Teljesíti a feltételt, így minden számnak osztója

lkkt tul:

- idemp. $a, b, c \in \mathbb{N}^+$
- komm.
- assoc. $\Rightarrow$
- distributivitás $[a, b] \cdot c = [ac, bc]$
- $[a, b] = a \Leftrightarrow b | a$

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

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

XVII

Irreducibilis egész, prímelemem egész

$a \neq 0$, $a \neq \pm 1$ ⟶ FONTOS ⟵ $a \neq 0$, $a \neq \pm 1$

a irreducibilis, ha $b \in \mathbb{Z}$-re igaz, hogy $b | a \Rightarrow$ vagy $b = \pm 1$, vagy $b = \pm a$

⇓

a-nak nincs valódi osztója

csak triviális osztója van.

a prímelem, ha valahányszor osztója egy szorzatnak $\Rightarrow$ mindig osztója a szorzat legalább egyik tényezőjének.

$a | bc \Rightarrow a | b$ vagy $a | c$

$(a | bc$ és $(a, b)) \Rightarrow a | c$

Tétel: Egész számok körében a fenti 2 fogalom megegyezik.

$(\mathbb{Z}, +, \cdot)$ integritás tart.-ban a fenti 2 fogalom fedi egymást

Biz: irred ⇒ prím

$\boxed{\text{prím} \Rightarrow \text{irred}}$ ✓

↳ mindig bizonyítható

lásd: TK!

Megj: prímszám a pozitív prímelem

2, 3, 5, 7, 11 ...

Tétel: számelmélet alaptétele: egyértelmű irreducibilis faktorizáció tétele

$\forall \quad a \in \mathbb{N} \setminus \{0, 1\}$ $(a \geq 2)$ egyértelműen írható fel véges sok prímszám szorzatára (sorrend nem számít, 1 tényezős szorzat is megengedett)

Biz:

létezés biz: ⇒ teljes indukcióval.

egyértelműség biz →

indirekt $\quad \exists \, a \geq 2 \quad a = p_1 \cdot p_2 \cdots p_r$

$a = q_1 \cdot q_2 \cdots q_t$

$p_i, q_i \Rightarrow$ prímek

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_t$$

1, $\left.\begin{array}{l} p_1 \text{ prím} \\ p_1 \mid q_1 \cdot q_2 \cdots q_t \end{array}\right\} \Rightarrow p_1 \mid q_1$ (nem fontos a sorrend, így bármilyen q_i)

de q_1 prím egyben irreducibilis

⇓

osztói: ± 1 és önmaga

↓ nem prím

⇓ $p_1 = q_1$

lehet egyszerűsíteni vele

$p_2 \cdots p_r = q_2 \cdots q_t$

⋮

$r \neq t \quad 1 = \overbrace{q_{r+1} \, q_{r+2} \cdots q_t}^{\text{ezek mind 1-ek, nem prímek}}$

↓

ellentmondás

XVIII. tétel

következmény: $a \geq 2$

$a = p_1$

$p_1^{\alpha_1} \, p_2^{\alpha_2} \cdots p_r^{\alpha_r} \qquad \alpha_i \geq 1$

$\Downarrow$

az „a" nem kanonikus alakja

pl.: $a = p_1^{\beta_1} \cdot \ldots \cdot p_r^{\beta_r} \qquad 0 \leq \beta_i$

$b = p_1^{\gamma_1} \cdots p_r^{\gamma_r} \qquad \underbrace{0 \leq \gamma_i}$

$\downarrow$

prímfaktorizációs alak)

$10 = 2 \cdot 5 \cdot 3^0$

$15 = 2^0 \cdot 5 \cdot 3$

pl.; $(a, b) = \prod_{i=1}^{r} p_i^{\delta_i}$, ahol $\delta_i = \min(\beta_i, \gamma_i)$

$[a, b] \; \prod_{i=1}^{r} p_i^{\varepsilon_i}$, $\varepsilon_i = \max(\beta_i, \gamma_i)$

Tétel: $\forall \, a \geq 4$ összetett egészhez $\exists$ olyan p prímszám, hogy $p \mid a$ és $p \leq \sqrt{a}$

Biz.: a összetett $\Rightarrow \exists$ prímosztója

p prím, hogy $p \mid a \Rightarrow a = p \cdot b \geq p \cdot p \Rightarrow a \geq p^2$

$p \leq b \qquad \sqrt{a} \geq p$

Eratoszthenészi szita:

pl.: ~~1~~, 2, 3, ~~4~~, 5, ~~6~~, 7, ~~8~~, ~~9~~, ~~10~~, 11, ~~12~~, 13

~~14~~, ~~15~~, ~~16~~, 17, ~~18~~, 19, ~~20~~.

bizt. NOR

Tétel: A prímszámok száma végtelen.

