $|b|$ lépésből áll.

Pl:

$$13 = 8 \cdot 1 + 5$$
$$8 = 5 \cdot 1 + 3$$
$$5 = 3 \cdot 1 + 2$$
$$3 = 2 \cdot 1 + 1$$
$$2 = 1 \cdot 2 + 0$$

Tétel: Legyen r_n az utolsó számtól különböző maradék. Végtelen sok x_n és y_n egész szám létezik, amelyekre: $ax_n + by_n = r_n$

Biz.: Megmutatjuk, h. minden $1 \leq k \leq n$ esetén létezner x_k és y_k egészek, melyekre $ax_k + by_k = r_k$

Rendezzük át!

$$r_1 = a - bq_0$$
$$r_2 = b - r_1 q_1$$
$$\vdots$$
$$r_{k-1} = r_{k-3} - r_{k-2} q_{k-2}$$
$$r_k = r_{k-2} - r_{k-1} q_{k-1}$$
$$\vdots$$
$$r_n = r_{n-2} - r_{n-1} q_{n-1}$$

Alkalmazzuk a k szerinti teljes indukciót!

$k = 1$, $k = 2$ esetben igaz.

Tfh: $\exists$ olyan $x_{k-2}, y_{k-2}, x_{k-1}$ és y_{k-1} egészek, h.

$$r_{k-2} = ax_{k-2} + by_{k-2}$$
$$r_{k-1} = ax_{k-1} + by_{k-1}, \text{ ahol } k \geq 3.$$

Így:

$$r_k = r_{k-2} - r_{k-1} q_{k-1} = ax_{k-2} + by_{k-2} - (ax_{k-1} + by_{k-1}) q_{k-1} =$$
$$= a(x_{k-2} - x_{k-1} q_{k-1}) + b(y_{k-2} - y_{k-1} q_{k-1}), \text{ ahol}$$

a és b együtthatóit x_k-val, ill. y_k-val jelölve

$$r_k = ax_k + by_k.$$

Látható, h. mindig nyerhető x_n, y_n számpár, amelyekre $ax_n + by_n = r_n$.

Oszthatóság:

Def.: $a \mid b$ $(a, b \in \mathbb{Z})$, ha az $ax = b$ egyenlet megoldható $\mathbb{Z}$-ben. Ezt az $a \mid b$, míg tagadását $a \nmid b$ szimbólum jelöli.

Az oszthatóság, mint bináris reláció, rendelkezik a következő tulajdonságokkal:

Tétel: $\mathbb{Z}$-ben az oszthatósági reláció:

- reflexív
- nem szimmetrikus
- nem antiszimmetrikus
- tranzitív

Tétel: $\forall a, b \in \mathbb{Z}$-re: ha $a \mid b$ és $b \mid a \Rightarrow |a| = |b|$

Tétel: $\forall a, b \in \mathbb{Z}$-re: ha $a \mid b \Rightarrow a \mid -b$; $-a \mid b$ és $-a \mid -b$.

Biz.: Mivel $a \mid b \Rightarrow a x_0 = b$ $(x_0 \in \mathbb{Z})$. De ekkor $-b = a(-x_0)$; $b = (-a)(-x_0)$ és $-b = (-a) x_0$ egyenlőségek igazak, így a tétel is igaz.

Def.: $(\mathbb{Z}; +; \cdot)$ integritástartomány 1 egységelemének az osztóit egységnek nevezzük.

Def.: Az a egész számot b egész szám asszociáltjának nevezzük, ha van olyan ε egység, amellyel $a\varepsilon = b$. (jel.: $a \sim b$)

(Nyilvánvaló a Z-ben egység: ± 1)

a és b pontosan akkor asszociáltak, ha $|a| = |b|$

Def.: ! $a, b (\neq 0) \in \mathbb{Z}$. Ha $a|b$ és se $a \sim 1$, se $a \sim b$, nem teljesül $\Rightarrow$ a-t b valódi osztójának, ellenkező esetben triviális osztójának nevezzük.

Így: $\forall a \in \mathbb{Z} \setminus \{-1; 0; 1\}$ egésznek pontosan 4 ($\pm 1, \pm a$) triviális osztója van.

