

2018. 02. 09.

1. konzultáció

Diszkrét matematika

www.math.u-szeged.hu/~kantai

Kantai @.

Kantai - László Hamilla az előadó, ügye

Vannak z-tesztok: 6 db van $\rightarrow 6 \times 4 \text{ pont} = 24 \text{ pont}$.

min. 10 pont kell.

ZH a gyakorlati részből: 2018. május 11.

$\Sigma 36 \text{ pont} \rightarrow$ kell belőle min. 16 pont.

$\rightarrow$ utolsó vizsga $\rightarrow$ 40 pont.

50% a félévközlőzáróknál kell.

Számelmélet:

Def.: $a, b \in \mathbb{Z}$, a osztója b -nek, ha $\exists z \in \mathbb{Z}$, hogy
 $a \cdot z = b$.
jele: $a \mid b$.

2. tétel: (1) $a \mid a$

biz: $z = 1$ -re $a \cdot 1 = a \Rightarrow a = a \Rightarrow a \mid a$.

(3) $a \mid b$ és $b \mid c \Rightarrow a \mid c$

Biz: $\exists z \quad a \cdot z = b \quad (a \mid b)$

$\exists l \quad b \cdot l = c \quad (b \mid c)$

$\Downarrow$

$$a \cdot \underbrace{z \cdot l}_w = c$$

$\in \mathbb{Z}!$ (mind mindkettő egész)

$\Downarrow$

$$a \cdot w = c$$

$\uparrow w \in \mathbb{Z} \rightarrow \boxed{a \mid c}$

osztatóság

$\Downarrow$

reláció, nem művelet.

$\rightarrow 0 \mid 0$ is igaz.

(1)

$$(6) \quad a|b \Leftrightarrow |a| \mid |b|.$$

és a tétel.

Biz:

$$\Rightarrow a|b : \exists z \quad a \cdot z = b.$$

$$|a \cdot z| = |b|$$

$$|a| \cdot \underbrace{|z|}_{\text{el is } \in \mathbb{Z}} = |b| \quad \Rightarrow |a| \mid |b|$$

belátható.

$$\Leftarrow \exists z, \text{ melyre}$$

$$|a| \cdot z = |b|$$

z eset van.

1. eset: $\text{sign}(a) = \text{sign}(b).$

$$a \cdot z = b.$$

2. eset: $\text{sign}(a) \neq \text{sign}(b).$

$$a \cdot (-z) = b.$$

Belátható.

$$(9) \quad a|b \text{ és } c|d \Rightarrow ac|bd.$$

Biz: $\exists z, \text{ hogy } a \cdot z = b \text{ és}$

$\exists l, \text{ hogy } c \cdot l = d. \quad \text{Eddig tuti.}$

$\Downarrow$

$$a \cdot z \cdot c \cdot l = b \cdot d$$

$$ac \cdot \underbrace{(z \cdot l)}_{\in \mathbb{Z}} = bd$$

$\in \mathbb{Z} \Rightarrow \text{Belátható.}$

A tétel lehet HF, egyenlő belátható.

Definíció: $a, b \in \mathbb{Z}$. $d \in \mathbb{Z}$ az a és b

legnagyobb közös osztója, ha:

(Léte 1) - $d|a$ és $d|b$ (d az közös osztó).

(Léte 2) - $\forall z \in \mathbb{Z}$, ami $z|a$ és $z|b$, $\Rightarrow z|d$.

Értékes feladat, de tulajdonképpen igaz.

A legnagyobb közös osztó nem egyértelmű. $c|a$ és $c|b \Rightarrow$
 $-c|a$ és $-c|b$.

Ezért.

(2) $\text{LKO}(0, a) \rightarrow a$
 $\downarrow$
 $-a$
Lemma.

(Léte 1) $a|a$ és $a|0$
 $z=1$ $z=0$

(Léte 2) $\forall z \in \mathbb{Z}$ $z|a$ és $z|0 \Rightarrow z|a$.

Így lehet bebizt.

L. lemma (3) $\underbrace{\text{LKO}(a, b)}_d \sim \underbrace{\text{LKO}(a+bc, b)}_{d'} \quad (a \sim b \text{ ha } a|b \text{ és } b|a)$

Biz.:

$d|d'$: $d|a$ és $d|b$.

$\downarrow$ (8)
 $d|bc$.

