ELTE IK Diszkrét modellek alkalmazásai

4. gyakorlat

Koch-Gömöri Richárd

2021. szeptember 30.

Legnagyobb közös osztó

def (közös osztó): A $c \in \mathbb{Z}$ szám az $a, b \in \mathbb{Z}$ számok közös osztója ha $c \mid a \wedge c \mid b$

def (legnagyobb közös osztó): Két egész szám legnagyobb közös osztói azok a közös osztók, amelyek minden közös osztónak többesei.

feladat: 4. fsor. 1. fel: Határozza meg a 18 és 24 egész számok legnagyobb közös osztóit valamint $lnko(18, 24)$-t.

a 18 osztói: $\pm 1, \pm 2, \pm 3, \pm 6, \pm 9, \pm 18$

a 24 osztói: $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 12, \pm 24$

keressük azokat a közös osztókat, amelyek minden közös osztónak többesei

itt ez a ± 6, azaz 6 és -6

jelöljük $lnko(a, b)$-vel az a és b legnagyobb közös osztói közül a pozitívat, így az lnko egyértelmű

tehát $lnko(18, 24) = 6$

4. fsor 2. fel: Határozza meg az euklideszi algoritmussal a következő egész számok legnagyobb közös osztóját.

(b) 126 és 150

$150 = 126 \cdot ? + ?$

$150 = 126 \cdot 1 + 24$

$126 = 24 \cdot ? + ?$

$126 = 24 \cdot 5 + 6$

$24 = 6 \cdot ? + ?$

$24 = 6 \cdot 4 + 0$

a maradék 0, az algoritmus itt leáll

az utolsó nemnulla maradék lesz az lnko $\implies$ $lnko(126, 150) = 6$

4. fsor 2. fel: Határozza meg az euklideszi algoritmussal a következő egész számok legnagyobb közös osztóját.

(b) 33 és 21

$33 = 21 \cdot 1 + 12$

$21 = 12 \cdot 1 + 9$

$12 = 9 \cdot 1 + 3$

$9 = 3 \cdot 3 + 0$

$lnko(33, 21) = 3$

Kongruencia

def (kongruencia): Legyen $a, b, m \in \mathbb{Z}$. Azt mondjuk, hogy a kongruens b-vel modulo m, ha $m \mid a - b$

jelölés: $a \equiv b \pmod{m}$ vagy röviden $a \equiv b \ (m)$

4. fsor 3. fel: Döntse el, hogy igazak-e a következő kongruenciák.

$7 \equiv 3 \pmod{3}$

behelyettesítés a def.-be: $3 \mid 7 - 3$ hamis

$7 \equiv 3 \pmod{2}$

behelyettesítés a def.-be: $2 \mid 7 - 3$ igaz

$7 \equiv 3 \pmod{1}$

behelyettesítés a def.-be: $1 \mid 7 - 3$ igaz

állítás: $a \equiv b \pmod{m} \iff a \mod m = b \mod m$

4. fsor 3. fel

állítás: $a \equiv b \pmod{m} \iff a \mod m = b \mod m$

pl. $7 \equiv 3 \pmod{2}$

$7 \mod 2 = 1$

$3 \mod 2 = 1$

4. fsor 3. fel

$8 \equiv 10 \pmod 5$

$5 \mid 8 - 10$, hamis

$2 \equiv -1 \pmod 3$

$3 \mid 2 - (-1)$, igaz

$6 \equiv 6 \pmod{100}$

$100 \mid 6 - 6$, igaz

4. fsor 3. fel

behelyettesítés után látható h

$11 \equiv 8 \pmod 3$, $8 \equiv 5 \pmod 3$, $11 \equiv 5 \pmod 3$ mind igaz

a kongruencia tranzitív

$6 \equiv 6 \pmod{100}$ sejthető h reflexív

oszthatóságnál az előjel nem számít $\implies$ szimmetrikus is

$6 \equiv 2 \pmod 4$, $3 \equiv -5 \pmod 4$, $18 \equiv -10 \pmod 4$ igazak

állítás: $a \equiv b \pmod m$ és $c \equiv d \pmod m \implies ac \equiv bd \pmod m$

4. fsor 3. fel

$160 \equiv 80 \pmod{16}$, $16 \equiv 8 \pmod{8}$ igazak

10-zel osztás után az új modulus: $16/lnko(16,10) = 16/2 = 8$

állítás: $ac \equiv bc \pmod{m} \iff a \equiv b \left(\bmod \dfrac{m}{lnko(c,m)}\right)$

Eml: Ekvivalenciareláció, ekvivalenciaosztály

Egy $R \subseteq A \times A$ relációt ekvivalenciarelációnak nevezünk, ha reflexív, szimmetrikus és tranzitív

