Egységgyök (ε)

$\varepsilon^n = 1 \qquad (\varepsilon = \sqrt[n]{1})$

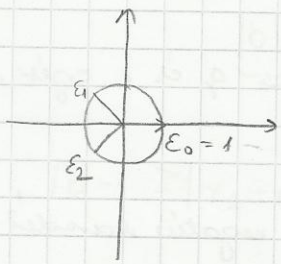
$1 = 1(\cos 0 + i \sin 0)$

$\varepsilon_0, \varepsilon_1 \dots \varepsilon_{n-1}$

$\varepsilon_j = 1\left(\cos \frac{j \cdot 2\pi}{n} + i \sin \frac{j \cdot 2\pi}{n}\right)$ egységgyök

pl.: $n = 2$ $\quad \varepsilon_0 = 1$, $\varepsilon_1 = -1$

$n = 3$ $\quad \varepsilon_0 = 1$ $\quad \varepsilon_1 = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ $\quad \varepsilon_2 = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$



$n = 4$

$\varepsilon_0 = 1$

$\varepsilon_1 = i$

$\varepsilon_2 = -1$

$\varepsilon_3 = -i$

$n = 2; 3; 4; 6; 8; 12$!!!

tudni kell!

$\sqrt[n]{z} = w_j$

$w_j = w_0 \cdot \varepsilon_j = w_0 \cdot \varepsilon_1^j$

Def.:

A n-dik egységgyök közül azt ε_j-t primitív n-dik egységgyök nevezzük, ha ε_j egész kitevős hatványaiként az összes n-dik gyök előállítható

Tétel: $\varepsilon_j \Leftrightarrow$ primitív, ha j és n relatív prím

X.29.

XIV tétel

Számelmélet elemeinek vizsgálata

$(\mathbb{Z}; +, \cdot)$ integritás tartomány

tul: $a, b \in \mathbb{Z}$

$$a \in \mathbb{Z} \quad |a| := \begin{cases} a, & \text{ha } a \in \mathbb{N} \\ -a, & \text{ha } a \in \mathbb{Z}^- \end{cases}$$

$|a| \cdot |b| = |ab|$

$|a+b| \leq |a| + |b|$ 3% egyenlőtlenség

$(\mathbb{Z}; \leq)$ lineárisan (teljesen) rendezett halmaz

(de: nem jól rendezett)

Tétel: A maradékos (euklidészi) osztás tétele:

$\forall a, b \in \mathbb{Z}$ $b \neq 0$ - hoz egyértelműen létezik olyan q és r egész,

hogy $a = b \cdot q + r$, ahol $a \leq r < |b|$

$17 = 6 \cdot 2 + 5$

a: osztandó, b: osztó, q: hányados, r: maradék

„r" legfeljebb nem negatív maradék

Bizt.: (létezik)

$M := \{a - b \cdot t \mid a - b \cdot t \geq 0, \ t \in \mathbb{Z}\} \neq \emptyset$, $M \subseteq \mathbb{N}$

$\mathbb{N}$ v. $\mathbb{Z}$

a jól rendezettség miatt ($\mathbb{N}$ halmazán)

$\Downarrow$

M-nek van minimuma

jelöljük ezt r-rel $(r := a - b \cdot t)$

éppen a minimumnál $t := q$

mivel $M \in \mathbb{Z}$, ezért az $a \leq r < |b|$ teljesül

$r \geq |b|$

$r \geq r - |b| = a - bq - |b| = \ldots \geq 0$

- ha $b \geq 0$
- ha $b < 0$

ellentmondás: $\rightarrow r < |b|$

r nem lehet nagyobb mint b a minimum

(egyértelműség)

Indirekt:

Tfh.: $a = bq_1 + r_1 \qquad 0 \le r_1 < |b|$

$a = bq_2 + r_2 \qquad 0 \le r_2 < |b|$

$q_1 \neq q_2 \qquad b(q_1 - q_2) = r_2 - r_1$

$\Downarrow$

$|b| \cdot |q_1 - q_2| = |r_2 - r_1|$

$|b| \ge 1$, mert $\neq 0$

$q_1 - q_2$, mivel $q_1 \neq q_2$, így $|q_1 - q_2| \ge 1$

$\underbrace{|b| \cdot |q_1 - q_2|}_{\ge |b|}$ → legalább $|b|$

$|b| - 1 \ge |r_2 - r_1| \ge 0$ ↯ ⇒ $q_1 = q_2$

→ maximum $|b|$ ⇓

$r_1 = r_2$

A tételben fellépő hányadosok és maradékok mindig egyértelműek.

de: $a = bq + r'$

$|r'| \le \frac{|b|}{2}$

$17 = 6 \cdot 2 + 5$ → ez ilyenkor nem jó

$17 = 6 \cdot 3 - 1$ és már jó, mert megfelel az $|r'| \le \frac{|b|}{2}$ felt-nek.

$18 = 4 \cdot 4 + 2$

$18 = 4 \cdot 5 - 2$

} ebben az esetben nem igaz az egyértelműség, csak abban, ahol a maradék $(r) \Rightarrow 0 \le r < |b|$

$a = bq_0 + r_1 \qquad 0 < r_1 < |b|$

$b = r q_1 + r_2 \qquad 0 < r_2 < r_1$

$r_1 = r_2 q_2 + r_3 \qquad 0 < r_3 < r_2$

ontóból ontandó } less

maradékból ontó

⋮

$r_{n-2} = r_{n-1} q_{n-1} + r_n \qquad 0 < r_n < r_{n-1}$

$r_{n-1} = r_n q_n + 0$ < Véges sok lépésben véget kell érnie >

↑

Ez a sor: Euklideszi algoritmus

Ennek az utolsó eleme az, ahol a maradék 0.

r_n = utolsó 0-tól különböző maradék

Tétel: $a, b \in \mathbb{Z}$ és $b \neq 0$ $\exists$ végtelen sok olyan

x és $y \in \mathbb{Z}$, hogy

$r_n = ax + by$ → lineáris kombináció

Biz: 1, $\exists$ olyan $x_n, y_n \in \mathbb{Z}$, hogy

$r_n = a x_n + b y_n$

n-re teljes indukcióval az Euklideszi algoritmusból

$r_1 = a \cdot 1 - b q_0$

$x_1 = 1 \qquad y_1 = -q_0$

$r_2 = b - r_1 \cdot q_0 = a(\ ) + b(\ )$

Euklideszi algoritmusból adódik: x_n; y_n

$r_n = a x_n + b y_n$

$r_n = a(x_n - tb) + b(y_n + ta) \qquad \forall t \in \mathbb{Z}$

$r_n = a x_n - atb + b y_n + bta$

p.: $a \in \mathbb{N}^+$ $g \in \mathbb{N} \geq 2$

$a = g \cdot q_0 + r_0$ $\quad 0 \leq r_0 < g$

$q_0 = g \cdot q_1 + r_1$ $\quad 0 \leq r_1 < g$

$\vdots$

$q_{n-1} = g \cdot q_n + r_n$ $\quad 0 < r_n < g$

vége: $q_n = 0$ $\quad a = (\underbrace{r_n r_{n-1} \dots r_0}) g$

az „a" „g" alapú számrendszerbe átírt alakja

pl.: $18 = 5 \cdot 3 + 3$

$3 = 5 \cdot 0 + 3$ ↑

$18 = 33_{(5)}$

XV. tétel

Oszthatóság $\mathbb{Z}$-ben:

Def: $a, b \in \mathbb{Z}$ a osztható b-vel, ha $\exists c \in \mathbb{Z}$, hogy $b \cdot c = a$

jele: $b \mid a$ ⇒ „b" osztója „a"-nak

$b \nmid a$ ⇒ „b" nem osztója „a"-nak

$\begin{matrix} 111 \\ 000 \end{matrix}_2$ osztója 0-nak? Igen! $0 \cdot 2 = 0$

Az oszthatóság nem művelet, hanem egy bináris reláció!!!)

