1. előadás

33. tétel

Kongruencia $\mathbb{Z}$-ben:

Def.: $a, b, m \in \mathbb{Z}$ m fix $(m \geq 2)$

$a \equiv b \pmod{m} \overset{def}{\iff} m \mid a-b$

integritástartomány
+, · művelet ért. van.

Tul.: – a $(\mathbb{Z}; +; \cdot)$-ban a „$\equiv$" kongruenciareláció
refl. szim., tr. add, multipl.
(5)

– a modulussal kapcsolatos tulajdonságok

- $a \equiv b \pmod{m} \wedge m_1 \mid m \Rightarrow a \equiv b \pmod{m_1}$
- $ca \equiv cb \pmod{m} \wedge c \neq 0 \Rightarrow a \equiv b \left(\bmod \frac{m}{(m, c)}\right)$
- $a \equiv b \pmod{m_1} \wedge a \equiv b \pmod{m_2} \Rightarrow a \equiv b \pmod{[m_1, m_2]}$

Köv: $(\mathbb{Z}, +, \cdot)$-ban „$\equiv$" létrehoz egy KOMPATIBILIS OSZTÁLYOZÁST.

$\mathbb{Z}/_\rho = \mathbb{Z}/_{(m)} = \{\bar{a}, \bar{b}, \bar{c} \ldots\}$; $\quad \bar{a} + \bar{b} := \overline{a+b}$

faktorhalmaz — ezen modulusra véve a faktorhalmaz $\quad \bar{a} \cdot \bar{b} := \overline{a \cdot b}$

maradékosztály → kongruencia osztályai (elemei)

Tétel: $a \equiv b \pmod{m} \iff a = mq_2 + r \wedge b = mq_2 + r$, ahol $0 \leq r \leq m-1$
legkisebb nem negatív maradék

$$\boxed{\mathbb{Z}/_{(m)} = \{\bar{0}, \bar{1}, \bar{2} \ldots \overline{m-1}\}}$$

teljes reprezentánsrendszer → minden osztályból 1 elemet reprezentálunk

nevezetes teljes reprezentánsrendszer:
- $0, 1, 2 \ldots m-1$ — legkisebb negatív
- $1, 2 \ldots m$ — legkisebb pozitív
- $0, \pm 1, \pm 2 \ldots \pm \frac{m-1}{2}$ — legkisebb abszolút

} reprezentáns rendszer

$(\mathbb{Z}/_{(m)}; +, \cdot)$ tulajdonságai:

Tétel: $(\mathbb{Z}, +, \cdot)$ integritástartomány

$f: \mathbb{Z} \to \mathbb{Z}/_{(m)}$ $\quad (a \mapsto \bar{a})$

→ term. homomorfizmus

$\forall\, a, b \in \mathbb{Z}$

$-\ f(a+b) = f(a) + f(b)$ gyűrű

$-\ f(a \cdot b) = f(a) \cdot f(a)$ ✓ teljesül

$(\mathbb{Z}/_{(m)}; +, \cdot)$

integr. tart.

kommut., egységelemes, gyűrű, zérusosztómentes!

faktorstruktúra

De: zérusosztóság külön vizsgálandó!

pl.: $m = 4 \Rightarrow \bar{2} \cdot \bar{2} = \bar{4} = \bar{0}$ nonat (?) értéke lehet úgy 0, hogy egyik kép eleme se 0.

$(\mathbb{Z}/_{(4)}, +, \cdot)$ zérusosztós

$m = 5$ $\quad \bar{a}, \bar{b} \in \mathbb{Z}/_{(5)} \setminus \{\bar{0}\}$ $\quad \bar{a}\bar{b} \neq \bar{0}$ $\quad (\mathbb{Z}/_{(5)}, +, \cdot)$ zérusosztómentes

SŐT:

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

zéruselem kivételével minden elemnek van inverze.

$(\mathbb{Z}/_{(5)}; +, \cdot)$ test

Tétel: $(\mathbb{Z}_{/(m)}; +; \cdot) \Leftrightarrow$ test, ha m prímszám.

