ELTE IK Diszkrét modellek alkalmazásai

5. gyakorlat

Koch-Gömöri Richárd

2021. október 6.

5. feladat

Oldja meg a következő kongruencia egyenleteket.

$2x \equiv 3 \pmod 4$

kongruencia egyenlet: keresünk olyat $x \in \mathbb{Z}$-et (vagy akár többet), amelyet beírva x helyére a $2x \equiv 3 \pmod 4$ kongruenciába, igazat kapunk

$2x \equiv 3 \pmod 4$ próbálgatással nem találunk megoldást
$2x \equiv 3 \pmod 4 \iff 4 \mid 2x - 3$, $2x - 3$ mindig páratlan, sose lesz 4-gyel osztható $\implies$ nincs megoldás

tétel (lineáris kongruencia egyenlet megoldhatósága):
Legyen $a, b, m, x \in \mathbb{Z}$. Az $ax \equiv b \pmod m$ lineáris kongruencia egyenlet akkor és csak akkor oldható meg, ha $lnko(a, m) \mid b$

ez itt valóban nem teljesült, hiszen $2 = lnko(2, 4) \mid 3$ hamis

5. feladat

$x \equiv 2 \pmod 3$

van megoldás?

$lnko(1,3) = 1 \mid 2 \implies$ van megoldás

$x = 2$ nyilván alkalmas

$x = 2 + 3 = 5$ is

$x = 2, 5, 8, 11, ..., -1, -4, -7, ...$

$x = 2 + k \cdot 3, k \in \mathbb{Z}$

a megoldás a $\overline{2}$ mod 3 maradékosztály

5. feladat

$x \equiv 7 \pmod 2$

van megoldás?

$lnko(1,2) = 1 \mid 7 \implies$ van megoldás

$x \equiv 7 \pmod 2$

$x \equiv 5 \pmod 2$

$x \equiv 3 \pmod 2$

$x \equiv 1 \pmod 2$

$x = 1 + k \cdot 2, k \in \mathbb{Z}$

a megoldás az $\overline{1}$ mod 2 maradékosztály

5. feladat

$12x \equiv 8 \pmod{20}$

$lnko(12, 20) = 4 \mid 8 \implies$ van megoldás

$12x \equiv 48 \pmod{20}$

$x \equiv 4 \pmod{\frac{20}{lnko(20, 12)}}$

$x \equiv 4 \pmod{5}$

$x = 4 + k \cdot 5, k \in \mathbb{Z}$

a megoldások a $\overline{4}$ mod 5 maradékosztály elemei

$x = 4, 9, 14, 19, 24, 29, 34, 39, 44, 49, 54, 59, \dots$

$$\overline{4 + 0 \cdot 5} \quad \text{mod } 20 = \{4 + k \cdot 20, k \in \mathbb{Z}\} = \{4, 24, 44, \dots\}$$
$$\overline{4 + 1 \cdot 5} \quad \text{mod } 20 = \{9 + k \cdot 20, k \in \mathbb{Z}\} = \{9, 29, 49, \dots\}$$
$$\overline{4 + 2 \cdot 5} \quad \text{mod } 20 = \{14 + k \cdot 20, k \in \mathbb{Z}\} = \{14, 34, 54, \dots\}$$
$$\overline{4 + 3 \cdot 5} \quad \text{mod } 20 = \{19 + k \cdot 20, k \in \mathbb{Z}\} = \{19, 39, 59, \dots\}$$

5. feladat

$lnko(20, 12) = 4$ db különböző maradékosztály modulo 20

a végső megoldás tehát a $\overline{4}, \overline{9}, \overline{14}, \overline{19}$ maradékosztályok modulo 20

Polinomok

Legyen A és B olyan halmaz, amelyen értelmezve van egy összeadás $(+)$ és egy szorzás $(\cdot)$ művelet, valamint teljesülnek a szokásos műveleti szabályok (pl. összeadás kommutativitása etc).

Ilyen halmaz pl. egész számok, valós számok, komplex számok, ...

def (Polinom) Legyen $a_0, a_1, ..., a_n \in A, \quad x \in B, \quad a_n \neq 0$. A feletti egyváltozós polinomnak nevezzük a
$p = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + ... + a_1 \cdot x + a_0$ kifejezéseket.

a_i a polinom együtthatói, x a polinom változója

a_n főegyüttható, a_0 a szabad tag / konstans tag

$\deg p := n$ a polinom fokszáma

jelölje $A[x]$ az A feletti, x-változós polinomok halmazát

pl. $A = \mathbb{Z}, \quad B = \mathbb{C}$

$p \in \mathbb{Z}[x], \quad p = x^3 - 15x^2 + 84x - 170$

$\deg p = 3$

$q \in \mathbb{Z}[x], \quad q = x$

ekkor $p + q = x^3 - 15x^2 + 85x - 170$

etc ...

def (helyettesítési érték) Egy $p \in A[x]$ $c \in B$-beli helyettesítési értéke:
$p(c) = a_n \cdot c^n + a_{n-1} \cdot c^{n-1} + ... + a_1 \cdot c + a_0$
A $c \in B$ a p gyöke, ha $f(c) = 0$

pl. $p \in \mathbb{Z}[x]$, $p = x^3 - 15x^2 + 84x - 170$
$p(2) = -54$, $p(0) = -170$, $p(5) = 0$
$x_1 = 5$ gyöke a p polinomnak
a másik két gyök: $x_2 = 5 - 3i$, $x_3 = 5 + 3i$
ez a két gyök komplex, a polinom együtthatói egészek

Moduláris aritmetika

Legyen $m \in \mathbb{N}$, $\mathbb{Z}_m := \{\overline{0}, \overline{1}, ..., \overline{m-1}\}$
pl. $m = 6$, $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$
$\overline{2} + \overline{3} = ?$

def (műveletek maradékosztályokkal) Legyen $\overline{a}, \overline{b} \in \mathbb{Z}_m$, $k \in \mathbb{Z}$.
Ekkor:
$\overline{a} + \overline{b} := \overline{a + b}$
$\overline{a} - \overline{b} := \overline{a - b}$
$\overline{a} \cdot \overline{b} := \overline{a \cdot b}$
$k \cdot \overline{a} := \overline{k \cdot a}$

$\overline{2} + \overline{3} = \overline{5}$
$\overline{2} + \overline{5} = \overline{7} = \overline{1}$, hiszen $7 \mod 6 = 1$
mod nélküli írásmód: $2 + 5 = 7 = 1$ (6)