ELTE IK Diszkrét modellek alkalmazásai

6. gyakorlat

Koch-Gömöri Richárd

2021. október 13.

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: $2 + 5 = 7 = 1 \ \ (6)$

Moduláris aritmetika

$m = 6$, $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$

$\overline{1} + \overline{2} = \overline{3}$

$\overline{4} + \overline{4} = \overline{8} = \overline{2}$

$\overline{2} \cdot \overline{2} = \overline{4}$

$\overline{3} \cdot \overline{4} = \overline{12} = \overline{0}$

osztás?

pl. $\dfrac{\overline{1}}{\overline{5}} = \dfrac{\overline{-5}}{\overline{5}} = \overline{-1} = \overline{5}$

de pl. $\dfrac{\overline{1}}{\overline{3}}$ nem végezhető el

multiplikatív inverz

multiplikatív inverz (reciprok) racionális számok körében:

a 2 multiplikatív inverze: $\frac{1}{2}$

a 3 multiplikatív inverze: $\frac{1}{3}$

def (multiplikatív inverz): Az x multiplikatív inverze: $\frac{1}{x}$

a racionális számok körében végezzük el a $8/4$ osztást:

- keressük 4 multiplikatív inverzét: $\frac{1}{4}$

- szorozzuk a számlálóhoz a nevező multiplikatív inverzét: $8 \cdot \frac{1}{4} = 2$

vegyük észre a multiplikatív inverz tulajdonságát:

$2 \cdot \frac{1}{2} = 1$

$3 \cdot \frac{1}{3} = 1$

$x \cdot \frac{1}{x} = 1$

multiplikatív inverz

def (maradékosztály multiplikatív inverze): Egy $\overline{a} \in \mathbb{Z}_m$ multiplikatív inverze: $\overline{x} \in \mathbb{Z}_m$, ha $\overline{a} \cdot \overline{x} = \overline{1}$

keressük az $\overline{5}$ multiplikatív inverzét:

$\overline{5} \cdot \overline{x} = \overline{1}$

$x = ?$

$\overline{5 \cdot x} = \overline{1}$

$5x \equiv 1 \pmod 6$

megoldható mert $lnko(5, 6) = 1 \mid 1$

$5x \equiv 25 \pmod 6$

$x \equiv 5 \pmod 6$

$\implies \frac{1}{5} = 5$

$\frac{\overline{3}}{\overline{5}} = ?$

keressük az $\overline{5}$ multiplikatív inverzét:

láttuk h $\frac{1}{\overline{5}} = \overline{5}$

$\implies \frac{\overline{3}}{\overline{5}} = \overline{3} \cdot \overline{5} = \overline{15} = \overline{3}$

keressük az $\overline{3}$ multiplikatív inverzét:

$\overline{3} \cdot \overline{x} = \overline{1}$

$x = ?$

$\overline{3 \cdot x} = \overline{1}$

$3x \equiv 1 \pmod 6$

nem oldható meg mert $lnko(3, 6) = 3$, a $3 \mid 1$ oszthatóság nem teljesül

$\overline{3}$-nak nem létezik multiplikatív inverze (mod 6-ban)

$\implies$ egy $\frac{\overline{a}}{\overline{b}}$ osztás nem biztos h elvégezhető keressünk olyan $m \in \mathbb{N}$ számokat, amikor mindig elvégezhető az osztás

minden $\overline{a} \in \mathbb{Z}_m$-re annak kell teljesülnie, h $lnko(a, m) \mid 1$

mivel lnko nemnegatív egész, ezért $lnko(a, m) = 1$

ezt csak a prímszámok elégítik ki

tétel (multiplikatív inverz létezése): Minden $\overline{a} \in \mathbb{Z}_m$ maradékosztálynak létezik $\overline{x} \in \mathbb{Z}_m$ multiplikatív inverze akkor és csak akkor, ha m prímszám.

$\mathbb{Z}_m$ feletti polinomok

legyen pl. $m = 7$ prímszám

$p \in \mathbb{Z}_m[x], \quad p = \overline{5} \cdot x^4 + x^3 + \overline{4} \cdot x^2 + \overline{6}$

$p(\overline{2}) = \overline{5} \cdot \overline{2}^4 + \overline{2}^3 + \overline{4} \cdot \overline{2}^2 + \overline{6} = \overline{110} = \overline{5} \pmod 7$

a továbbiakban használjuk a mod nélküli írásmódot:

$p(2) = 5 \cdot 2^4 + 2^3 + 4 \cdot 2^2 + 6 = 110 = 5 \ \ (7)$

továbbá pl. $p + 5 \cdot x^2 + 1 = 5 \cdot x^4 + x^3 + 4 \cdot x^2 + 6 + 5 \cdot x^2 + 1 =$
$5 \cdot x^4 + x^3 + 2 \cdot x^2 \ \ (7)$

Interpoláció

lényege: Olyan polinomot keresünk, amely adott pontokra illeszkedik.