$d|a+bc$

$d|b$ és $d|a+bc \Rightarrow d|d'$. Ennek.
Léte (2)

$d'|d$: $d'|a+bc$ és $d'|b$.

$\downarrow$ (8)
 $d'|bc$

$d'|a$

(3)

$$d' \mid a \text{ és } d' \mid b \Rightarrow d' \mid d$$

lko 2



$$d \sim d' \text{ be is látszik.}$$

Ezt használja ki az euklideszi algoritmus is.

5. Tétel: $a, b \in \mathbb{Z}, b \neq 0$.

Egyértelműen meghatározott q, r egész számok

$$a = b \cdot q + r$$

$$0 \leq r < |b|.$$

maradékos osztás tételén.

Biz.: $b > 0$ esete.

$$a = bq + r \Rightarrow r = a - bq.$$

$$0 \leq \underbrace{a - bq}_r < |b| = b$$

$$0 \leq a - bq < b \quad / + bq$$

$$bq \leq a < b + bq = b(1 + q) \quad / : b$$

$$q \leq \frac{a}{b} < 1 + q$$

$b > 0$ ezt tudjuk.

$$\text{pl.: } 4 \leq \frac{22}{5} < 1 + 4!$$

Altså egészszámszerűen...

Ha b negatív,
fordít minden
reláció.

$$q = \left\lfloor \frac{a}{b} \right\rfloor.$$

Euklidész algoritmus:

Természetes számokra lett megfogalmazva.

$$r_0 = q_1 r_1 + r_2$$

$$r_1 = q_2 r_2 + r_3$$

⋮ Addig tart, amíg 0 adódik maradékként.

$$r_{n-1} = q_n \underbrace{r_n}_{\text{leltö}(a,b)} + r_{n+1}$$

↑

Ezt bizonyítani kellene. Az algoritmus végezetét legalábbis.

(7).

$$\underbrace{r_1}_{>0} > r_2 > r_3 > \dots > r_n > r_{n+1} \geq 0.$$

Alulról is van korlát.

pozitív (vagy negatív) maradékok határozatlan csökkenő sorozata eléri a nullát.

$$r_n = \text{leltö}(a, b) \quad \text{Ezt is lássuk be.}$$

(leltö 1) alulról feljelle.

$$r_{n-1} = q_n r_n + \underbrace{r_{n+1}}_{=0}$$

↓

$$\boxed{r_n \mid r_{n-1}}$$

$$r_{n-2} = \underbrace{q_{n-1} r_{n-1}}_{(8)} + \underbrace{r_n}_{r_n \mid r_n} \quad (1)$$

$$\underbrace{r_n \mid q_{n-1} r_{n-1}}_{(7)}$$

$$r_n \mid r_n + q_{n-1} r_{n-1}$$

↓

$$\boxed{r_n \mid r_{n-2}}$$

⑤

Három tételt
használtunk
tehát.

Es így tovább.

$$r_1 = q_2 r_2 + r_3$$

$$r_n | r_3, \quad r_n | q_2 r_2 \Rightarrow \boxed{r_n | r_1}$$

$$r_n | a$$

$$r_0 = q_1 r_1 + r_2$$

$$\underbrace{r_n | r_1 \quad r_n | r_2}_{r_n | r_0}$$

$$\boxed{r_n | r_0}$$

$$\boxed{r_n | b}$$

Így belátható, hogy $r_n | a$ és $r_n | b$.

(Létezik) felülől lefelé lehet belátni.

$$\forall z \in \mathbb{Z}, \quad z | a \quad \text{és} \quad z | b$$

$$\underbrace{z | a}_{r_0} \quad \underbrace{z | b}_{r_1}$$

$$r_0 = q_1 r_1 + r_2$$

$$r_2 = r_0 - q_1 r_1$$

$$\uparrow \quad \underbrace{\quad}_{(3)}$$

$$z | r_0 \quad (2) \quad z | q_1 r_1$$

$$\underbrace{\quad}_{z | r_2}$$

Es így tovább.

$$r_n = r_{n-2} - q_{n-1} r_{n-1}$$

$$\underbrace{\quad}_{z | r_n}$$

Ennyi az egész.

Legkisebb közös többszörös definíciója:

(Def 1) $a \mid t$ és $b \mid t$ (többször, közös!)

(Def 2) $a \mid x$ és $b \mid x \Rightarrow t \mid x$

$$\text{lko}(a, b) \approx \frac{a \cdot b}{\text{ko}(a, b)}$$

lg számolható.