Tétel: $\forall a, b, c, d \in \mathbb{Z}$-re:

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

b) Ha $a|b$ és $c|d \Rightarrow ac|bd$. multiplikatív tul.

Tétel: $\forall a \in \mathbb{Z}$-re igaz:

a) $a|0$

b) $0|a \Leftrightarrow$ ha $a = 0$

c) $e \in \mathbb{Z}$ szám $\Leftrightarrow$ osztója $\forall a \in \mathbb{Z}$-nek, ha $e = \pm 1$.

Tétel: $\forall$ a és $b (\neq 0)$ egész számra igaz, hogy

a) ha $a|b \Rightarrow |a| \leq |b|$

b) b-nek véges sok osztója van.

Lucro:

Def.: Az a és $b (\neq 0)$ egész számok legnagyobb közös osztójának nevezünk egy d egész számot, ha

1: d közös osztó, azaz $d|a$ és $d|b$

2: d a legnagyobb abban az értelemben, hogy a és b $\forall$ d' közös osztójának többszöröse, azaz ha $d'|a$ és $d'|b \Rightarrow d'|d$

Tétel: Ha $a, b (\neq 0) \in \mathbb{Z}$-nek $\exists$ nagyobb közös osztója $\Rightarrow$ az asszociáltság erejéig egyértelműen meghatározott.

Biz.: Tfh.: d_1 és d_2 kielégíti a fenti definíciót. $\Rightarrow$

$d_1 \mid d_2$ és $d_2 \mid d_1$, melyből ($\forall a, b \in \mathbb{Z}$-re, ha $a \mid b$ és $b \mid a \Rightarrow |a| = |b|$) tétel szerint $|d_1| = |d_2| \Rightarrow$

$d_1 \sim d_2$

Tétel: $\forall a, b (\neq 0) \in \mathbb{N}$-nak van lnko-ja, és $b \nmid a$ esetén $(a, b) = r_n$, ahol r_n az a és b egészeken végrehajtott euklideszi algoritmus utolsó zérustól különböző maradéka, míg $b \mid a$ esetén $(a, b) = 0$.

Tétel: $\forall a, b (\neq 0)$, c tetsz. számra igaz:

- $(a, b) = (b, a)$
- $((a, b), c) = (a, (b, c))$
- $(b, b) = b$
- $(a, b)c = (ac, bc)$, ha $c \neq 0$
- $(a, b) = b \Leftrightarrow$ ha $b \mid a$
- $(a, b) = (a + \xi b, b)$, ahol $\xi \in \mathbb{Z}$

Def.: Ha $(a_1, a_2 \dots a_n) = 1$ $(n \geq 2) \Rightarrow$ az $a_1, a_2 \dots, a_n$ egészeket relatív prímeknek nevezzük. Ha $(a_i, a_j) = 1$, $\forall 1 \leq i \leq j \leq n$ esetén $\Rightarrow$ páronként relatív prím egészekről beszélünk.

Tétel: $\forall a, b (\neq 0)$ tetsz. számra:

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

Biz.: ($(a,b)c = (ac,bc)$, ha $c \neq 0$ szerint)

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

$$(a,b)\left(\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) - 1\right) = 0$$

Mivel $(a,b) \geq 1$, ezért igaz a tétel.

Tétel: ! $a(\neq 0), b, c \in \mathbb{N}$. $(a,b)=1$ és $(a,c)=1 \Leftrightarrow$, ha $(a,bc)=1$.

Tétel: ! $a(\neq 0), b, c \in \mathbb{N}$. Ha $a \mid bc$ és $(a,b)=1 \Rightarrow a \mid c$.

Tétel: ! $a(\neq 0), b, c \in \mathbb{N}$. Ha $a \mid b$, $c \mid b$, $(a,c)=1 \Rightarrow ac \mid b$.

Lkkt.

Def.: Legyen $a, b \in \mathbb{Z} \setminus \{0\}$. Az a és a b legkisebb közös többszörösének nevezzük $m \in \mathbb{Z}$-t, ha

a) m közös többszörös, azaz $a \mid m$ és $b \mid m$.

b) m „legkisebb" abban az értelemben, hogy a és b $\forall$ m' közös többszörösének osztója a, azaz, ha $a \mid m'$ és $b \mid m'$, $\Rightarrow m \mid m'$.

