Diszkrét modellek alkalmazásai

4. gyakorlat

Boda Bálint

2022. őszi félév

1. Euklideszi algoritmus

Az Euklideszi algoritmus egy optimális mód az $a, b \in \mathbb{Z}$ számok legnagyobb közös osztójának meghatározására. Ha $a < b$, akkor felcseréljük a két számot majd addig ismételjük a következő lépést amíg az r_i osztási maradék 0 nem lesz.

$$
\begin{aligned}
a &= q_0 \cdot b + r_0 \\
b &= q_1 \cdot r_0 + r_1 \\
r_0 &= q_2 \cdot r_1 + r_2 \\
r_1 &= q_3 \cdot r_2 + r_3 \\
&\dots
\end{aligned}
$$

Ekkor $\operatorname{lnko}(a, b) = r_{i-1}$.

Példa. $lnko(360, 225) = 45$

$$
\begin{aligned}
360 &= 1 \cdot 225 + 135 \\
225 &= 1 \cdot 135 + 90 \\
135 &= 1 \cdot 90 + \mathbf{45} \\
90 &= 2 \cdot 45 + 0
\end{aligned}
$$

1. Számítsuk ki a következő számok legnagyobb közös osztóját!

a) 30 és 70 b) 126 és 150 c) 105 és 231

d) 132 és 275 e) 33 és 21

Megoldás.

a) $\mathrm{lnko}\,(30, 70) = 10$

$$\begin{aligned} 70 &= 2 \cdot 30 + \mathbf{10} \\ 30 &= 3 \cdot 10 + 0 \end{aligned}$$

b) $\mathrm{lnko}\,(126, 150) = 6$

$$\begin{aligned} 150 &= 1 \cdot 126 + 24 \\ 126 &= 5 \cdot 24 + \mathbf{6} \\ 24 &= 4 \cdot 6 + 0 \end{aligned}$$

c) $\mathrm{lnko}\,(105, 231) = 21$

$$\begin{aligned} 231 &= 2 \cdot 105 + \mathbf{21} \\ 105 &= 5 \cdot 21 + 0 \end{aligned}$$

d) $\mathrm{lnko}\,(132, 275) = 11$

$$\begin{aligned} 275 &= 2 \cdot 132 + \mathbf{11} \\ 132 &= 12 \cdot 11 + 0 \end{aligned}$$

e) $\mathrm{lnko}\,(33, 21) = 3$

$$\begin{aligned} 33 &= 1 \cdot 21 + 12 \\ 21 &= 1 \cdot 12 + 9 \\ 12 &= 1 \cdot 9 + \mathbf{3} \\ 9 &= 3 \cdot 3 + 0 \end{aligned}$$

1.1. Python nyelven

```
def lnko(a,b):
    if a == b:
        return a
    if a < b:
        a, b = b, a
    while (b > 0):
        a, b = b, a % b
    return a
```

2. Kongruencia

Definíció (Kongruencia)**.** Kongruenciának nevezzük a

$$\{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a \bmod m = \ b \bmod m \quad (m \in \mathbb{Z})\}$$

$a \equiv b \pmod m$-el (ejtsd: a kongruens b modulo m) jelölt relációt.

Tétel. A kongruencia ekvivalenciareláció, ekvivalenciaosztályait pedig **maradékosztályoknak** nevezzük.

Példa.

- $5 \equiv 11 \pmod 6$
- $2 \not\equiv 6 \pmod 3$
- $-8 \equiv 10 \pmod 6 = 0$, mert $-2 \cdot 6 + 4 = -8$ és $1 \cdot 6 + 4 = 10$

2. Igazak-e a következő kongruenciák?

a) $7 \equiv 3 \pmod 3$	b) $7 \equiv 3 \pmod 2$	c) $7 \equiv 3 \pmod 1$
d) $8 \equiv 10 \pmod 5$	e) $2 \equiv -1 \pmod 3$	f) $6 \equiv 6 \pmod{100}$
g) $11 \equiv 8 \pmod 3$	h) $8 \equiv 5 \pmod 3$	i) $11 \equiv 5 \pmod 3$
j) $6 \equiv 2 \pmod 4$	k) $3 \equiv -5 \pmod 4$	l) $18 \equiv -10 \pmod 4$
m) $160 \equiv 80 \pmod{16}$	n) $16 \equiv 8 \pmod 8$	

Megoldás.

a) hamis $(1 \neq 0)$	b) igaz $(1 = 1)$	c) hamis $(0 = 0)$
d) hamis $(3 \neq 0)$	e) igaz $(2 = 2)$	f) igaz $(6 = 6)$
g) igaz $(2 = 2)$	h) igaz $(2 = 2)$	i) igaz $(2 = 2)$
j) igaz $(2 = 2)$	k) igaz $(3 = 3)$	l) igaz $(2 = 2)$
m) igaz $(0 = 0)$	n) igaz $(0 = 0)$	

2.1. Lineáris kongruenciák

Lineáris kongruenciának nevezzük az $ax \equiv b \pmod{m}$ alakú kongruenciákat.