BIZ.:

1, Legyen m összetett $(m = m_1 \cdot m_2 \quad : 2 \leq m_1 \leq m_2 \leq m)$

állítjuk: $\overline{m_1}$-nek $\nexists$ multiplikatív inverze $\Rightarrow (\mathbb{Z}_{/(m)}, +, \cdot)$ nem test

indirekt:

Tfh: $\overline{m_1} \cdot k = \overline{1} \Leftrightarrow m_1 \cdot k \equiv 1 \pmod m$

$m_1 \cdot k - 1 = -my \quad y \in \mathbb{Z}$

$\underbrace{m_1 k}_{m_1 |} + \underbrace{my}_{m_1 | \, (m_1 | m)} = 1$

$m_1 | 1 \; ↯ \; 2 \leq m_1$

m_1, m_2: zérusosztók.

2, $m = p$ prímszám

$\mathbb{Z}_{/(p)} \setminus \{\overline{0}\} = \{\overline{1}, \overline{2}, \dots, \overline{p-1}\} = P_p$ -redukált maradékosztály $\Rightarrow (P_p, \cdot)$ csop ✓

$(\mathbb{Z}_{/(p)}; +; \cdot)$ test

A legkisebb test: $(\mathbb{Z}_{/(2)})$

Tétel:

Wilson-féle prímkritérium:

$m \geq 2$ egész $\Leftrightarrow$ prímszám ha $(m-1)! \equiv -1 \pmod m$

BIZ:

I. m összetett $\quad m = m_1 \cdot m_2 \quad (2 \leq m_1 \leq m_2 < m)$

ind

$(m-1)! \equiv -1 \pmod m \Rightarrow (m-1)! \equiv -1 \pmod{m_1}$

de $(m-1)! = 1 \cdot 2 \cdot 3 \dots m_1 \dots (m-1) \equiv 0 \pmod m$

benne van m_1

$1 \equiv 0 \pmod{m_1} \Rightarrow m_1 \mid 1$ ↯ $2 \leq m_1$

II. $m = p$ prímszám

$m = p = 2$ $\qquad (2-1)! \equiv -1 \pmod 2$

$$1 \equiv -1 \pmod 2$$
$$2 \equiv 0 \pmod 2 \checkmark$$

$m = p = 3$ $\qquad (3-1)! \equiv 1 \pmod 3$

$$3 \equiv 0 \pmod 3 \checkmark$$

$m = p \geq 5$:

$$\overline{(p-1)!} = \overline{1} \cdot \overline{2} \cdot \overline{3} \cdots \overline{(p-1)}$$

$$\left.\begin{array}{l} \overline{1} \cdot \overline{1} = \overline{1} \checkmark \\ \overline{(p-1)}\,\overline{(p-1)} = \overline{p^2 - 2p + 1} = \overline{1} \end{array}\right\} \left(\mathbb{Z}_{(p)} \setminus \{\overline{0}\}\right) \qquad \begin{array}{l} \overline{1} \text{ inv} = \overline{1} \\ \overline{p-1} \text{ inv} = \overline{p-1} \end{array}$$

Segédtétel:

$2 \leq m_1 \leq \overset{p-2}{(p-1)-1}$ $\qquad \overline{m_1} \cdot \overline{m_1} \neq \overline{1}$

ind

$$\overline{m_1} \cdot \overline{m_1} = \overline{1}$$

$$m_1^2 \equiv 1 \pmod p$$

$$p \mid (m_1^2 - 1) = (m_1 + 1)(m_1 - 1)$$

Mivel p prím $\Rightarrow p \mid \underbrace{m_1 + 1}_{3 \leq \ \leq p-1} \vee p \mid \underbrace{m_1 - 1}_{1 \leq \ \leq p-3}$

ell ↯ ezek között nincsenek p-vel osztható számok

$$\overline{(p-1)}! = \overline{1} \cdot \overline{2} \cdot \overline{3} \cdot \overline{0} \cdots \overline{p-1} = \overline{p-1}$$

$$\boxed{(p-1)! \equiv p-1 \equiv -1 \pmod p}$$

ha prím − 1-el kongruens.