$n+1$ db pontra n-edfokú polinom illeszkedik

def (interpoláció) Legyen $x_0, x_1, \ldots, x_n \in [a; b]$ különböző alappontok, $y_0, y_1, \ldots, y_n \in \mathbb{R}$ értékek. Keresünk olyan n-edfokú $p \in \mathbb{C}[x]$ polinomot, melyre $\forall i = 0, 1, \ldots, n: \quad p(x_i) = y_i$
p-t interpolációs polinomnak nevezzük

sokféle megoldás van erre a feladatra, egy konkrét interpolációs polinomot előállító módszer a Lagrange-interpoláció

def (Lagrange-alappolinom) Az $x_0, x_1, \ldots, x_n$ különböző alappontok által meghatározott k-adik Lagrange-alappolinom:

$$l_k(x) = \prod_{j=0, j\neq k}^{n} \frac{x - x_j}{x_k - x_j} \qquad k \text{ lehet } 0, 1, \ldots, n$$

pl. legyen 4 pont, erre 3-adfokú polinom illeszthető

$n = 3, x_0 = 0, x_1 = 1, x_2 = 4, x_3 = -1$

$$l_0(x) = \prod_{j=0, j\neq 0}^{3} \frac{x - x_j}{x_0 - x_j} = \frac{x-1}{0-1} \cdot \frac{x-4}{0-4} \cdot \frac{x+1}{0+1} = \frac{1}{4}x^3 - x^2 - \frac{1}{4}x + 1$$

$$l_1(x) = \prod_{j=0, j\neq 1}^{3} \frac{x - x_j}{x_1 - x_j} = \frac{x-0}{1-0} \cdot \frac{x-4}{1-4} \cdot \frac{x+1}{1+1} = -\frac{1}{6}x^3 + \frac{1}{2}x^2 + \frac{2}{3}x$$

$$l_2(x) = \prod_{j=0, j\neq 2}^{3} \frac{x - x_j}{x_2 - x_j} = \frac{x-0}{4-0} \cdot \frac{x-1}{4-1} \cdot \frac{x+1}{4+1} = \frac{1}{60}x^3 - \frac{1}{60}x$$

$$l_3(x) = \prod_{j=0, j\neq 3}^{3} \frac{x - x_j}{x_3 - x_j} = \frac{x-0}{-1-0} \cdot \frac{x-1}{-1-1} \cdot \frac{x-4}{-1-4} =$$

$$-\frac{1}{10}x^3 + \frac{1}{2}x^2 - \frac{2}{5}x$$

def (Lagrange interpolációs polinom) $p(x) := \sum_{k=0}^{n} y_k \cdot l_k(x)$

a példában legyen $y_0 = 3, y_1 = 3, y_2 = 7, y_3 = 0$
ekkor: $p(x) = 3 \cdot l_0(x) + 3 \cdot l_1(x) + 7 \cdot l_2(x) + 0 \cdot l_3(x) =$
$\frac{22}{60}x^3 - \frac{3}{2}x^2 + \frac{68}{60}x + 3$

tétel (interpolációs polinom létezése) $n \geq 0$ esetén $n+1$ darab ponthoz egyértelműen létezik p interpolációs polinom, melyre $\deg p = n$

Feladat: Illesszünk Z_5-beli interpolációs polinomot a $(2,4),(1,0),(4,3)$ pontokra.
$n = 2$

$l_0(x) = \prod_{j=0, j\neq 0}^{2} \frac{x - x_j}{x_0 - x_j} = \frac{(x-1)\cdot(x-4)}{(2-1)\cdot(2-4)} = \frac{x^2 - 4x - x + 4}{3} =$
$\frac{x^2+4}{3}$ (5)

$l_1(x) = \prod_{j=0, j\neq 1}^{2} \frac{x - x_j}{x_1 - x_j} = \frac{(x-2)\cdot(x-4)}{(1-2)\cdot(1-4)} = \frac{x^2 - 4x - 2x + 8}{3} =$
$\frac{x^2+4x+3}{3}$ (5)

$$l_2(x) = \prod_{j=0, j\neq 2}^{2} \frac{x - x_j}{x_2 - x_j} = \frac{(x-2)\cdot(x-1)}{(4-2)\cdot(4-1)} = \frac{x^2 - x - 2x + 2}{1} =$$

$$x^2 + 2x + 2 \ \ (5)$$

$$p(x) = \sum_{k=0}^{2} y_k \cdot l_k(x) =$$

$$4 \cdot \frac{x^2+4}{3} + 0 \cdot \frac{x^2+4x+3}{3} + 3 \cdot (x^2+2x+2) =$$

$$\frac{4x^2+16}{3} + 3x^2 + 6x + 6 = \frac{4x^2+16+9x^2+18x+18}{3} =$$

$$\frac{13x^2+18x+34}{3} = \frac{3x^2+3x+4}{3} = x^2 + x + \frac{4}{3} \ \ (5)$$

végezzük el a $\frac{4}{3}$ (5) osztást

végezzük el a $\frac{4}{3}$ (5) osztást

3 inverze legyen $y \in \mathbb{Z}_5$

$3 \cdot y = 1 \ \ (5)$

$3y \equiv 1 \pmod 5$

$3y \equiv 6 \pmod 5$

$y \equiv 2 \pmod 5$

3 inverze: 2

$$\frac{4}{3} = 4 \cdot 2 = 8 = 3 \ \ (5)$$

$$p(x) = x^2 + x + 3$$