

DISZKRÉT MATEMATIKA II ELŐADÁS

Waldhauser Tamás

SZTE Bolyai Intézet

2026. február 26.

Tartalom

Bemelegítés

Lineáris kongruenciarendszerek

Maradékosztályok és maradékrendszerek

Számolás maradékosztályokkal

Redukált maradékosztályok, multiplikatív inverz, rend

CS teszt: 2. előadás - milyennap

Ma csütörtök van, 1 nap múlva péntek lesz, 2 nap múlva szombat, ...

Milyen nap lesz 71439 nap múlva?

- wifi hálózat (SSID): Kiss Arpad terem GUEST
- jelszó: 12345678
- coospace: Diszkrét matematika 2. ea. színtér



Tartalom

Bemelegítés

Lineáris kongruenciarendszerek

Maradékosztályok és maradékrendszerek

Számolás maradékosztályokkal

Redukált maradékosztályok, multiplikatív inverz, rend

1	2	3	4	5	6	7	8	9	10	...
H	K	Sze	Cs	P	Szo	V	H	K	Sze	...
										...

Kérdés

Fogok-e valaha kedden kosarazni?

Válasz

$$\left. \begin{array}{l} x \equiv 2 \pmod{7} \\ x \equiv 3 \pmod{4} \end{array} \right\} \iff x \equiv 23 \pmod{28}$$

A 23. napon fogok először kedden kosarazni (és onnantól 28 naponta).

1	2	3	4	5	6	7	8	9	10	...
H	K	Sze	Cs	P	Szo	V	H	K	Sze	...
										...
										...

Kérdés

Fogok-e valaha egy napon pizzát enni és kosarazni?

Válasz

$$\left. \begin{array}{l} x \equiv 6 \pmod{6} \\ x \equiv 3 \pmod{4} \end{array} \right\} \text{ nincs megoldása}$$

Nem fogok soha egy napon pizzát enni és kosarazni.

1	2	3	4	5	6	7	8	9	10	...
H	K	Sze	Cs	P	Szo	V	H	K	Sze	...
										...
										...

Kérdés

Fogok-e valaha egy napon almát enni és kosarazni?

Válasz

$$\left. \begin{array}{l} x \equiv 5 \pmod{6} \\ x \equiv 3 \pmod{4} \end{array} \right\} \iff x \equiv 11 \pmod{12}$$

A 11. napon fogok először egy napon almát enni és kosarazni (és onnantól 12 naponta).

1	2	3	4	5	6	7	8	9	10	...
H	K	Sze	Cs	P	Szo	V	H	K	Sze	...
										...
										...

Kérdés

Fogok-e valaha hétfőn almát enni és kosarazni?

Válasz

$$\left. \begin{array}{l} x \equiv 5 \pmod{6} \\ x \equiv 3 \pmod{4} \\ x \equiv 1 \pmod{7} \end{array} \right\} \iff \left. \begin{array}{l} x \equiv 11 \pmod{12} \\ x \equiv 1 \pmod{7} \end{array} \right\} \iff x \equiv 71 \pmod{84}$$

A 71. napon fogok először hétfőn almát enni és kosarazni.

Lineáris kongruenciarendszer

Definíció

Adott a_i, b_i, n_i ($i = 1, 2, \dots, k$) egész számok esetén az alábbi „egyenletrendszert” **lineáris kongruenciarendszernek** nevezzük:

$$\left. \begin{array}{l} a_1 x \equiv b_1 \pmod{n_1} \\ \vdots \\ a_k x \equiv b_k \pmod{n_k} \end{array} \right\}$$

Megjegyzés

Ha a rendszer valamelyik kongruenciájának nincs megoldása, akkor a rendszernek sincs. Ha minden kongruenciának van megoldása, akkor egyenként megoldva őket, ilyen alakú kongruenciarendszert kapunk:

$$\left. \begin{array}{l} x \equiv c_1 \pmod{m_1} \\ \vdots \\ x \equiv c_k \pmod{m_k} \end{array} \right\}$$

(Az itt szereplő modulusok nem feltétlenül ugyanazok, mint a fentiek!)

Lin. kongrsz.: megoldhatóság és általános megoldás

Az

$$\left. \begin{array}{l} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{array} \right\}$$

kongruenciarendszer átfogalmazható az $x = my + a = nz + b$ diofantoszi egyenletre. Rendezve:

$$my - nz = b - a.$$

Ebből következik, hogy...