Néhány példa:

$$\text{lko}(60, 27) = ?$$

eurk. alg.

$$60 = 27 \cdot 2 + \boxed{6}$$

$$\rightarrow 6 = 60 - 27 \cdot 2$$

$$\rightarrow 3 = 27 - 6 \cdot 4$$

$$27 = 6 \cdot 4 + \boxed{3}$$

legutolsó nem nulla maradék.

$$6 = 2 \cdot 3 + 0$$

Vége.

$$3 = 27 - 6 \cdot 4$$

$$3 = 27 - (60 - 27 \cdot 2) \cdot 4$$

ide vissza-
ragaszt.

$$\text{lko}(60, 27) = 3$$

$$3 = g \cdot 60 + w \cdot 27 \text{ mindig felírható. (9).}$$

$$3 = 27 - 4 \cdot 60 + 8 \cdot 27$$

$$\boxed{3 = 60 \cdot (-4) + 27 \cdot 9}$$

Ehhez az egész.

"lineáris kombináció" - lehet

lehet.

Relatív prím fogalma.

Piofantoszi egyenlet:

$$ax + by = c, \quad a, b, c \in \mathbb{Z} \text{ adottak.}$$

pontosan akkor lehet megoldás, ha $\text{ltko}(a, b) \mid c$.

Ha x_0, y_0 egy megoldás, akkor

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

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

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

Bizonyítás:

$$ax + by = c$$

$$\text{ltko}(a, b) = d.$$

$$\underbrace{d \mid a \text{ és } d \mid b}$$

$$d \mid ax + by \quad \text{és} \quad d \mid c. \quad \checkmark$$

Elegendő.

$\text{ltko}(a, b) = ax + by$ alakú. (Euklideszi algoritmusból jön).

$$\text{ltko}(a, b) \mid c \Rightarrow \exists z \in \mathbb{Z} \quad \text{ltko}(a, b) \cdot z = c$$

$$\underbrace{\text{ltko}(a, b) \cdot z}_c = a(zx) + b(zy)$$

x_0 és y_0 egy megoldás.

$$\begin{aligned} & a \left(x_0 + \frac{b}{\text{ltko}(a, b)} \cdot t \right) + b \left(y_0 + \frac{a}{\text{ltko}(a, b)} \cdot t \right) = \\ & = \underbrace{ax_0 + by_0}_c + \frac{ab}{\text{ltko}(a, b)} t - \frac{ab}{\text{ltko}(a, b)} t = c \end{aligned}$$

Elegendő.

$$60x + 27y = 12$$

PELDA.

1. lépés:

euclidesu algoritmusmal meghatározzuk a legnagyobb közös osztót.
(lásd előbb).

$$\text{lnko}(60, 27) = 3. \quad \rightarrow 3 \mid 12 \Rightarrow \text{HEGOLDHATÓ.}$$

2. lépés:

$$\text{lnko}(60, 27) = ax + by \quad (60 \text{ és } 27 \text{ lin.}$$

kombinációjából).

3. lépés: $\text{lnko}(60, 27) = 3 = 60 \cdot (-1) + 27 \cdot 9$ (érdemes utánasímozni...)
/ · 4 (BE KELL SZOROSNI)

/ Mit akarunk megoldani? /

$$12 = 60 \cdot \underbrace{(-16)}_{x_0} + 27 \cdot \underbrace{(36)}_{y_0}$$

4. lépés:

$$\left. \begin{aligned} x &= -16 + \frac{27}{3} \cdot t \\ y &= 36 - \frac{60}{3} \cdot t \end{aligned} \right\} t \in \mathbb{Z}$$

$$(x = -16 + 9t)$$

$$(y = 36 - 20t)$$

Ezt tudni kell, pont.

Primszámok:

p felbonthatatlansága

$p \geq 2$ Ha $p = ab$ akkor ez triviális, tehát

$$a = \pm 1$$

$$b = \pm p \text{ vagy fordítva.}$$

Ez a triviális felbontás
③

p prím, ha $p \geq 2$ ha $p | ab \Rightarrow p | a$ (vagy) $p | b$.

Ez a definíciója.

↑ megengedő vagy.

(pl.) 6 nem prím, mert $6 | 2 \cdot 3$, de $6 \nmid 2$ és $6 \nmid 3$.

Ilyen kis egyszerű példa.

17. Tétel

p prím $\iff p$ felbonthatatlan.