Biz. ind.

$p_1, p_2 \dots p_n$ db

$A := p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$

$p_i \nmid A$ $(1 \le i \le n)$ $\lightning$ A számelm. alapt.-tel

———o———

XIX. tétel: bev!

Test fölötti polinomgyűrűk:

$(T; +; \cdot)$ $\qquad (p: T = \mathbb{Q}, \mathbb{R}, \mathbb{C})$

„x" határozatlan

$f(x) := a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ formális összeg, ahol

$a_i \in T$, $n \in \mathbb{N}$.

$f(x)$ T test fölötti polinom (sok tag)

$f(x)$ polinom foka (f°): n, ha $a_n \neq 0$

pl.: $f(x) = 3x^2+1$ $\qquad f^\circ = 2$ $\qquad f^{\circ\circ} = 4$

$g(x) = 2x+1$ $\qquad g^\circ = 1$ $\qquad f^{\circ\circ} = 2$

$t(x) = 3$ $\qquad t^\circ = 0$ $\qquad f^{\circ\circ} = 1$

$h(x) = 0$ $\qquad h^\circ \nexists$ nincs benne olyan együtthatója, ami $\neq 0$, mert minden együtthatója 0.

$h^{\circ\circ} = 0$

módosított fokszám $(f^{\circ\circ})$

$$f^{\circ\circ} := \begin{cases} 2^{f^{\circ\circ}}, & \text{ha } \exists f^\circ \\ 0, & \text{ha } \nexists f^\circ \end{cases}$$

$g(x) = b_n x^n + b_{n-1} x^{n-1} + \dots + b_1 x \, b_0 \qquad b_i \in T$

$f(x) + g(x) := (a_n + b_n)x^n + \dots (a_1 + b_1) x + a_0 + b_0$

$f(x) \cdot g(x) := \dots \quad (a_1 b_0 + a_0 b_1) x + a_0 b_0$

$T_{[x]} := \{ f(x) \mid f(x) = a_n x^n + \dots a_0 \; , \; a_i \in T \}$

$\downarrow$

összes olyan polinom, aminek az

együtthatói a testből kerülnek ki.

VIZSGA IDŐ:

~~XII. 30 prog~~ progr.: XII. 30, I. 8, I. 15

I. 3., I. 10; I. 17; I. 22.

UV.: I. 29-30.

Tétel: $(T_{[x]}, +, \cdot)$ integritás tartomány

~~XIX~~ XIX

Biz: ✓

Megj: A $(\mathbb{Z}[x] \,;\, + ; \cdot)$ is integritás tartomány

$\mathbb{Z}[x] \subset \mathbb{Q}_{[x]} < \mathbb{R}_{[x]} < \mathbb{C}_{[x]}$

Polinomok között nincs rendezés csak a fokszámaik között.

XIX. tétel

Maradékos osztás tétele $T_{[x]}$-ben:

$f(x), g(x) \in T_{[x]}$ $\;g(x) \neq 0$ -hoz egyértelműen létezik $q(x), r(x) \in T_{[x]}$, hogy

$$f(x) = g(x) \cdot q(x) + r(x), \text{ ahol}$$

$$r^{\circ\circ} < g^{\circ\circ} \quad (r^\circ < g^\circ \text{ vagy } r(x) = 0)$$

$r^{\circ\circ} \Rightarrow r$ módosított foka

Biz: lásd TK!

pl.: $\overbrace{(3x^4 - 2x^3 + 3x^2 - x + 1)}^{f(x)} : \overbrace{(x^2 - 2x + 3)}^{g(x)} = \underbrace{3x^2 + 4x + 2}_{q(x)}$

$$\begin{array}{l}
-(\cancel{3x^4} - 6x^3 + 9x^2) \\
\quad \cancel{4x^3} - 6x^2 - x + 1 \\
\quad -(\cancel{4x^3} - 8x^2 + 12x) \\
\qquad \cancel{2x^2} - 13x + 1 \\
\qquad -(\cancel{2x^2} - 4x + 6) \\
\qquad\quad \underbrace{-9x - 5}_{r(x)} \text{ maradék}
\end{array}$$

