A 11a, 12a, 13a feladatok megoldásai

11a feladat

Számítsa ki az f és g polinomok legnagyobb közös osztóját.

$$f = x^4 + 2x^3 + 4x^2 + 2x + 3, \qquad g = x^3 + x^2 + x - 3.$$

Megoldás.

Hajtsuk végre az euklideszi algoritmust:

$$\begin{aligned} x^4 + 2x^3 + 4x^2 + 2x + 3 &= (x+1) \cdot \left(x^3 + x^2 + x - 3\right) + 2x^2 + 4x + 6 \\ x^3 + x^2 + x - 3 &= (x-1) \cdot \left(x^2 + 2x + 3\right) + 0 \end{aligned}$$

Tehát $\text{Inko}\,(f, g) \sim 2x^2 + 4x + 6 \sim x^2 + 2x + 3$.

Hab a tortán:

$$\begin{aligned} f &= \left(x^2 + 1\right)\left(x^2 + 2x + 3\right), \quad \text{gyökei:} \quad \pm i, \ -1 \pm \sqrt{2}i \\ g &= (x-1)\left(x^2 + 2x + 3\right), \quad \text{gyökei:} \quad 1, \ -1 \pm \sqrt{2}i \end{aligned}$$

Még több hab a tortán

Az euklideszi algoritmus tömörebben összefoglalva:

$$\begin{aligned} f &= (x+1)\cdot g &+ \quad & 2x^2+4x+6 \\ g &= (x-1)\cdot\left(x^2+2x+3\right) &+ \quad & 0 \end{aligned}$$

Tehát $\operatorname{Inko}(f,g) \sim 2x^2+4x+6 \sim x^2+2x+3$.

Fejezzük ki a legnagyobb közös osztót f és g segítségével:

$$x^2+2x+3 = \frac{1}{2}\left(f-(x+1)\cdot g\right) = \frac{1}{2}\cdot f + \left(-\frac{1}{2}x-\frac{1}{2}\right)\cdot g$$

Azt kaptuk, hogy az $fu+gv = \operatorname{Inko}(f,g)$ egyenlet egy megoldása:

$$u_0 = \frac{1}{2}, \quad v_0 = -\frac{1}{2}x-\frac{1}{2}.$$

12a feladat

Oldja meg az $fu + gv = \text{lnko}\,(f, g)$ egyenletet.

$$f = x^6 + \overline{6}, \qquad g = x^4 + \overline{5}x + \overline{1} \in \mathbb{Z}_7\,[x]$$

Megoldás.

Euklideszi algoritmussal számolunk, és a maradékokat kifejezzük f és g segítségével:

$$\begin{aligned}
f &= x^2 \cdot g &&+ \overline{2}x^3 + \overline{6}x^2 + \overline{6} \\
g &= (\overline{4}x + \overline{2}) \cdot (\overline{2}x^3 + \overline{6}x^2 + \overline{6}) &&+ \overline{2}x^2 + \overline{2}x + \overline{3} \\
\overline{2}x^3 + \overline{6}x^2 + \overline{6} &= (x + \overline{2}) \cdot (\overline{2}x^2 + \overline{2}x + \overline{3}) &&+ \overline{0}
\end{aligned}$$

Az első osztás maradéka:

$$\overline{2}x^3 + \overline{6}x^2 + \overline{6} = f - x^2 \cdot g$$

A második osztás maradéka:

$$\begin{aligned}
\overline{2}x^2 + \overline{2}x + \overline{3} &= g - (\overline{4}x + \overline{2}) \cdot (\overline{2}x^3 + \overline{6}x^2 + \overline{6}) \\
&= g - (\overline{4}x + \overline{2}) \cdot (f - x^2 \cdot g) \\
&= -(\overline{4}x + \overline{2}) \cdot f + (\overline{1} + (\overline{4}x + \overline{2})\,x^2) \cdot g \\
&= (\overline{3}x + \overline{5}) \cdot f + (\overline{4}x^3 + \overline{2}x^2 + \overline{1}) \cdot g
\end{aligned}$$

12a feladat

Azt kaptuk, hogy

$$\overline{2}x^2 + \overline{2}x + \overline{3} \;=\; \left(\overline{3}x + \overline{5}\right) \cdot f + \left(\overline{4}x^3 + \overline{2}x^2 + \overline{1}\right) \cdot g$$