<u>Jót</u> $(m-1)! = \begin{cases} 2 ; & \text{ha } m=4 \\ 0 ; & \text{ha } m>4 \text{ összetett} \\ -1 , & \text{ha } m=p \text{ prímszám} \end{cases}$

lsd: TK

---

34. tétel

Euler-féle φ fgv:

$\varphi : \mathbb{N}^+ \to \mathbb{N}^+$ $\left(\begin{array}{l} \varphi(1) = 1 \\ \varphi(m) = |P(m)| , \text{ ha } m \geq 2 \end{array} \right)$ m modulusra képest relatív prímek számát jelöli a φ.

$P(m) = \{ r_1, r_2 \ldots \}$

$(r_i, m) = 1 .$ $r_i \not\equiv r_j \pmod m$
$i \neq j$

/ $\varphi(m)$ jelöli a $0, 1, 2 \ldots m-1$ sorozatban az m-hez relatív prímek számát /

Tétel: $a, b \in \mathbb{N}^+$ $(a, b) = 1$

$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$

(a „φ" fgv multiplikatív)

Ha $m = p$ prímszám $\Rightarrow \varphi(p) = p-1$

$m = p_1^{\alpha_1} \ldots p_r^{\alpha_r} \Rightarrow \varphi(m) = \prod_{i=1}^{r} \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1} \right)$

Euler-Fermat-féle kongruencia tétel:

$(a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \pmod m$

Speciális eset:

Kis Fermat-tétel:

$n = p$ prím

- $(a, p) = 1 \Rightarrow a^{p-1} \equiv 1 \pmod p$

- $\times$ nincs feltétel $\quad a^p \equiv a \pmod p$ ↳ beszorozva a-val

? Prímkritérium-e a kis Fermat-tétel? Nem!

11.19. 2. előadás

Igaz-e a megfordítás?

$(a, n) = 1$

$a^{n-1} \equiv 1 \pmod n \Rightarrow n$ prím

VÁLASZ: NEM! mert pl.:

$n = 341 = 11 \cdot 31 \qquad a = 2;$

$(2, 341) \qquad 2^{340} \equiv 1 \pmod{341}$

biz.:
$2^{340} \equiv (2^{10})^{34} \equiv 1^{34} \equiv 1 \pmod{11}$ → kis-Fermat tétel szerint
$2^{340} \equiv (2^5)^{68} \equiv 1 \pmod{31}$ ⇒

$2^5 = 32$

$\Rightarrow 2^{340} \equiv 1 \pmod{341}$ (SARRUS 1819)

⇓

emiatt nem prímkritérium

nem prím a 341, mégis teljesíti a feltételt.

Def.: n összetett szám (pozitív egész), $(2, n) = 1 \Rightarrow n$ páratlan

Ha $2^{n-1} \equiv 1 \pmod{n}$ akkor pszeudoprímnek nevezzük.

majdnem prím
álprím

A legkisebb pszeudoprím a 341.

Sierpiński (1947)

Tétel: Ha n pszeudoprím $\Rightarrow N = 2^n - 1$ is pszeudoprím

Következmény: végtelen sok pszeudoprím létezik.

BIZ.:

1; $N = 2^n - 1$ összetett

Mivel n pszeudoprím $\Rightarrow n$ összetett $(n = n_1 \cdot n_2)$ $(n_1, n_2 \geq 2)$ → n páratlan

$$N = 2^n - 1 = 2^{n_1 n_2} - 1 = (2^{n_1})^{n_2} - 1 = \underbrace{(2^{n_1} - 1)}_{\geq 7} \cdot \underbrace{A}_{\geq 3}$$

n legkisebb értéke 3.

ÖSSZETETT → felírható 2 szám szorzataként.

2; $N \mid 2^{N-1} - 1$?

$$2^{N-1} - 1 = 2^{2^n - 1 - 1} - 1 = 2^{2(2^{n-1} - 1)} - 1 = *$$

De: $n \mid 2^{n-1} - 1$ → felírható $n \cdot q$, mivel n az osztója

nem szükséges kiírni

$$* = 2^{2nq} - 1 = (2^n)^q - 1^q = \underbrace{(2^n - 1)}_{N} B$$

(A következmény igaz) a TÉTEL IS IGAZ!