$f(x) = g(x) \cdot q(x) + r(x)$

Euklidészi algoritmus:

$$f(x) = g(x)\cdot q_0(x) + r_1(x)$$

$$g(x) = r_1(x)\cdot q_1(x) + r_2(x)$$

$$\vdots$$

$$r_{n-2}(x) = r_{n-1}(x)\cdot q_{n-1}(x) + r_n(x) \qquad g^\circ > r_1^\circ > r_2^\circ > \dots > r_n^\circ$$

$$r_{n-1}(x) = r_n(x)\cdot q_n(x) + 0 \qquad r_n(x) \neq 0$$

$$\Downarrow$$

$\exists\ X_n(x),\ Y_n(x) \in T[x]$

$$r_n(x) = f(x)X_n(x) + g(x)Y_n(x)$$

XX. tétel

Oszthatóság $T[x]$-ben:

$f(x)$ osztója $g(x)$-nek, ha $\exists\ h(x)$, amelyre $f(x)\cdot h(x) = g(x)$

$f(x) \mid g(x)$ tagadása $f(x) \nmid g(x)$

Def. XIV

T. „|" tulajdonságai:

- reflexív ✓
- nem szimmetrikus $(f(x) \mid g(x) \not\Rightarrow g(x) \mid f(x))$
- nem antiszimm $(f(x) \mid g(x) \wedge g(x) \mid f(x) \not\Rightarrow f(x) = g(x))$
- tranzitivitás ✓
- $f(x) \mid g(x),\ g(x) \mid f(x) \Rightarrow f(x) \simeq g(x) \quad c \in T \setminus \{0\}$

csak a konstansban térhet el, ami nem 0.

—o—

$1 \mid f(x)$

$e(x) \mid 1 \Rightarrow e(x) = c \in T \setminus \{0\}$

↳ tetszőleges nem 0 konstans

Két polinom asszociált, ha nem 0 konstansban térnek csak el.

$f(x) \sim g(x)$, ha $\exists\ c \in T \setminus \{0\}$, hogy $f(x) = c \cdot g(x)$ ✓

0-val kapcs. tul. lásd Z-nél!

$f(x)\,;\,g(x) \neq 0$ lnko-ja $d(x) \in T[x]$

1, $d(x) \mid f(x)$, $d(x) \mid g(x)$

$\forall\, d'(x)$, ha $\underbrace{d'(x) \mid f(x) \wedge d'(x) \mid g(x)}$

$\Downarrow$

$d'(x) = d(x)$

Tétel:

$(f(x)\,;\,g(x)) = d(x) = 1x^n$ Azt választjuk, ahol a főegyütthatója 1.

$\Downarrow$

normált polinom.

lkkt. ✓ → XXI.

prímelem, irreducibilis elem XXII

$\underbrace{p(x) \in T[x] \setminus T}_{p(x) \text{ legalább elsőfokú}}$

↳ a 0-t és a nemzérokonstanst vonjuk ki.

pl.: elsőfokú polinom prím, ha ....

Ha a p(x) legalább elsőfokú polinom és nincs valódi faktorizáció,

⇒ irreducibilis.

Ha nem lehet felbontani legalább elsőfokú polinomok szorzatára

Tétel: $T[x]$-ben az irreducibilis és prímelemek azonosak.

Biz.: Lásd TK!

XXII.

Polinomelmélet alaptétele: $\forall$ legalább elsőfokú polinom egyértelműen írható fel konstansszorzótól eltekintve véges sok prím vagy irreducibilis elemére.

Konkrét testek fölötti prímpolinomok diszkussióját lásd az algebrai egyenletek témakör után

XXI.