Egy $a \in A$ elem által meghatározott ekvivalenciaosztály:
$\overline{a} = \{b \in A : aRb\}$

pl. $A = \{1,2,3,4,5\}$, $R =$
$\{(1,1),(1,5),(2,2),(3,3),(3,4),(4,3),(4,4),(5,1),(5,5)\} \subseteq A \times A$
keressük meg mi lesz az 1 által meghatározott ekvivalenciaosztály, azaz $\overline{1}$

$\overline{1} = \{b \in A : 1Rb\} = \{1,5\}$

$\overline{2} = \{b \in A : 2Rb\} = \{2\}$

$\overline{3} = \{b \in A : 3Rb\} = \{3,4\}$

$\overline{4} = \{b \in A : 4Rb\} = \{3,4\} = \overline{3}$

$\overline{5} = \{b \in A : 5Rb\} = \{1,5\} = \overline{1}$, és több ekv. osztály nincs

Eml: Ekvivalenciareláció, ekvivalenciaosztály

az ekv. osztályok: $\{1,5\},\{2\},\{3,4\}$

ez egy osztályfelbontása az A halmaznak, hiszen:

- egyik sem üres
- páronként diszjunkt
- az uniójuk kiadja A-t

4. feladat

Mutassa meg, hogy a $R \subseteq \mathbb{Z} \times \mathbb{Z}$, $aRb \iff a \equiv b \pmod 5$ reláció ekvivalenciareláció. Mik lesznek az ekvivalenciaosztályok?

RST

ekv. osztályok?

$\overline{0} = \{b \in \mathbb{Z} : 0Rb\} = \{b \in \mathbb{Z} : 5 \mid 0 - b\} =$
$\{0, 5, 10, 15, \ldots, -5, -10, -15, \ldots\} = \{5\text{-tel osztva 0 a maradék}\}$

$\overline{1} = \{b \in \mathbb{Z} : 1Rb\} = \{b \in \mathbb{Z} : 5 \mid 1 - b\} =$
$\{1, 6, 11, 16, \ldots, -4, -9, -14, \ldots\} = \{5\text{-tel osztva 1 a maradék}\}$

$\overline{2} = \{5\text{-tel osztva 2 a maradék}\}$

$\overline{3} = \{5\text{-tel osztva 3 a maradék}\}$

$\overline{4} = \{5\text{-tel osztva 4 a maradék}\}$

más ekv. osztály nincs

a $0, 1, 2, 3, 4$ számokat reprezentánsoknak nevezzük

Maradékosztály

def (maradékosztály): Az $R \subseteq \mathbb{Z} \times \mathbb{Z}$, $aRb \iff a \equiv b \pmod m$ ekvivalenciareláció ekvivalenciaosztályait modulo m maradékosztályoknak nevezzük.

jelölés: az $x \in \mathbb{Z}$ elem által reprezentált maradékosztály modulo m: $\overline{x} \mod m$ vagy röviden: $\overline{x}$

Maradékosztály

$\overline{0} \mod 5 = \{0, 5, 10, 15, 20, 25, ...\}$
$\overline{1} \mod 5 = \{1, 6, 11, 16, 21, ..., \}$
$\overline{2} \mod 5 = \{2, 7, 12, 17, 22, ...\}$
$\overline{3} \mod 5 = \{3, 8, 13, 18, 23, ...\}$
$\overline{4} \mod 5 = \{4, 9, 14, 19, 24, ...\}$

állítás: $\overline{x} \mod m = \{x + k \cdot m | k \in \mathbb{Z}\}$

Maradékosztály

pl. $2 \equiv 7 \pmod 5$, de az nem igaz h $2 \equiv 3 \pmod 5$

állítás: $a, b \in \overline{x} \mod m \iff a \equiv b \pmod m$

pl. $\overline{4} = \{4, 9, 14, 19, 24, ...\}$

pl. $\overline{9} = \{..., 9, 14, 19, 24, 29, ...\}$

$\overline{4} = \overline{9} \ (\mod 5)$

az egyenlőség nem véletlen, hisz $4 \equiv 9 \pmod 5$

állítás: $\overline{a} = \overline{b} \ (\mod m) \iff a \equiv b \pmod m$

Maradékosztály

pl. $2 \equiv 12 \pmod 5$, valamint $12 \equiv 7 \pmod 5$

a tranzitivitás miatt ekkor $2 \equiv 7 \pmod 5$, ami valóban igaz

rövidebben: a 12-ből kivontunk 5-öt , sőt akárhányszor kivonhatjuk vagy hozzáadhatjuk a modulust

$2 \equiv 7 \pmod 5$

$2 \equiv 2 \pmod 5$

$2 \equiv -3 \pmod 5$

$2 \equiv -8 \pmod 5$

$2 \equiv 17 \pmod 5$

$2 \equiv 22 \pmod 5$

$2 \equiv 27 \pmod 5$

... hiszen ugyanazoknak a maradékosztályoknak a reprezentánsai