- akkor és csak akkor van megoldás, ha $\text{lko}(m, n) \mid a - b$;
- ha $x_0 = my_0 + a = nz_0 + b$ egy megoldás, akkor az általános megoldás

$$y = y_0 + \frac{n}{\text{lko}(m, n)} \cdot t, \quad z = z_0 + \frac{m}{\text{lko}(m, n)} \cdot t,$$

$$x = x_0 + \frac{mn}{\text{lko}(m, n)} \cdot t = x_0 + \text{lkt}(m, n) \cdot t \quad (t \in \mathbb{Z}),$$

ami így fogalmazható meg kongruenciával:

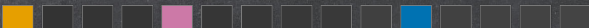
$$x \equiv x_0 \pmod{\text{lkt}(m, n)}.$$

CS teszt: 2. előadás - sorminta

Igazak-e az alábbi állítások a sormintára?

1. Van a 0-s oszlopban rózsaszín négyzet.
2. Van az 1-es oszlopban rózsaszín négyzet.
3. Van a 2-es oszlopban kék négyzet.
4. Van a 7-es oszlopban kék négyzet.
5. Van a 9-es oszlopban narancssárga négyzet.

sorok hossza (m): minta hossza (n):

minta: 

0	1	2	3	4	5	6	7	8	9	10	11
12	13	14	15	16	17	18	19	20	21	22	23
24	25	26	27	28	29	30	31	32	33	34	35

CS teszt: 2. előadás - sorminta

Igazak-e az alábbi állítások a sormintára?

- | | |
|---|------|
| 1. Van a 0-s oszlopban rózsaszín négyzet. | Nem |
| 2. Van az 1-es oszlopban rózsaszín négyzet. | Igen |
| 3. Van a 2-es oszlopban kék négyzet. | Nem |
| 4. Van a 7-es oszlopban kék négyzet. | Igen |
| 5. Van a 9-es oszlopban narancssárga négyzet. | Igen |

sorok hossza (m): minta hossza (n):

minta: 

0	1	2	3	4	5	6	7	8	9	10	11
12	13	14	15	16	17	18	19	20	21	22	23
24	25	26	27	28	29	30	31	32	33	34	35

Lin. kongrsz.: megoldhatóság és általános megoldás

Tétel

Tekintsük az alábbi kongruenciarendszert.

$$\left. \begin{array}{l} x \equiv c_1 \pmod{m_1} \\ \vdots \\ x \equiv c_k \pmod{m_k} \end{array} \right\}$$

- A kongruenciarendszernek akkor és csak akkor van megoldása, ha

$$\forall i, j: \text{lko}(m_i, m_j) \mid c_i - c_j.$$

- Ha van megoldás, akkor a megoldások egyetlen maradékosztályt alkotnak modulo $\text{lkt}(m_1, \dots, m_k)$. Tehát ha x_0 egy megoldás, akkor az általános megoldás így fest:

$$x \equiv x_0 \pmod{\text{lkt}(m_1, \dots, m_k)}.$$

Kínai maradéktétel

Tétel

Tekintsük az alábbi kongruenciarendszert.

$$\left. \begin{array}{l} x \equiv c_1 \pmod{m_1} \\ \vdots \\ x \equiv c_k \pmod{m_k} \end{array} \right\}$$

- Ha a modulusok páronként relatív prímek, akkor a $c_1, \dots, c_k$ számoktól függetlenül mindig van megoldás.
- Modulo $m_1 \cdot \dots \cdot m_k$ egyetlen megoldás van.

Tartalom

Bemelegítés

Lineáris kongruenciarendszerek

Maradékosztályok és maradékrendszerek

Számolás maradékosztályokkal

Redukált maradékosztályok, multiplikatív inverz, rend

Emlékeztető

A modulo m kongruencia ekvivalenciareláció az egész számok halmazán.

Két szám akkor és csak akkor kongruens modulo m , ha ugyanazt a maradékot adják m -mel osztva.

Ezért itt az ekvivalenciaosztályokat **modulo m maradékosztályoknak** nevezzük.

Példa

A modulo 3 maradékosztályok:

$$\bar{0} = \{ \dots, -6, -3, 0, 3, 6, 9, 12, \dots \}$$

$$\bar{1} = \{ \dots, -5, -2, 1, 4, 7, 10, 13, \dots \}$$

$$\bar{2} = \{ \dots, -4, -1, 2, 5, 8, 11, 14, \dots \}$$

Definíció

Egy a egész szám **modulo m maradékosztálya** a következő halmaz:

$$\bar{a} = \{b \in \mathbb{Z} : b \equiv a \pmod{m}\} = \{a + km : k \in \mathbb{Z}\}.$$

A modulo m maradékosztályok halmazát $\mathbb{Z}_m$ jelöli:

$$\mathbb{Z}_m = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}.$$

Megjegyzés

A definícióból világos, hogy tetszőleges a, b egész számok esetén

$$\bar{a} = \bar{b} \iff a \equiv b \pmod{m}.$$

Példa

$$\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\} = \{\bar{1}, \bar{2}, \bar{3}\} = \{\overline{-325}, \overline{1707}, \overline{1777}\}$$

CS teszt: 2. előadás - maradékosztályok

Igazak-e az alábbi állítások?