Euklideszi gyűrűk:

Def.: $(\overset{\text{végtelen gyűrűk „halmaza”}}{R}; +; \cdot)$ integritástartomány euklideszi gyűrű, ha létezik olyan f leképezés, úgy, hogy $f: R \to \mathbb{N}$

$$1: \; f(a) = \underbrace{0}_{\in \mathbb{N}} \iff \overset{\in R}{a = 0}$$

$$2; \; f(a \cdot b) = f(a) \cdot f(b)$$

$$3; \; a; b \neq 0 \in R \quad \exists\, q, r \in R, \text{ hogy}$$

$$a = bq + r, \text{ ahol } f(r) < f(b)$$

↓ maradékos osztás tétele.

ezt a f-t euklideszi normának nevezzük.

pl.:

$(\mathbb{Z}; +; \cdot)$	$(T_{[x]}; +; \cdot)$
„f” az $\lvert\ \rvert$ abszolút érték	„f”: a módosított fokszám
$\lvert a \rvert = 0 \iff a = 0$	$f^{\circ\circ} = 0 \iff f(x) = 0$
$\lvert a \cdot b \rvert = \lvert a \rvert \cdot \lvert b \rvert$	$(f \cdot g)^{\circ\circ} = f^{\circ\circ} \cdot g^{\circ\circ}$
$a = bq + r;\ 0 \le r < \lvert b \rvert$	$f(x) = g(x) \cdot q(x) + r(x) \quad r^{\circ\circ} < g^{\circ\circ}$

Minden zérustól és egységtől különböző $\overset{\text{gyűrűbeli}}{\vee}$ elem a tényezők sorrendjétől eltekintve egyértelműen írható fel.

XXIII

Kongruencia $\mathbb{Z}$-ben

m fix ; $m \in \mathbb{Z}$; $m \geq 2$ m = modulus

$a, b \in \mathbb{Z}$: a kongruens b-vel modulo m, ha $m | a-b$.

jelölés: $\underset{\substack{\uparrow \\ \text{kongruens}}}{a \equiv b}$ $(\text{mod } m)$

pl.: $m = 6$

$7 \not\equiv 12 \pmod 6$

$18 \equiv 24$ mod 6 ✓ $6 | 24-18$

„ $\equiv$ " egy reláció $(\mathbb{Z}; +; \cdot)$ integritás tart.-ban

Tétel: „ $\equiv$ " kongruenciareláció $(\mathbb{Z}; +; \cdot)$-ban

Biz.: $\underbrace{\text{reflx, szimm, trans}}_{\text{ekvivalencia}}$, additív, multiplik.

$a \equiv b \pmod m \wedge c \equiv d \pmod m \Rightarrow a+c \equiv b+d \pmod m$

— " — $\Rightarrow a \cdot c \equiv b \cdot d \pmod m$

Kongruenciarel.

$\mathbb{Z}/m = \{\bar{a}, \bar{b}, \bar{c} \dots\}$

Maradékosztály:

Tétel: $a_1, a_2 \in \bar{a} \Leftrightarrow$, ha $a_1 = mq_1 + r$ és $a_2 = mq_2 + r$

$0 \leq r < m$

Két elem akkor esik be a maradékosztályba, ha m-mel osztva ugyanazt a maradékot adják.

Biz.: ind. $\Rightarrow a_1 - a_2 = m(q_1 - q_2) + r_1 - r_2$ $\rightarrow 1 \leq r_1 - r_2 \leq n-1$ ellentmondás $\Rightarrow r_1 = r_2$

$a_1 \equiv a_2 \pmod m \Rightarrow m | a_1 - a_2$ $\rightarrow m | m(q_1 - q_2)$

$\Leftarrow$

$\mathbb{Z}_{/(m)} = \{\bar{0}, \bar{1}, \dots \overline{m-1}\}$

$\Downarrow$

maradékosztály

$(\mathbb{Z}_{/m}; +; \cdot) \Rightarrow$ $\bar{a} + \bar{b} = \overline{a+b}$

$\bar{a} \cdot \bar{b} = \overline{a \cdot b}$

$\Downarrow$

GYŰRŰ

pl.: $m = 6$

$\bar{2} \cdot \bar{3} = \bar{6} = \bar{0}$

$\Downarrow$

pl.: $(\mathbb{Z}_{/6}; +; \cdot)$ nem integritástartomány, mert van benne zérusosztó

pl.: $(\mathbb{Z}_{/(p)}; +; \cdot)$ TEST

$\downarrow$

prím

Ha a modulus prímszám → TESTET kapunk.

Bármennyi = végtelen sok test van ⇒ prímmel elosztva a maradékosztályt, végtelen sok test lesz. (Eddig: racionális, valós, komplex)

$(\{\bar{0}, \bar{1}\}; +; \cdot)$ $\mathbb{Z}_{(2)}$ test