(Biz.)

①

$\Rightarrow$

p prímszám.

$$p = ab \Rightarrow p | ab \quad (2.1)$$

$\Downarrow$

$p | a$ vagy $p | b$.

Tfh.: $p | a$.

$a | a \cdot 1$ (10. tétel)

$a \neq 0$.

$6 | 1$.

$$2 \cdot 6 = 1 \Rightarrow$$

$$\boxed{6 = \pm 1}$$

lévén hogy egész számok.

②

$\Leftarrow$

p felbonthatatlan.

$p | ab \rightarrow p | a$ ✓ Ez kész.

$\Downarrow p \nmid a$

A 12. lemmát itt fogjuk használni.

$$\text{luko}(a, p) = ?$$

$$\text{luko}(a, p) / p$$

↑ felbonthatatlan

(p)

(1)

Ez akkor lenne igaz ha

(10)

Ez kész.

$p | a$.

ELLENT-
MOND.

$$\ln_0(a, p) \sim 1. \quad p|ab \Rightarrow p|b. \quad \checkmark$$

Ennyi. Beláttuk.

A számelmélet alaptétele:

$$\mathbb{N} = \{1, 2, \dots\}.$$

űres szorzattal kapható meg az 1.



Minden természetes szám prímszámok szorzataként áll elő.

(Biz.)

A felbontás létezik.

$$a \in \mathbb{N}.$$

Ha $a = 1$: (nulla tényezőes szorzat)

Ha a prím: (egy tényezőes szorzat)

Ha a nem prím: akkor vagy nem is felbonthatatlan.



Az ezzel nagyobb osztói közül vesszük a legkisebbet, ami prím.

$$\stackrel{p_1}{\equiv}$$

$$a = p_1 \cdot a_1 \text{ alakban előáll } a.$$

Ha a_1 prím: készen van.

Ha a_1 nem prím, akkor lát az előre lépést.

$$a_1 = p_2 \cdot a_2.$$

ATÖ...

Mivel a p_1 prím: $a > a_1 > a_2 > \dots > a_n \geq 1$.

Ezért az algoritmus véget fog érni.

Hogy látszik, hogy a felbontás egyértelmű?

Indirekt úton belátható.

Tfh. nem egyértelmű, tehát $\exists$ két lényegesen különböző felbontás.

$$a = p_1 \cdot p_2 \cdot p_k = q_1 \cdot q_2 \cdot q_k$$

Ha $p_1 = q_1$, akkor leoszthatunk vele.

Alt.: $p_i = q_j \rightarrow$ leoszthat.

$$b = \underbrace{r_1 \cdots r_j}_{r_1 \text{ osztoja és prím}} = \underbrace{s_1 \cdots s_n}_{r_1 \text{ ehhez is osztoja.}} \quad (\text{minszint egy faktor prím})$$

$s_1 \cdots s_n$ valamely tényezőjének is osztoja.

$$r_1 \mid s_j \quad \leftarrow \text{felbontható}$$

$r_1 \neq 1$ nem prím

$r_1 \neq s_j$ ELLENTMONDÁS.

$$12 = 2 \cdot 3 \cdot 2 = 2^2 \cdot 3 \cdot 5^0 \quad \text{Prímhatványképzés sorozat.}$$

$$15 = 3 \cdot 5 \cdot 2^0 \quad \text{Itt az a csúsz, ahogy a középértékben.}$$

(T:) α b α és csd is α b, ha $\alpha_i \leq \beta_i$.

(lásd a mellékelt anyagot).

$\Rightarrow$

$\Leftarrow$ $\beta_i - \alpha_i$ a k szám, amit találhatunk.

(1)

19. tétel / 2.

$$\text{lnc}(a, b) \mid a, \quad \text{lnc}(a, b) \mid b.$$

$$\min(L_i, B_i) \leq \frac{L_i}{B_i} \Rightarrow \checkmark \quad \text{lnc}(1) \text{ - es tétel.}$$

$$(\text{lnc } 2) \quad \forall z \in \mathbb{Z}, \text{ ha } z \mid a \text{ és } z \mid b.$$

$$x_i \leq L_i \quad x_i \leq B_i$$

$$x_i \leq \min(L_i, B_i)$$

$$(20.) \quad \text{lnc}(a, b) \cdot \text{lrc}(a, b) = ab. \quad \text{Ismeret már.}$$

Eszenyi, itt a vége.

