

MARADÉKOSZTÁLYOK

Waldhauser Tamás

SZTE Bolyai Intézet

Tartalom

Maradékosztályok és maradékrendszerek

Számolás maradékosztályokkal

Redukált maradékosztályok, multiplikatív inverz, rend

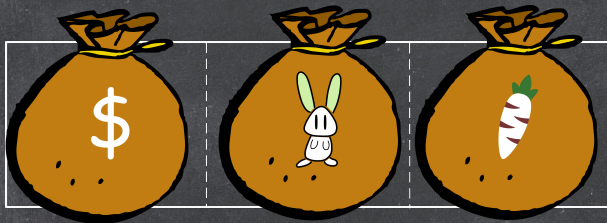
Emlékeztető

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.

9^{-6}	-5	8
12	1	14
0	13	5^{-4}
-3	7	11
3	10^{-2}	-1
6	4	2

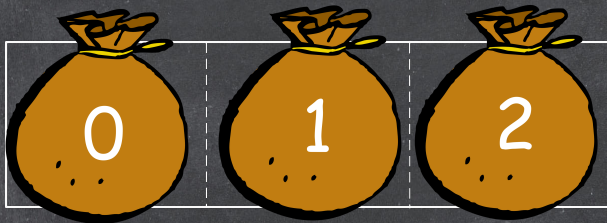
Emlékeztető

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.



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.



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

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

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

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

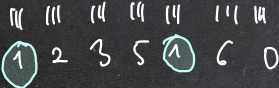
$$\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\} = \{\bar{1}, \bar{2}, \bar{3}\} = \{\overline{-325}, \overline{1707}, \overline{1777}\}$$

" " "
2 0 1

Definíció

Azt mondjuk, hogy az $a_1, \dots, a_m$ egész számok **teljes maradékrendszert** alkotnak modulo m , ha minden maradékosztályból pontosan egy elem lép fel, azaz $\{\overline{a_1}, \dots, \overline{a_m}\} = \mathbb{Z}_m$.

Példák

- $0, 1, 2$ teljes maradékrendszer modulo 3
- $1, 2, 3$ teljes maradékrendszer modulo 3
- $-325, 1707, 1777$ teljes maradékrendszer modulo 3
- $1, 2, 3, 5, 8, 13, 21$ NEM teljes maradékrendszer modulo 7


$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{5}$	$\overline{8}$	$\overline{13}$	$\overline{21}$
1	2	3	5	1	6	0

Példa

Teljes maradékrendszer-e $1000, 2000, \dots, 7000$ modulo 7?

$$1000z \quad (z=1, \dots, 7)$$

$$1000z_1 \equiv 1000z_2 \pmod{7}$$

$$\Updownarrow \text{ fel } (1000, 7) = 1$$

$$z_1 \equiv z_2 \pmod{7}$$

$$\Updownarrow$$

$$z_1 = z_2$$

IGTN

Tartalom

Maradékosztályok és maradékrendszerek

Számolás maradékosztályokkal

Redukált maradékosztályok, multiplikatív inverz, rend

Emlékeztető

A kongruenciareláció egy fontos tulajdonsága:

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

Ugyanez maradékosztályokkal megfogalmazva:

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

δ	δ	δ	δ
a_1	a_2	$a_1 + a_2$	
b_1	b_2	$b_1 + b_2$	

$\mathbb{Z}$

Definíció

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

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

+	...	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	...
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

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

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

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

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

Példák

Számoljunk $\mathbb{Z}_{15}$ -ben!

$$\bullet \bar{8} + \bar{10} = \overline{18} = \bar{3}$$

$$\bullet \bar{8} - \bar{10} = \overline{-2} = \bar{13}$$

$$\bullet \bar{8} \cdot \bar{10} = \overline{80} = \bar{5}$$

$$\bullet \bar{8} / \bar{10} = \cancel{\overline{8/10}} \quad \bar{8} / \bar{10} = \bar{x} \Leftrightarrow \bar{10} \cdot \bar{x} = \bar{8}$$