A felülvonások mindenütt modulo 4 maradékosztályt jelentenek.

1. $\overline{2} = \overline{-2}$

2. $\overline{2026} = \overline{0}$

3. $7 \in \overline{3}$

4. $\mathbb{Z}_4 = \{\overline{10}, \overline{11}, \overline{12}, \overline{13}\}$

5. $\mathbb{Z}_4 = \{\overline{10}, \overline{20}, \overline{30}, \overline{40}\}$

6. $\mathbb{Z}_4 = \{\overline{11}, \overline{22}, \overline{33}, \overline{44}\}$

CS teszt: 2. előadás - maradékosztályok

Igazak-e az alábbi állítások?

A felülvonások mindenütt modulo 4 maradékosztályt jelentenek.

1. $\overline{2} = \overline{-2}$ Igen

2. $\overline{2026} = \overline{0}$ Nem

3. $7 \in \overline{3}$ Igen

4. $\mathbb{Z}_4 = \{\overline{10}, \overline{11}, \overline{12}, \overline{13}\}$ Igen

5. $\mathbb{Z}_4 = \{\overline{10}, \overline{20}, \overline{30}, \overline{40}\}$ Nem

6. $\mathbb{Z}_4 = \{\overline{11}, \overline{22}, \overline{33}, \overline{44}\}$ Igen

Tartalom

Bemelegítés

Lineáris kongruenciarendszerek

Maradékosztályok és maradékrendszerek

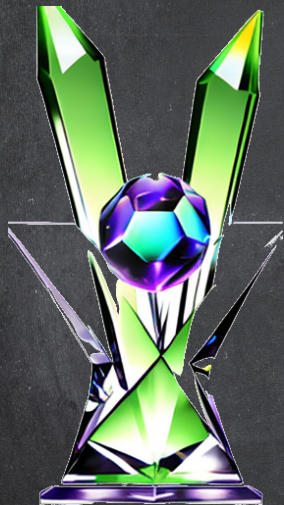
Számolás maradékosztályokkal

Redukált maradékosztályok, multiplikatív inverz, rend

Varázsgömb



Varázsgömb



Emlékeztető

A kongruenciareláció egy fontos tulajdonsága:

$$\left. \begin{array}{l} a_1 \equiv b_1 \pmod{m} \\ a_2 \equiv b_2 \pmod{m} \end{array} \right\} \implies \begin{array}{l} a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{m} \text{ és} \\ a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m}. \end{array}$$

Ugyanez maradékosztályokkal megfogalmazva:

$$\left. \begin{array}{l} \overline{a_1} = \overline{b_1} \\ \overline{a_2} = \overline{b_2} \end{array} \right\} \implies \begin{array}{l} \overline{a_1 \pm a_2} = \overline{b_1 \pm b_2} \quad \text{és} \\ \overline{a_1 \cdot a_2} = \overline{b_1 \cdot b_2}. \end{array}$$

Definíció

A modulo m maradékosztályok halmazán értelmezzük az összeadást, a kivonást és a szorzást a következőképpen:

$$\bar{a} \oplus \bar{b} := \overline{a + b}, \quad \bar{a} \ominus \bar{b} := \overline{a - b}, \quad \bar{a} \odot \bar{b} := \overline{a \cdot b}.$$

+	...	0	1	2	3	4	...
:	...	:	:	:	:	:	...
0	...	0	1	2	3	4	...
1	...	1	2	3	4	5	...
2	...	2	3	4	5	6	...
3	...	3	4	5	6	7	...
4	...	4	5	6	7	8	...
:	...	:	:	:	:	:	...

+	...	0	1	2	3	4	...
:	...	:	:	:	:	:	...
0	...	0	1	2	3	4	...
1	...	1	2	3	4	5	...
2	...	2	3	4	5	6	...
3	...	3	4	5	6	7	...
4	...	4	5	6	7	8	...
:	...	:	:	:	:	:	...

$\mathbb{Z}_4$ összeadó- és szorzótáblája

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

$\odot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Példa

Számoljunk $\mathbb{Z}_{15}$ -ben!

- $\bar{8} + \bar{10} = \bar{18} = \bar{3}$
- $\bar{8} - \bar{10} = \overline{-2} = \bar{13}$
- $\bar{8} \cdot \bar{10} = \overline{80} = \bar{5}$
- $\bar{8}/\bar{10} = ???$

Példa

Oldjuk meg $\mathbb{Z}_{15}$ -ben a $\overline{10} \cdot \overline{x} = \overline{8}$ egyenletet.

Megoldás

A $10x \equiv 8 \pmod{15}$ kongruenciát kell megoldani, de ennek nincs megoldása, mert $\text{lko}(10, 15) \nmid 8$.