Tétel. Egy $ax \equiv b \pmod{m}$ kongruencia, akkor oldható meg, ha

$$\operatorname{lnko}(a, m) \mid b$$

Példa.

$$x \equiv 5 \pmod{7}$$

Mivel $\operatorname{lnko}(1, 7) = 1$ osztója 5-nek ezért a kongruenciaegyenlet megoldható és megoldásai az $5 + 7t$ ($t \in \mathbb{Z}$) alakú egész számok.

Megjegyzés. A megoldások halmaza, az $x \equiv 5 \pmod{7}$ reláció, azon ekvivalenciaosztálya, melynek eleminek 7-el vett osztási maradéka 5.

2.1.1. Kongruencia azonosságai

- A kongruenciához szabadon hozzáadhatunk és kivonhatunk.

$$x + 4 \equiv 5 \pmod{7} \iff x \equiv 1 \pmod{7}$$

- A kongruencia egyik oldalához hozzáadhatjuk vagy kivonhatjuk m-et.

$$x \equiv 12 \pmod{7} \iff x \equiv 5 \pmod{7}$$

- A kongruenciát megszorozhatunk egy tetszőleges $k \in \mathbb{Z}$ számmal.

$$x \equiv 4 \pmod{7} \iff 2x \equiv 8 \pmod{7}$$

- A kongruenciát leoszthatjuk egy tetszőleges $k \in \mathbb{Z}$ számmal, de ekkor a modulust is osztani kell.

$$4x \equiv 8 \pmod{14} \iff x \equiv 2 \pmod{7}$$

$$ax \equiv b \pmod{m} \iff x \equiv \frac{b}{a} \left(\bmod \frac{m}{\operatorname{lnko}(a, m)} \right)$$

3. Oldja meg a következő kongruenciaegyenleteket!

a) $2x \equiv 3 \pmod 4$ b) $x \equiv 2 \pmod 3$ c) $x \equiv 7 \pmod 2$

d) $12x \equiv 8 \pmod{20}$ e) $22x \equiv 8 \pmod{10}$ f) $15x \equiv -1 \pmod 7$

Megoldás.

a) $2x \equiv 3 \pmod 4$, mivel $\text{lnko}(2,4) = 2 \nmid 3$, ezért nincs megoldás.

b) $x \equiv 2 \pmod 3$, $\text{lnko}\,(1,3) = 1 \mid 2$, ezért a kongruencia megoldható és megoldásai a $2 + 3t$ $(t \in \mathbb{Z})$ alakú számok.

c) $x \equiv 7 \pmod 2$, $\text{lnko}\,(1,2) = 1 \mid 7$
$x = 7 + 2t\,(t \in \mathbb{Z})$

d) $12x \equiv 8 \pmod{20}$ $\qquad \text{lnko}\,(12,20) = 4 \mid 8$

$$\begin{aligned} 12x \equiv 8 \pmod{20} &\iff 12x \equiv 48 \pmod{20} \\ &\iff x \equiv 4 \quad \left(\text{mod } \frac{20}{lnko(12,20)} = \frac{20}{4} = 5\right) \end{aligned}$$

$x = 4 + 5t$ $(t \in \mathbb{Z})$

e) $22x \equiv 8 \pmod{10}$ $\qquad \text{lnko}\,(12,10) = 2 \mid 8$

$$\begin{aligned} 22x \equiv 8 \pmod{20} &\iff 22x \equiv 88 \pmod{10} \\ &\iff x \equiv 4 \quad \left(\text{mod } \frac{10}{2} = 5\right) \end{aligned}$$

$x = 4 + 5t$ $(t \in \mathbb{Z})$

f) $15x \equiv -1 \pmod 7$ $\qquad \text{lnko}\,(15,7) = 1 \mid -1$

$$\begin{aligned} 15x \equiv -1 \pmod 7 &\iff 15x \equiv 6 \pmod 7 \\ &\iff 15x \equiv 90 \pmod 7 \\ &\iff x \equiv 6 \pmod 7 \end{aligned}$$

$x = 6 + 7t$ $(t \in \mathbb{Z})$