Példa

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

$$10x \equiv 8 \pmod{15}$$

$$\text{Léte } (10, 15) \nmid 8 \Rightarrow \text{nincs megoldás.}$$

$$\frac{\bar{8}}{\bar{10}} \text{ nem értelmezett}$$

Példa

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

$$9x \equiv 6 \pmod{15} \quad |:3$$

$$3x \equiv 2 \pmod{5}$$

$$3x \equiv 12 \pmod{5} \quad |:3$$

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

$$\frac{\bar{6}}{\bar{9}} = \bar{4}, \bar{9}, \bar{14}$$

nem egyértelmű

$$x = \dots, -1, 4, 9, 14, 19, 24, 29, 34, \dots$$

(Note: The numbers 14, 9, 14, 4, 9, 14, 9 are written below the sequence, with a green bracket underlining the first four: 14, 9, 14, 4)

Tartalom

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: $\bar{b} = \bar{a}^{-1}$.

Tétel

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

Biz. $\bar{x}$ inverze $\bar{a}$ -nak $\Leftrightarrow \bar{a} \cdot \bar{x} = \bar{1}$

$$\Leftrightarrow ax \equiv 1 \pmod{m}$$

$$\text{Van } x \Leftrightarrow \text{Inko}(a, m) \mid 1 \quad \square$$

Példa

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

$$\mathbb{Z}_{15} = \{\cancel{0}, \bar{1}, \bar{2}, \cancel{3}, \bar{4}, \cancel{5}, \cancel{6}, \bar{7}, \bar{8}, \cancel{9}, \cancel{10}, \bar{11}, \cancel{12}, \bar{13}, \bar{14}\}$$

$$\mathbb{Z}_{15}^* = \{\bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, \bar{11}, \bar{13}, \bar{14}\}$$

$$2x \equiv 1 \pmod{15}$$

$$2x \equiv 16 \pmod{15}$$

$$x \equiv 8 \pmod{15}$$

Példa

Oldjuk meg $\mathbb{Z}_{15}$ -ben a $\bar{7} \cdot \bar{x} = \bar{6}$ egyenletet.

$$\bar{7} \cdot \bar{x} = \bar{6} \iff \bar{x} = \bar{7}^{-1} \cdot \bar{6} = \bar{13} \cdot \bar{6} = \bar{78} = \bar{3}$$

$$\frac{\bar{6}}{\bar{7}} = \bar{6} \cdot \bar{7}^{-1}$$

$$\frac{\bar{6}}{\bar{7}} = \bar{6} \cdot \bar{7}^{-1}$$

Példa

Számítsuk ki $\mathbb{Z}_7$ -ben a $\bar{2}^{102}$ és $\bar{2}^{2021}$ hatványokat.

k	0	1	2	3	4	5	6	7	...	102	...	2021
$\bar{2}^k$	$\bar{1}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{2}$	...	$\bar{1}$	...	$\bar{4}$

Diagram illustrating the powers of $\bar{2}$ in $\mathbb{Z}_7$. The sequence of powers $\bar{2}^k$ for $k=0, 1, 2, \dots$ is $\bar{1}, \bar{2}, \bar{4}, \bar{1}, \bar{2}, \bar{4}, \bar{1}, \bar{2}, \dots$. The powers repeat every 3 steps, forming a cycle of length 3. The values $\bar{1}, \bar{2}, \bar{4}$ are highlighted in green boxes, and the cycle is indicated by orange brackets and ellipses.

$$102 \equiv 0 \pmod{3} \Rightarrow \bar{2}^{102} = \bar{2}^0 = \bar{1}$$

$$2021 \equiv 2 \pmod{3} \Rightarrow \bar{2}^{2021} = \bar{2}^2 = \bar{4}$$

$$\bar{2} \text{ rendje } 3 \quad \sigma(\bar{2}) = 3$$

$$\varphi$$

$$\bar{2}^*$$

$$\bar{1} \rightarrow \bar{2} \rightarrow \bar{4} \rightarrow \bar{1}$$

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

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