A legnagyobb közös osztó a fenti piros polinommal asszociált főpolinom:

$$\begin{aligned} \text{Inko}\,(f, g) &= \overline{2}^{-1} \cdot \left(\overline{2}x^2 + \overline{2}x + \overline{3}\right) \\ &= \overline{4} \cdot \left(\overline{2}x^2 + \overline{2}x + \overline{3}\right) \\ &= x^2 + x + \overline{5} \end{aligned}$$

A legnagyobb közös osztó kifejezése f és g segítségével:

$$\begin{aligned} \overline{2}^{-1} \cdot \left(\overline{2}x^2 + \overline{2}x + \overline{3}\right) &= \overline{4} \cdot \left(\overline{3}x + \overline{5}\right) \cdot f + \overline{4} \cdot \left(\overline{4}x^3 + \overline{2}x^2 + \overline{1}\right) \cdot g \\ &= \left(\overline{5}x + \overline{6}\right) \cdot f + \left(\overline{2}x^3 + x^2 + \overline{4}\right) \cdot g \end{aligned}$$

Az $fu + gv = x^2 + x + \overline{5}$ egyenlet egy megoldása:

$$u_0 = \overline{5}x + \overline{6}, \quad v_0 = \overline{2}x^3 + x^2 + \overline{4}.$$

13a feladat

Oldja meg az $f \cdot u \equiv \overline{1} \pmod{m}$ kongruenciát.

$$f = x^2 + \overline{3}x + \overline{1}, \qquad m = x^3 + \overline{2}x^2 + \overline{4}x + \overline{2} \in \mathbb{Z}_5[x].$$

Megoldás.

A kongruenciát átfogalmazzuk diofantoszi egyenletté:

$$f \cdot u \equiv \overline{1} \pmod{m} \iff \exists v \in \mathbb{Z}_5[x] : \; fu = \overline{1} + mv$$

$$\iff \exists v \in \mathbb{Z}_5[x] : \; fu - mv = \overline{1}$$

Egy megoldás: $u_0 = x^2 + \overline{4}x + \overline{1}$ (és $v_0 = \overline{4}x$).

Az általános megoldás: $u \equiv x^2 + \overline{4}x + \overline{1} \pmod{m}$.

Megjegyzés.

Eredményünk így is megfogalmazható: az $\overline{f} \in \mathbb{Z}_5[x] \,/\, (m)$ maradékosztály multiplikatív inverze

$$\left(\overline{f}\right)^{-1} = \overline{x^2 + \overline{4}x + \overline{1}}.$$

Még egy lineáris kongruencia

Oldja meg az $f \cdot u \equiv \overline{1} \pmod{m}$ kongruenciát a $\mathbb{Z}_2[x]$ polinomgyűrűben, ahol

$$f = x^2 + \overline{1}, \qquad m = x^3 + x^2 + \overline{1}.$$

A szokásos módszer:

$$\begin{aligned} f \cdot u \equiv \overline{1} \pmod{m} \quad &\iff \quad \exists v \in \mathbb{Z}_2[x] : \ fu = \overline{1} + mv \\ &\iff \quad \exists v \in \mathbb{Z}_2[x] : \ fu - mv = \overline{1} \end{aligned}$$

$\ldots$ $u_0 = x^2 + x + \overline{1}$. Tehát a kongruencia megoldása: $u \equiv x^2 + x + \overline{1} \pmod{m}$.

Egy másik gondolatmenet:

$$\begin{aligned} f \cdot u \equiv \overline{1} \pmod{m} \quad &\iff \quad \left(x + \overline{1}\right)^2 \cdot u \equiv x^3 + x^2 \pmod{x^3 + x^2 + \overline{1}} \\ &\iff \quad \left(x + \overline{1}\right) \cdot u \equiv x^2 \pmod{x^3 + x^2 + \overline{1}} \\ &\iff \quad \left(x + \overline{1}\right) \cdot u \equiv x^3 + \overline{1} \pmod{x^3 + x^2 + \overline{1}} \\ &\iff \quad u \equiv x^2 + x + \overline{1} \pmod{x^3 + x^2 + \overline{1}} \end{aligned}$$