Oszthatóság tulajdonságai:

tranzitív: $a|b$ és $b|c \Rightarrow a|c$ ✓

reflexív: $\forall a \in \mathbb{Z}$ igaz $a|a$ ✓

antiszimm.: $5|-5$ és $-5|5$ $-5 \neq 5$ —

szimmetrikus: $3|6$, de $6 \nmid 3$ —

$a|b$ és $b|a \Rightarrow |a| = |b|$

Megj: $a|b \Rightarrow \pm a | \pm b$ → oszthatósági problémáknál elegendő $\mathbb{N}$-re korlátozódni.

—o— oszthatóság

„+" additív tul. $a|b \wedge a|c \Rightarrow a|b \pm c$

„·" multiplikatív tul. $a|b \wedge c|d \Rightarrow ac|bd$

Biz: TK-ben!

0 és 1-gyel kapcsolatos tulajdonságok:

- $\forall a \in \mathbb{Z}$ $a|0$ $(a \cdot 0 = 0$ ✓$)$

- ha $0|a \Leftrightarrow a = 0$ → csak saját magának osztója
 $(0 \cdot x \neq a)$

- $\forall a \in \mathbb{Z}$ $1|a$

 $e \in \mathbb{Z}$-ra igaz, hogy $\forall a \in \mathbb{Z}$ $e|a \Rightarrow e = \pm 1$

 ↳ egységelem osztója = e

Az „a" asszociáltja b, ha $a = \pm b$
$(a \cdot b \neq 0)$ $a = e \cdot b$ → előjelben tér el

jele: $a \sim b$
↓
asszociáltja

$12 \sim -12$

$a \in \mathbb{Z} \setminus \{0\}$

$b|a$ b nem triviális (valódi) osztója a-nak, ha $b \neq \pm 1$ $b \neq \pm a$

kivéve: ± 1 (ezek csak 2 van) ill. 0 (minden a halmazban)

triviális osztó: ± 1; $\pm a$

— o —

$a \neq 0$

$b|a$ $|b| \leq |a| \Rightarrow$ a osztóinak száma mindig véges!

Lnko, Lkkt:

$a, b (\neq 0) \in \mathbb{Z}$ $d \in \mathbb{Z}$

- az a és b lnko-ja d, ha:

① $d|a$ és $d|b$

② $\forall d' \in \mathbb{Z} : d'|a \wedge d'|b \Rightarrow d'|d$ (legnagyobb ebben az esetben $\Rightarrow$ d többszöröse d'-nek)

XV - XVI. tétel

Lkkt:

$a, b \in \mathbb{Z} \setminus \{0\}$ $u \in \mathbb{Z}$

- az a és b lkkt-e u, ha:

① $a|u \wedge b|u$

② $\forall u' \in \mathbb{Z} : a|u' \wedge b|u' \Rightarrow u|u'$

— o —

Tétel: Ha $\exists$ a és b lnko-ja, akkor asszociáltságon erejéig egyértelmű ⇒asszociáltak

Tétel: —"— lkkt-e —"—

lnko

d_1 d_2 $\left.\begin{matrix} d_2|d_1 \\ d_1|d_2 \end{matrix}\right\} |d_1| = |d_2|$