Tétel: Ha az $a, b \in \mathbb{Z} \setminus \{0\}$ egészeknek $\exists$ lkkt-e $\Rightarrow$ az asszociáltságig egyértelműen meghatározott.

Biz.: Tfh m_1 és m_2 lkkt-e a és b egészeknek. $\Rightarrow$ def. alapján $m_1 \mid m_2$ és $m_2 \mid m_1$ is teljesül, amelyből $|m_1| = |m_2|$, azaz $m_1 \sim m_2$.

Tétel: $\forall$ a,b pozitív egész számokra van létre-e, és:

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

Tétel: $\forall$ a,b,c pozitív egészekre igazak az alábbi tulajdonságok:

- $[a,b] = [b,a]$
- $[[a,b],c] = [a,[b,c]]$
- $[a,a] = a$
- $[a,b]c = [ac, bc]$
- $[a,b] = b \Leftrightarrow$, ha $a \mid b$.

Def.: Az $a_1, a_2 \dots a_n$ természetes egész számok $[a_1, a_2 \dots a_n]$-nel jelölt LKT-ja értjük $n \geq 3$ esetben az

$$[a_1, a_2 \dots, a_n] = [[a_1, a_2 \dots a_{n-1}], a_n]$$

pozitív egész számot.

Irreducibilis és prímelem:

Def.: A 0-tól és ± 1-től különböző p egész számot irreducibilisnek (felbonthatatlannak) nevezzük, ha nincs valódi osztója, azaz, ha $a \in \mathbb{Z}$ és $a \mid p \Rightarrow$ vagy $a = \pm 1$ vagy $a = \pm p$. Ellenkező esetben p-t reducibilisnek nevezzük.

Def.: A 0-tól és ± 1-től különböző p egész számot prímnek nevezzük, ha az valahányszor osztója egy szorzatnak, mindannyiszor osztója a szorzat legalább egyik tényezőjének, azaz ha $a, b \in \mathbb{Z}$, $p \mid ab$, de $p \nmid a \Rightarrow$ $p \mid b$.

Tétel: $A(\mathbb{Z}; +; \cdot)$ integritástartományban az irreducibilis egészek és a prímek egybeesnek, azaz a p egész szám $\Leftrightarrow$ irreducibilis, ha prím.

Tétel: $\forall$ 0-tól és ± 1-től különböző egész szám véges sok irreducibilis szám szorzatára bontható és ez a felbontás a tényezők sorrendjétől és az egységtényezőktől eltekintve egyértelmű.

Irreducibilis faktorizáció létele = számelm. alaptétele

Tétel: Minden $n \geq 2$ term. szám sorrendtől eltekintve egyértelműen állítható elő véges sok prímszám szorzataként, ahol prímszámokon a pozitív prímeket értjük és az egységtényezős szorzat megengedett.

Tétel: $\exists\, m, n, d \in \mathbb{N} \setminus \{0\}$. Ha $(m,n) = 1$ és $d \mid mn \Rightarrow \exists$-nek olyan d_1, d_2 pozitív egészek, amelyekre $d_1 \mid m$, $d_2 \mid n$, $d = d_1 d_2$ és $(d_1, d_2) = 1$.

Tétel: $\exists\, k \in \mathbb{N} \setminus \{0\}$. Ha $m = n^k = m_1 m_2$ és $(m_1, m_2) = 1$, akkor léteznek olyan n_1 és n_2 term. számok, amelyekre $m_1 = n_1^k$ és $m_2 = n_2^k$

Tétel: Ha az $n \geq 2$ term. számnak nincs $\sqrt{n}$-nél nem nagyobb prímszáma osztója, akkor n prímszám, azaz minden összetett természetes számnak van $\sqrt{\ }$-énél nem nagyobb prímosztója.

BIZ.: $\exists\, n$ összetett szám, $\exists\, p$ a legkisebb prímosztója. $\Rightarrow$ $n = pm$, ahol $m \geq p$. Ezért $n \geq p^2$ és $p \leq \sqrt{n}$, tehát a legkisebb prímosztó valóban legfeljebb $\sqrt{n}$.

Tétel : Végtelen sok prímszám van.