SÖT: (Lehmer)

$P_1(x) := \{ n \mid n \text{ pseudoprím és } n < x \}$, $x \in \mathbb{R}^+$

x-nél kisebb pseudoprímek halmaza

$\exists$ $x_0 \in \mathbb{R}^+$ és $c \in \mathbb{R}$, hogy $|P_1(x)| > c \cdot \log x$, ha $x > x_0$

term. alapú „log" = „ln"

(két logaritmus csak a konstansban tér el egymástól $\Rightarrow$ mindegy milyen alapú)

($P_1(x)$-hez minoráltunk egy dolgot, ami tolja maga előtt. $\Rightarrow$ meghatároztuk)

BIZ.: —

100000 mennyi pprím van? annyi, mint $c \cdot \log 100000$.

- Mersenne-féle számok: $M_p = 2^p - 1$, ahol p prímszám
- Fermat-féle számok: $F_n = 2^{2^n} + 1$, ahol $n = 0, 1, 2 \dots$

$\to$ F_0, F_1, F_2, F_3, F_4 valós prím $\Rightarrow$ sejtése: mindig prímek ezek a számok

Euler: F_5 már nem prím

Ma több Fermat-prím nem ismert, de az sem bizonyított, hogy $\nexists$.

pl.: $M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89$

Mj.: Ma 34db Mersenne-féle prímszámot ismer a matematika.

Tétel: Mind a Mersenne, mind a Fermat-féle számok vagy prímek, vagy pszeudoprímek.

BIZ.: LSD TK!

(A Mersenne v. a Fermat-féle számok mindig teljesítik a kis-Fermat tételt.)

Általánosan:

$(a,n) = 1$, $(a \geq 2)$ n összetett

Ha $a^{n-1} \equiv 1 \pmod{n}$ $\Rightarrow$ n-et „a" vonatkozású pszeudoprímnek nevezzük.

(A 341 = 2-re nézve pszeudoprím, de 3-ra nézve már nem pprím)
Lsd TK.

Sok számok, amelyek $\forall$ a-ra pszeudoprímek o. prímek, mindig teljesül).

n abszolút pszeudoprím, ha $\forall$ a-ra $(a,n)=1$ „a"-ra vonatkozóan pprím.

pl.: $561 = 3 \cdot 11 \cdot 17$ $a^{560} \equiv 1 \pmod{561}$

legkisebb

(biz-ható)

Carmichael-féle számok = abszolút pprímek.

$P_2(x) := \{ n \mid n$ abszolút pprím, $n < x \}$ $x \in \mathbb{R}^+$

Ha x elég nagy (megadható olyan korlát, amitől nagyobb) $\Rightarrow$
$\Rightarrow \underbrace{|P_2(x)|}_{(\text{ha } x \to \infty \Rightarrow x^{\frac{2}{7}} \to \infty)} > x^{\frac{2}{7}}$

pprím: pszeudoprím

Abszolút pprímekből végtelen sok van.

Algebrai kongruenciák:

35. tétel

(algebrai egyenlet : polinom = 0.)

$f(x) \in \mathbb{Z}[x]$; $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$

! $m \geq 2$ fix egész (a modulusra nézve)

– $f(x)$ modulo m foka n, ha $a_n \not\equiv 0 \pmod{m}$

(*) $\forall i$ $(0 \leq i \leq n)$-re $a_i \equiv 0 \pmod{m}$ $\Rightarrow$

$f(x)$-nek $\nexists$ modulo m foka

$6x^{83} + 27x^2 + 2x^1 + 1$ modulo 3 foka : 1

osztható 3-mal

– " – modulo 5 foka : 83

Def.: $f(x) \equiv 0 \pmod{m}$ n-edfokú algebrai kongruencia, ha $a_n \equiv 0 \pmod{m}$

↓ legalább elsőfokú $n \geq 1$

Ha x_0 egészre igaz $f(x_0) \equiv 0 \pmod{m}$ $\Rightarrow$ x_0 megoldás

(Algebra alaptétele !!!) – komplex nulák halmaz van gyöke minden n-edfokú egyenletnek $n \geq 1$

De: $15x \equiv 4 \pmod{12}$ → elsőfokú kongruencia $12 \nmid 15$

$x_0 \not\equiv 0$

$x_0 \not\equiv \pm 1$

$\vdots$

12 | 15.5 th

$x_0 \not\equiv \pm 5$

$x_0 \not\equiv 6$ → 12 maradékosztály