jelölés: a és b lnko-jai közül a pozitívat (a,b)-vel jelöljük

—"— lkkt-i —"— $[a,b]$ —"—

Tétel: $a, b \in \mathbb{Z} \quad (b \neq 0)$

1, ha $b \mid a \Rightarrow (a,b) = b$

2, ha $b \nmid a \Rightarrow (a,b) = r_N$

Biz.: ① $a = bq_0 + r_1 \qquad r_N \mid b;\ r_N \mid a$

$b = r_1 q_1 + r_2$

$\vdots$

$r_{N-2} = r_{N-1} q_{N-1} + r_N \qquad r_N \mid r_{N-2}$ additiv tul. miatt

$r_{N-1} = r_N \cdot q_N + 0 \qquad r_N \mid r_{N-1}$

② $d' \mid a \wedge d' \mid b$

$\Downarrow$

$d' \mid r_1$

$d' \mid r_2$ additiv tul miatt

$d' \mid r_N$

Megj: r_N mindig előállítható: $\boxed{r_N = a x_N + b y_N}$ alakban

$x_N; y_N \in \mathbb{Z}$

2002. XI. 6.

Lnko tulajdonságai:

$a, b, c \in \mathbb{N}^+$

- $(a,a) = a$ idempotens tul.
- $(a,b) = (b,a)$ kommutatívitás
- $((a,b),c) = (a,(b,c))$ asszociativitás

} Lnko, mint művelet tulajdonságai

- $(a,b) \cdot c = (ac, bc)$ disztributív az Lnko a szorzásra nézve
- $(a,b) = (a, b+ca)$
- $(a,b) = a \Leftrightarrow a \mid b$

Biz.: triviális

Nov 14 – 25 → Nincs Csőke !!!

Vizsga: 7 nap /15 fő/nap/

- $((a,b)\,c) = (a,(b,c))$

$a_1, a_2 \dots a_N \in \mathbb{N}^+$

$(a_1, a_2 \dots a_N) := ((a_1; a_2 \dots a_N), a_N)$

Hasonlóan:

$x_1, x_2 \dots x_N \in \mathbb{Z}$, hogy

$a_1x_1 + a_2x_2 + \dots a_Nx_N = (a_1; a_N \dots a_N)$

Spec eset: Ha $(a_1, a_2, a_3 \dots a_n) = 1$ teljesül $\Rightarrow a_1, a_2 \dots a_n$ számok relatív prím egész számok.

Ha $\forall\, i < j \le n$-re $(a_i, a_j) = 1$ teljesül, akkor $a_1, a_2 \dots a_N$ számok páronként relatív prímek.

1., $a, b \in \mathbb{N}^+$

$\left(\frac{a}{(a,b)}; \frac{b}{(a,b)}\right) = 1$ → relatív prímeket ad

Biz.,

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

$(a,b) = c$, $c \neq 0$

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

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

Tétel:

Általánosított prímtulajdonság:

$a, b, c \in \mathbb{N}^+$

$(a, b) = 1, \quad a \mid bc \Rightarrow a \mid c$

Lást: def ✓

$[a, b] > 0$

Tétel: $a, b \in \mathbb{N}^+$

$[a, b] = \frac{a \cdot b}{(a, b)}$ → az Euklidészi algoritmusra alapszik

Biz.:

1; $a \mid \frac{ab}{(a,b)}$ $\quad$ $b \mid \frac{ab}{(a,b)}$ ✓

$\in \mathbb{N}$ $\quad$ $\in \mathbb{N}$ (hiszen, amivel a b-t szorozni megj)

2; m' egy tetszőleges közös többszöröse a és b-nek

$a \cdot c = m' \qquad b \cdot d = m' \qquad c, d \in \mathbb{Z}$

$ac = bd \quad / : (a, b)$

$\frac{a}{(a,b)} \cdot c \quad \frac{b}{(a,b)} \cdot d$

$\frac{a}{(a,b)} \mid \frac{b}{(a,b)} \cdot d$ → mégpedig benne „c"-re

de: $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1 \Rightarrow$ alt. prímtul. miatt $\frac{a}{(a,b)} \mid d$

$\exists \quad e \in \mathbb{Z}$

$\frac{a}{(a,b)} \cdot e = d \Rightarrow b \cdot \frac{a}{(a,b)} e = m'$ $\quad m \mid m'$