Példa

Oldjuk meg $\mathbb{Z}_{15}$ -ben a $\overline{9} \cdot \overline{x} = \overline{6}$ egyenletet.

Megoldás

A $9x \equiv 6 \pmod{15}$ kongruenciát kell megoldani, ennek megoldása

$$x \equiv 4 \pmod{5},$$

ami három modulo 15 maradékosztályt is lefed.

Tehát három megoldás van $\mathbb{Z}_{15}$ -ben:

$$x = \overline{4}, \overline{9}, \overline{14}.$$

Tartalom

Bemelegítés

Lineáris kongruenciarendszerek

Maradékosztályok és maradékrendszerek

Számolás maradékosztályokkal

Redukált maradékosztályok, multiplikatív inverz, rend

Definíció

Azt mondjuk, hogy $\bar{a} \in \mathbb{Z}_m$ **redukált maradékosztály**, ha $\text{Inko}(a, m) = 1$.
A modulo m redukált maradékosztályok halmazát $\mathbb{Z}_m^*$ jelöli:

$$\mathbb{Z}_m^* = \{\bar{a} \in \mathbb{Z}_m : \text{Inko}(a, m) = 1\}.$$

Definíció

Azt mondjuk, hogy az $\bar{a}, \bar{b} \in \mathbb{Z}_m$ maradékosztályok egymás **multiplikatív inverzei**, ha $\bar{a} \cdot \bar{b} = \bar{1}$. Jelölés: $\bar{b} = \bar{a}^{-1}$.

Példa

Soroljuk fel $\mathbb{Z}_{15}^*$ elemeit, és határozzuk meg mindegyik elem inverzét.

Tétel

Egy $\bar{a} \in \mathbb{Z}_m$ maradékosztálynak akkor és csak akkor van multiplikatív inverze, ha $\text{Inko}(a, m) = 1$, azaz $\bar{a} \in \mathbb{Z}_m^*$.

Bizonyítás.

Az $ax \equiv 1 \pmod{m}$ lineáris kongruenciának akkor és csak akkor van megoldása, ha $\text{Inko}(a, m) \mid 1$.



A modulo 12 maradékosztályok hatványai

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	2	4	8	4	8	4	8	4	8	4	8	4	8	4	8	4	8	4	8
3	1	3	9	3	9	3	9	3	9	3	9	3	9	3	9	3	9	3	9	3
4	1	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
5	1	5	1	5	1	5	1	5	1	5	1	5	1	5	1	5	1	5	1	5
6	1	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	1	7	1	7	1	7	1	7	1	7	1	7	1	7	1	7	1	7	1	7
8	1	8	4	8	4	8	4	8	4	8	4	8	4	8	4	8	4	8	4	8
9	1	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9
10	1	10	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
11	1	11	1	11	1	11	1	11	1	11	1	11	1	11	1	11	1	11	1	11

Megfigyelések:

- A hatványok sorozata előbb-utóbb periodikussá válik.
- Ha redukált maradékosztályt hatványozunk, akkor a hatványok sorozata már a legelejétől kezdve periodikus. A következő periódus ilyenkor mindig 1-essel kezdődik.

Definíció

Egy $\bar{a}$ redukált maradékosztály **rendjén** azt a legkisebb pozitív egész kitevőt értjük, amelyre $\bar{a}$ -t emelve $\bar{1}$ -t kapunk. Jelölés: $o(\bar{a})$.

$$o(\bar{a}) := \min\{n \in \mathbb{N} : \bar{a}^n = \bar{1}\}$$

Tétel

Ha $\bar{a} \in \mathbb{Z}_m^*$ és $o(\bar{a}) = n$, akkor minden $k, \ell \in \mathbb{Z}$ esetén

$$\bar{a}^k = \bar{a}^\ell \iff k \equiv \ell \pmod{n}.$$

Az $\ell = 0$ speciális esetben azt kapjuk, hogy

$$\bar{a}^k = \bar{1} \iff n \mid k.$$

A modulo 9 redukált maradékosztályok hatványai

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	2	4	8	7	5	1	2	4	8	7	5	1	2	4	8	7	5	1	2
4	1	4	7	1	4	7	1	4	7	1	4	7	1	4	7	1	4	7	1	4
5	1	5	7	8	4	2	1	5	7	8	4	2	1	5	7	8	4	2	1	5
7	1	7	4	1	7	4	1	7	4	1	7	4	1	7	4	1	7	4	1	7
8	1	8	1	8	1	8	1	8	1	8	1	8	1	8	1	8	1	8	1	8

- $o(\overline{1}) = 1$
- $o(\overline{2}) = 6$
- $o(\overline{4}) = 3$
- $o(\overline{5}) = 6$
- $o(\overline{7}) = 3$
- $o(\overline{8}) = 2$